Global Information Assurance Certification Paper

Global Information Assurance Certification
GCIH Practical Assignment
Option 1 – Exploit in Action
Version 2.1a

Exploit in Action: Lovgate – Lessons Learned From The Lovgate Worm

By William T Tucek
August 25th 2003

Table of Contents

Summary

In early February of 2003 a new Worm had been propagating throughout the Internet known as Lovgate. This Worm and its variants are still active today. Lovgate may not be considered as harmful as other viruses such as Nimda, but it has the ability to spread very quickly, which inevitably it did do in the early part of February 2003. This is due in part to the use of two delivery methods utilized by the Worm, which includes social engineering and abuse of mis configurations of Windows file sharing systems. The Worm also carried an additional payload, which included an outbound e-mail and the potential for a Trojan.

This paper will describe not only the Worm in detail but also will illustrate how it impacted a mid sized companies network and data security. It was also discuss how the network was vulnerable due to the lack of some very basic security measures and the absence of defense in depth. The Incident Response procedure will be discussed to understand how it was performed during this incident.

The Exploit

1.1 NAME:

W32/lovgate.a@m and variants

Related CERT Advisory: CA-2003-08 [1]

Snort TM Event ID: 2123 [2]

Bugtrak ID: 7385 [3]

1.2 Affected Operating Systems:

Microsoft Windows 95 & 98SE

Microsoft Windows ME

Microsoft Windows XP Home & XP Professional

Microsoft Windows 2000 Professional & Server

Microsoft Windows 2000 Advanced Server

Microsoft Windows 2000 Datacenter Server

1.3 Affected Applications, Services and Protocols

Application: Microsoft Outlook, Outlook Express, Windows sharing

Service: Messaging API Windows functions, workstation service.

Protocols: SMB Services including Ports 139 TCP, SMTP services, RPC

1.4 Brief Description

The Worm propagates itself via email (it contains its own SMTP engine) and over network shares. It copies itself to folders/subfolders on open shares, and replies to messages in the user inbox. Additionally, it drops a backdoor component (port 10168, and 1192 on Windows NT and Windows 2000 based systems, is opened on victim machines). The Worm itself is a Windows PE EXE file, written in Microsoft Visual C++, and compressed by "AsPack". The infection length is 78,848 Bytes. [4]

1.5 Aliases and Variants

Aliases

WORM_LOVGATE.C [Trend],
Win32/Lovgate.C@mm [RAV],
W32/Lovgate.c@M [McAfee],
I-Worm.Supnot.c [KAV],
W32/Lovgate-B [Sophos],
Win32.Lovgate.C [CA]

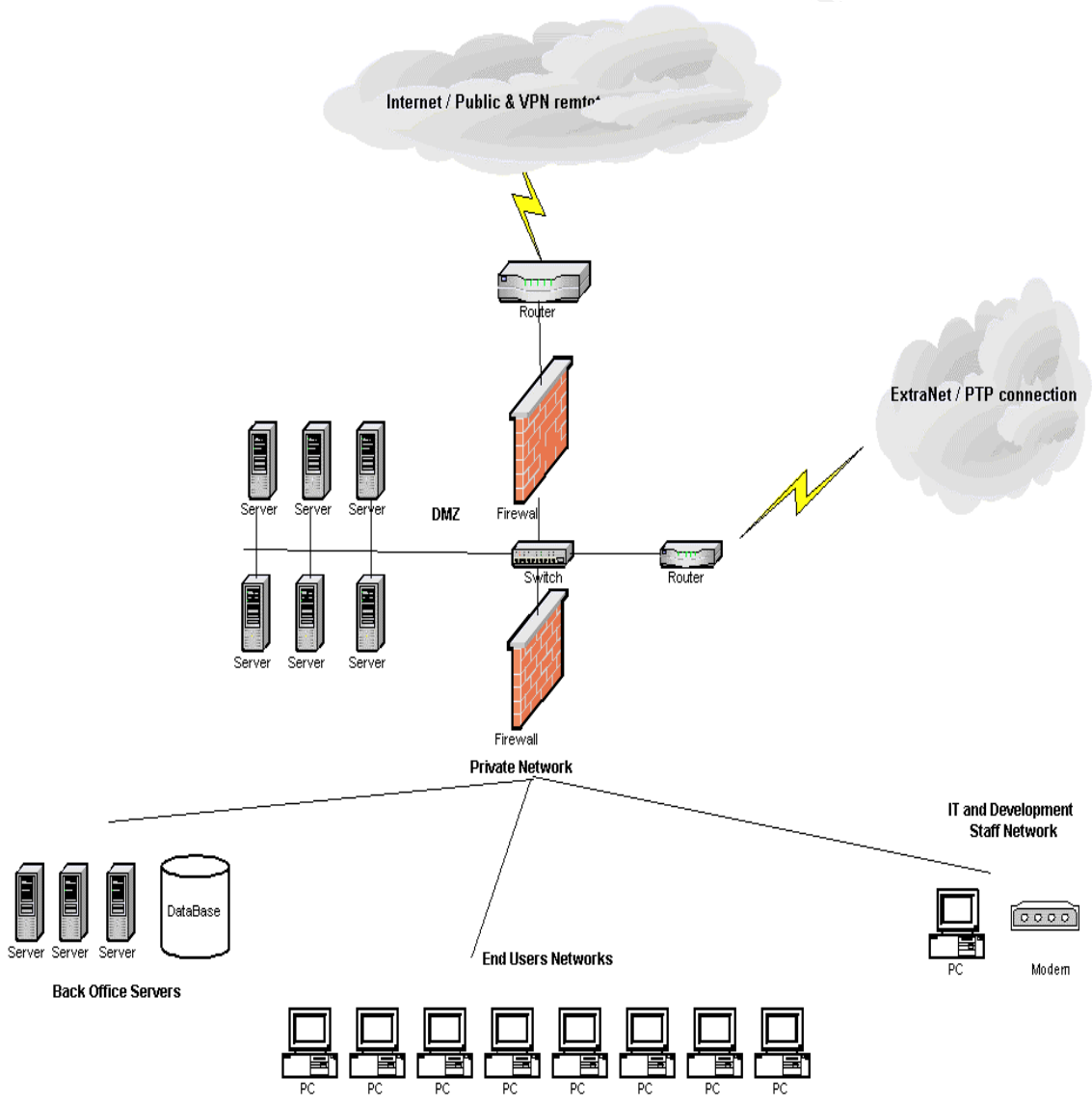
Variants

Worm.lovegate.f,
W32/LovGate.F-m,
I-Worm.LovGate.f,
W32/Lovegate.g
W32.HLLW.Lovgate@mm
W32.HLLW.Lovgate.B@mm

2. The Attack

2.1 Network Diagram

Figure 1



2.2 Description of Network

The Network can be characterized as typical of many of today's' corporate networks by having an adequate perimeter security infrastructure. However, it is lacking in a layered approach to security within the perimeter. This includes not only network devices but also in security procedures as well. From the public we side a firewall is in place which blocks unwanted inbound traffic and a valiant attempt was made to Architect a tiered solution to create a DMZ and segregate internet facing servers. We will describe however the weak controls of outbound initiated protocols were present. In addition several unauthorized modems existed along with weak policies for external VPN users and poor or non-existent anti virus configurations.

Figure 1 represents the Network described in this paper along with the key components of the diagram, which are listed below.

Perimeter Security

Perimeter security, as defined in this network is comprised of several layers of network infrastructure. The first layer of security is a router, which sits at the border of the external network. The router is configured to provide basic static filtering for ping floods and other network type denial of service attacks.

DMZ and Internet Facing Servers

The DMZ consists of an area protected in a two tiered layers firewalls. The outer most firewall, a Cisco PIX, provides primary security for the DMZ and private network by rules that allow only needed traffic to the Internet facing servers such as HTTP and HTTPS from the Internet.

Within the DMZ, a number of Internet facing servers including SMTP gateway, FTP and a number of web-based applications servers are held. These servers have hardened operating systems according to industry best practices and relatively good security. An IDS Sensor, ISS Network Sensors are also deployed within the DMZ on a port-duplicating switch to capture traffic on this Network.

Finally on the innermost layer of the perimeter is a Checkpoint FW1, which provides network address translation and has strong external rules to prevent inbound attacks that make it past the PIX. However the rules for outbound traffic are very limited and allow for most protocols to be accessed to both the Internet and the DMZ.

Extranet Connection

This network connection, a Frame Relay enables a business partner to connect to applications hosted in both the DMZ and those held on back office servers within the private network. Traffic from the extranet router is allowed for specific protocols and destination IP addresses.

VPN Connections

VPN service is provided to employees into the private network by use of CheckPoint Firewall 1 Client to Site VPN. Unfortunately, in the configuration exists two weaknesses within the areas of Policy enforcement and two-factor authentication. VPN administration and process of accounts also have weaknesses such as poor account cleanup and no review of logging for usage.

Private Network

Finally the internal layer of the network is the private network. Located behind the CheckPoint Firewall 1. The Private network contains a large number of end user subnets containing over 500 Nodes. In addition, a number of back office servers including databases are held along with a network containing development servers. The majority of these systems are Microsoft operating systems for back office servers primarily being windows 2K and NT4.0 Servers, The end user workstations are predominantly Microsoft which includes windows 98, NT.40 workstation, 2000 Professional and Windows XP.

2.3 Protocol Description

There are two primary protocols involved in the propagation of the Lovgate Worm. The first is use of the SMTP service and the second is the use of SMB services. The use of SMTP services is invoked when an infected machine, which has MAPI-compliant e-mail clients such as Microsoft Outlook or Outlook Express, takes advantage of these programs auto reply function within the e-mail program.

When e-mail arrives, the virus attempts to send a copy of itself to the sender through this functionally. This functionality of the Worm adds a bit social engineering with it's presentation appearing to be from trusted or at least acknowledged e-mail addresses to unsuspecting recipients of the Worm.

The second protocol involved is the use of SMB Services. SMB Services – Server Message Blocks, are described as way or protocol for sharing of data on a network. This can include things such as files, printers, serial ports and other communications types such as named pipes. Microsoft uses this protocol with NTLM authentication for user level access. [5]

The W32/lovgate.a@m work takes advantage of this protocol by guessing at commonly used username and password scenarios to access remote shares by way of SMB services.

Other TCP ports utilized by the Worm include 10168,1192 and 20168, which have been identified as source for back door authentication and remote control of the infected machine.

2.4 How the Exploit Works

When the Worm is executed depending upon the version of Windows operating system several things occur during the installation which are as follows: This description was prepared from information provided at the Network Associates web site [5]

On Windows 95,98 & ME the following occurs:

- The Worm makes several copies of itself within the operating system in up to five different locations within the Windows operating system.
- On Windows 95/98 & ME Operating Systems, RPC services are added
- Several files are created in the "%System% folder " and then executed, within these files a Trojan back door is included.
- Adds several values to the registry and installs a command shell.
- A modification to the several default registry values is made to make the command shell accessible remotely.
- The Worm Copies itself to all the network-shared folders and subfolders with file names that are to entice a user to open or execute by use of social engineering.
- Port is opened and listens on TCP port 10168 and notifies the hacker using email at one of the two addresses. The hacker then has an authentication routine for access to the machine. After entering the correct password, the Worm will start a command shell for the hacker.
- Searches several folders to see if the Worm has already been installed on the machines and attempts to locate e-mail address on the machine and sends a copy of it to those addresses.
- Attempts to reply to any messages received from an e-mail client if present on the machine and sends a copy of it to those addresses, which are located within the user profiles.

On Windows NT4.0, 2000 and XP the following occurs:

- The Worm Copies itself as %System%\Ssrv.exe or the "Winnt\System32"
- It creates a Registry Key for KittyXP.sql\Install and Services\dll_reg

- Next, it adds a value for RPC services to the registry, and the following values are also added. taskdll ondll_reg server

- If the Worm detects the process Lsass.exe, it attempts to create a remote thread in that particular process and inject a hook to 1.dll

- Injects another thread into Lsass.exe, which creates a listening server on TCP port 20,168. This server gives anyone remote access without any authentication.

- Starts the Backdoor Trojan component as the service, "Windows Management Extension," which listens on TCP port 1192.

- Scans all the computers on the local network and uses the following passwords to attempt to log in as "Administrator:"

- If the Worm successfully logs on to a remote computer, it attempts to copy itself as \\<remote.computer.name>\admin$\system32\stg.exe ,
and then, it attempts to start the file on the remote computer as the service, "Microsoft Network Services Firewall."

2.5 Descriptions and Diagram of Attack

Phase I – The Invasion

In this attack it was believed that the Worm obtained it's beachhead on the company's private network through a poorly secured NT4.0 workstation. This was determined through analysis of Intrusion Detection System, Firewall and Server logs. The Log review consisted of analyzing time stamps from these logs, particularly for suspicious network scans, failed access to locked down servers and outbound e-mails after the Worm had propagated. The log Review aids in identifying the vector machine.

The workstation (We will call "X1" for the sake of this paper) was identified as belonging to a test network maintained by the Systems Administration staff and was found to be non compliant to the companies security policies and standards described for a personal computing device. X1 was found to have an unauthorized modem and RAS – Remote Access Services running, which were used by the owner to subvert Internal security controls for access to blocked web sites and other outbound protocols by the company.

X1 was used to download e-mail from a POP3 account from the users Internet service provider, which is how the Worm was believed to have entered the network. Anti virus software was found running on the machine, however the software was not scheduled to scan and the Antiviral signatures were almost a year old.

In addition, X1 had several network accessible shares with read and write access. The user made a practice to log into the machine as a "local administrator" which was the same user / password used as part of a standard for Systems Administrators for doing maintenance on console of stand alone (not belonging to a domain or workgroup) Servers.

Finally, X1 had become infected, which was through the owner falling prey to the socially engineered methods to entice the user to execute it. Once executed, the Worm began to spread rapidly throughout the company's networks, through open shares and e-mail replies. The infection included what were thought to be hardened servers, which hosted Internet applications.

Phase II – The Enemy Digs in

With one machine now infected, the Worm began to spread on the test network to other machines on that subnet. These machines included QA machines used to test applications to be eventually used in a production environment. Some machines actually communicate to the production environment acting as a fail over box for disaster recovery purposes.

Servers also communicated to the Internet facing tier through the use of Microsoft Net bios services, which a firewall rule permitted access. In addition, these servers were standalone servers and were accessed via console or by PCAnywhere by use of the same user and password, which was used by X1.

Phase III – The Enemy Advances

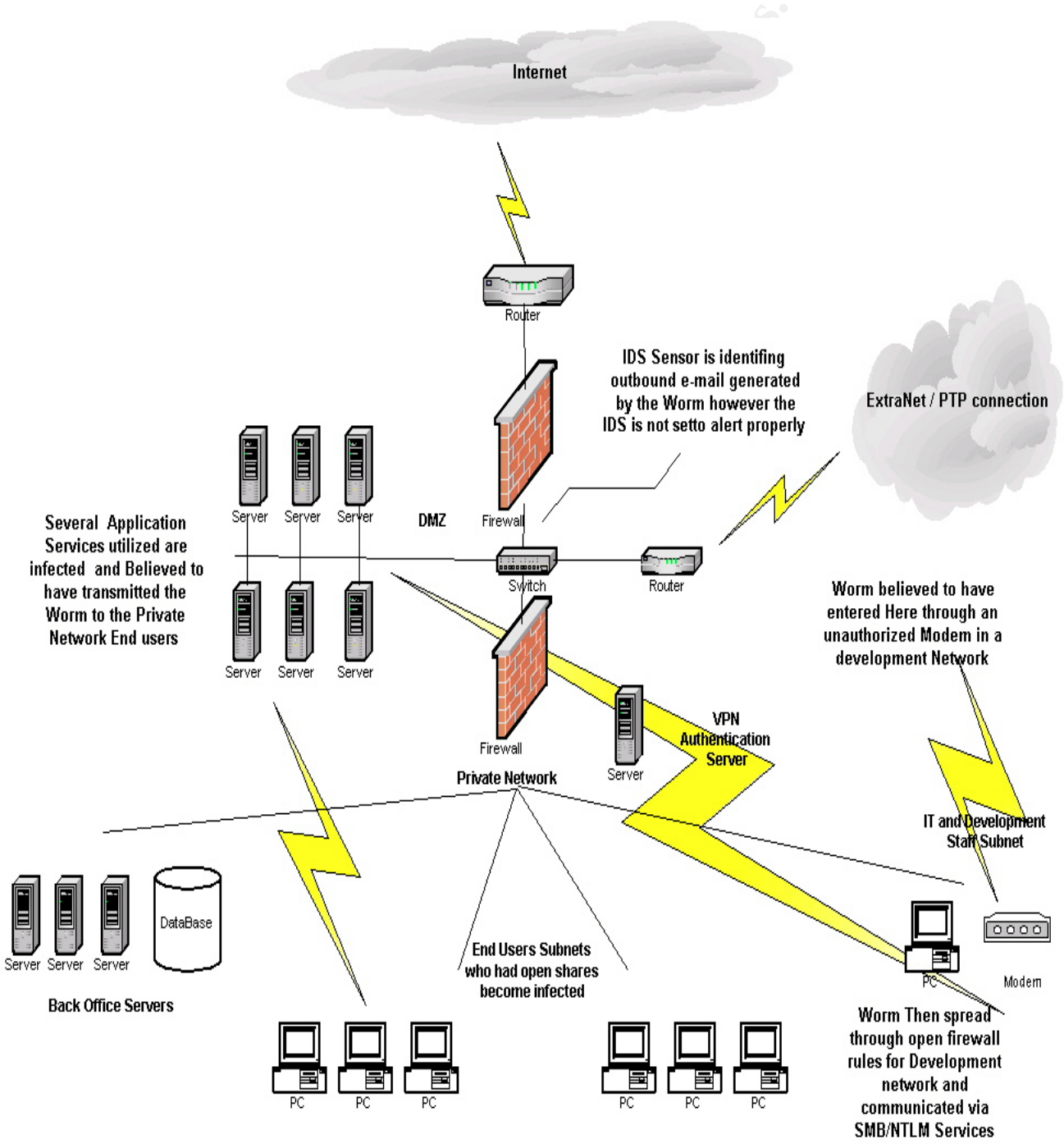
One production server within the DMZ (we will call the machine X2), was left logged on all the time with no time out values or failed logins attempts for shut down in order to overcome issues with the application locking out it's users. Rather than address the application issues not meeting the security requirements the decision had been made to accept the risk by management. These vulnerabilities led to the second major area of Infection of the Worm, and the greatest impact to the business, which was the servers, located in the DMZ, which were used by customers, and employees who worked in the field.

Phase IV – We are being overrun

Now with the Worm spreading to a number of test and application servers, it now propagates to several end users PC's in the private network. Although the IT staff work hard to update Anti virus software and scan machines throughout the network, some machines appear to be re infected after being cleaned initially. This appears to be from the Worm's ability to take advantage of open and write able windows shares. At this point the IT staff is overwhelmed to contain the Worm since the current environment has no policy addressing Windows ability to secure Microsoft's Windows sharing.

Many PC's on the network have open shares with poor access control allowing for even write able access to the "everyone group". To fuel the spread, poor desktop management allows for some users to have local administrator access of there own PC's, which they sometime use, as does the Worm to spread. Also at this time the mail service is seeing a good deal of traffic dealing with the Worm generating e-mail going to both the hackers site and reply's to other infected victims.

Figure 2 Network Diagram



2.5 Signature of Attack

The Worm could be identified by several methods, which were as follows: An E-mail, which generated by use of a particular subject and attachment. Scanning activity of the infected machine for net bios shares and the signature or footprint of an infected machine.

Email Signatures

In order to multiply, the Worm uses its own SMTP engine for the creation of email messages. IT then adds infected attachments to the email as described earlier. Next the mass mails with the infected email messages are broadcast, during which the email message may appear to be one of the following, which were provided by a description of this Worm at http://www.viruslist.com/ [6]

Subject: Documents
Attachment: Docs.exe
Message:: Send me your comments...

Subject: Roms
Attachment: Roms.exe
Message:: Test this ROM! IT ROCKS!.

Subject: Pr0n!
Attachment: Sex.exe
Message:: Adult content!!! Use with parental advisory.

Subject: Evaluation copy
Attachment: Setup.exe
Message:: Test it 30 days for free.

Subject: Help
Attachment: Source.exe
Message:: I'm going crazy... please try to find the bug!

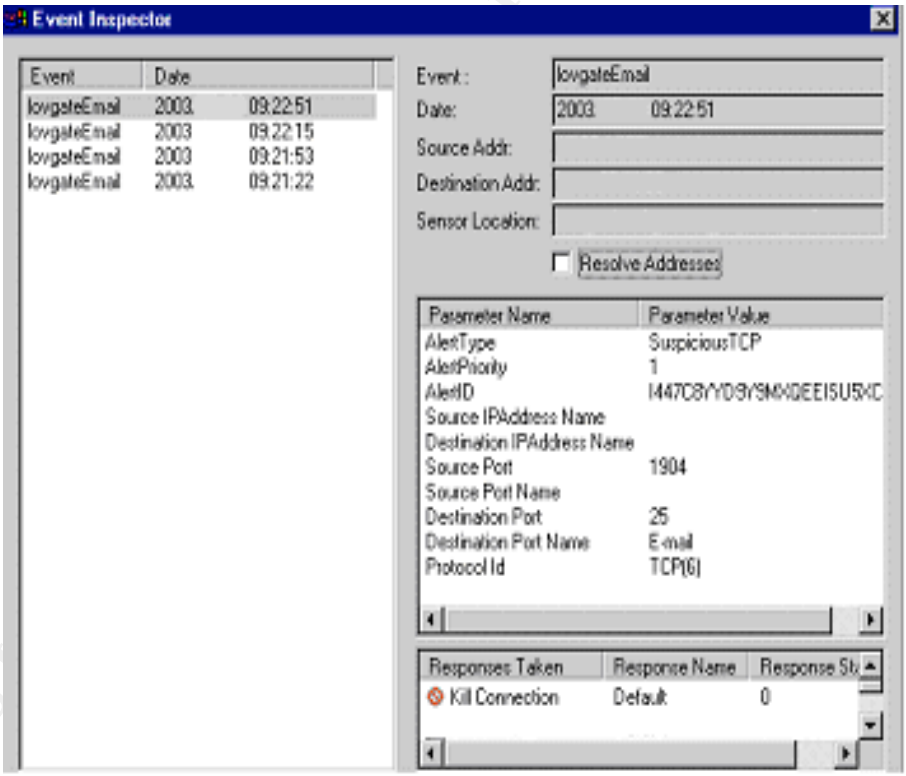
Subject: Beta
Attachment: _SetupB.exe
Message: Send reply if you want to be official beta tester.

Subject: Do not release
Attachment: Pack.exe
Message: This

Intrusion Detection

Signatures for the lovgate Worm for Intrusion Detection systems are also available from different sources including commercial and non-commercial sites. ISS [7] – http://www.iss.net, for example has developed an IDS signature matching a pattern for the lovgate Worm for use with its RealSecure System, which appears to be based on the e-mail, which is generated from the mass mailings of the Worm as illustrated in the example below.

Figure 3 – ISS Alert for Lovgate



Other Intrusion Detection Systems, such as Snort, have signatures seeking infected machines scanning subnets for open shares, such as in the example below.

alert tcp $EXTERNAL_NET any -> $HOME_NET 139 (msg:"VIRUS Lovgate Fileshare 139"; dsize > 500; content:"|40 00 00 C0 2E 61 73 70 61 63 6B 00|"; rev:1;) [8]

Footprint of an Infected Machine

Typically with Lovgate infected machines, TCP port 10168 open on the victim machine. A method of identification for any infected machines should include port scans of this port, network wide, to identify any suspected machines as illustrated below. In addition to the open port, it is often found that there are sometimes writable shares open on the machines as well.

Starting nmap V. (www.insecure.org/nmap/)
Host (XX.XX.XX.XX) appears to be up ... good.
Initiating SYN Stealth Scan against (XX.XX.XX.XX)
Adding TCP port 139 (state open).
Adding TCP port 135 (state open).
Adding TCP port 10168 (state open).

2.6 How to protect against the attack

Protecting against the attack of the Lovgate Worm can be done in a tactical and strategic approach. In both methods several aspects should be addressed to solve only this Worm outbreak but also future virus attacks to come.

Tactical approach – Lovgate outbreak

For the outbreak of this Worm, quick identification, containment and eradication are needed. In a layered security approach, precautions should be taken at all areas of the network, which includes the following:

- External Firewalls: Block all outbound and outbound net bios traffic - TCP Ports 135, 139, as well as any unneeded protocols.

- Intrusion Detections Systems: ensure that IDS signatures are loaded for this Worm and send e-mail alert to Security staff. The list of infected machines then should be sent to help desk support to clean the infected machine properly.

- E-mail systems: Should be configured to block attachments used by this Worm such as .exe. Also block any inbound or outbound from e-mail from the Worm writers creators site such as “163.com”

- Configuration and Desktop Management: Shares with write access for everyone or anonymous access should be reconfigured for only authenticated users and specific to user ID’s as needed. Anti Virus software should be updated and configured to scan the machines on a frequent basis.

- Security Awareness: End users should be informed of the current Threat and an e-mail describing it should be sent out or posted on an internal web page.

Strategic Approach – the long-term approach

For future Virus, Worms and other related attacks a more strategic plan should be adopted in each of the areas mention below.

- Perimeter Security: a formulated method and schedule for review of perimeter security should be developed. This includes a review of Firewall and router rules and access lists. New firewall rules and router updates should be processed through a procedure to include security review.

- Intrusion Detections Systems and Antivirus software on mail gateways should be reviewed at least weekly to ensure that systems are configured properly. Systems should have the latest updates and signatures, alerts should be sent to the correct staff and provide procedures to follow up on the alerts.

- E-mail systems: Should be configured to block attachments commonly used by viruses and Worm such as .vbs, .bat, .exe, .pif and .scr files. Domains, which are blacklisted on such sites that a frequent violators for SPAM or vectors for viruses should be blocked.

- Configuration Management: Procedures for standardized desktop configurations should be created and should be enforced within the organization. Change management procedures should be created for access and changes made to production servers and adhered to. Antivirus management should be automated and reporting of policy violators should be reported on an enterprise wide.

- Security Awareness: Programs aimed at social engineering should be included in training of end users. Training programs should be a required part of the employee-training regimen on an ongoing basis. Training specific to System Administration and development staff should also be included to ensure staff with access to production system fully understands security risks and exposures.

3.0 The Incident Handling Process

This incident was one of a number, which affected this company that was unfortunately ill prepared for these types of occurrences. In addition, the company did not have strong Information Technology policies and procedures for incidence handling and also a number of other areas that led to this incident. Unfortunately, many companies, both large and small do not have adequate methods to deal with crises when it relates to technological issues that can impact the business.

3.1 Preparation

Preparation for this incident and others like it could be considered minimal. The company had limited means to detect security violations and react to them in either the technological and or organization areas. Despite these major shortcomings the IT department did maintain the following areas in order to deal with or prevent security incidents:

- The Company had been developing a Disaster Recovery Plan, which included organization of personal. This plan had been modified and utilized in the previous minor outages of the production environment and also utilized for this incident.

- The primary persons responsible for the declaration of an IT related emergency were the CIO and Director of IT who would then organize the IT Team to attend to the issue.

- The Company subscribed to antiviral protections, which were installed at e-mail gateways, these gateways were kept updated on a regular basis. Notifications were sent to the e-mail administrator.

- An Intrusion Detection system was in place, however it was not well configured to Alert for key events. The Event logs were available, however they were rarely reviewed, as was the case for Firewall logs and Server logs.

3.2 Identification

The identification of this incident began when a Systems Administrator received numerous calls from end users that called to report what appeared to be strange e-mails being generated from other company employees. Around the same time, the e-mail administrator was receiving alerts for e-mail being generated internally for the Lovgate Worm.

Also during the early investigation, it was observed that the infected end user machines often had outdated Antivirus signatures or did not have the software properly configured or even running. Which aided in the spread of the Worm. The Intrusion Detection System also reported alerts for the Worm, however the IT staff was not actively monitoring the system.

The sample below of infected e-mails as provided by information regarding this Worm at Symantec [9]

From: <Infected User's Name>
To: <Original Sender>
Subject: RE: <Original Subject>

Message body:
"'<Infected User's Name>' wrote:
====
><Original Body>
>
====

<Original Sender's SMTP account> account auto-reply:

If you can keep your head when all about you
Are losing theirs and blaming it on you;
If you can trust yourself when all men doubt you,
But make allowance for their doubting too;
If you can wait and not be tired by waiting,
Or, being lied about,don't deal in lies,
Or, being hated, don't give way to hating,
And yet don't look too good, nor talk too wise;
... ... more look to the attachment.

> Get your FREE <Original Sender's SMTP account> account now! <
Attachment: (Randomly selected from any of the following)
I am For u.doc.exe
Britney spears nude.exe.txt.exe
joke.pif
DSL Modem Uncapper.rar.exe
Industry Giant II.exe
StarWars2 - CloneAttack.rm.scr
dreamweaver MX (crack).exe
Shakira.zip.exe
SETUP.EXE
Macromedia Flash.scr
How to Crack all gamez.exe
Me_nude.AVI.pif
s3msong.MP3.pif
Deutsch BloodPatch!.exe
Sex in Office.rm.scr
the hardcore game-.pif

3.3 Containment

Once the Worm was identified and the technical aspects understood the IT team went into action. The team realized that the Worm was spreading via e-mail and by open shares.

There first action was to ensure that the end users were aware of the situation and an e-mail alert to the company's end users was sent out about the virus and instructed users not to open

any attachments from unknown sources and or any attachments fitting the signature of the Worm.

The External Firewalls were then reviewed to ensure that all outbound net bios traffic - TCP Ports 135, 139, as well as any unneeded protocols was blocked. Intrusion Detections Systems were updated and signatures were loaded for this Worm.

The e-mail system – a Microsoft Exchange system was next reviewed to ensure that it was configured properly, had the latest antiviral signatures and was scanning all mail both inbound and out. Any alert for an infected e-mail was forwarded to the team to identify the internal sender for staff to clean the machine.

E -mail systems were reviewed to ensure that attachments used by this Worm such as .exe were denied entry into the network. Also blocked was any inbound or outbound from e-mail from the Worm writers creators site such as "163.com"

3.4 Eradication

Now with the Worm contained, the team next focused on purging it from the network.

The group's next step was to identify all vulnerable and infected machines on the network. These were identified in one of three ways – virus software console e-mail notifications, IDS alerts for the Worm signature or ISS scan results.

A network scan was performed on all networks within the company utilizing a commercial product – ISS. Scans from the network revealed some surprising results to the IT staff. Several dozen machines were identified with vulnerabilities susceptible to the Worm, which included null passwords and open shares.

The IDS system was updated with newer signatures and alerts were configured specifically to send e-mail to the team whenever the Worms's patterns were identified on the network. The machines identified as infected or vulnerable were then removed from the network by the network staff turning off the switch port connection for the machine.

Now armed with a list of infected machines the IT team then visited each of the machines to ensure that it was no longer a vector for the Worm. Each infected machine was reviewed to remove and clean the machine for the Worm per the anti virus vendor's suggestions.

Next, the work began to secure the environment. Network Shares were locked down to the only specified users and groups. Machines were checked to ensure that they had a secure local administrator password. A review of the configuration antiviral software was done to ensure latest virus definitions and scanning activity was scheduled.

Figure #5 - ISS scans finding of Lovgate infected PC

Network Vulnerability Assessment Report **Sorted by Severity**

This report lists the vulnerabilities detected by Internet Scanner after scanning the network.
Intended audience: This report is intended for security technicians (Security Administrators, Network Administrators,
Workstation Support Engineers, or Helpdesk Support Engineers).
Purpose: For each host, the report provides the IP address, the DNS name, the operating system type, and remedy
information for vulnerabilities detected by Internet Scanner.

Vulnerability H High M Medium A Low

Session Information

Session Name:	lovgate footprint	**File Name:**	lovgate footprint
Policy:	Writable Shares	**Key:**	
Hosts Scanned:	1	**Hosts Active:**	1
Scan Start:		**Scan End:**	
Comment:			

Sample #2 ISS scans finding of Lovgate infected PC

H **accountblankpw: User account has blank password (CAN-1999-0504)**

Additional Information *More Information*

An account has been detected with a blank password. Some vendors ship Windows NT pre-installed with a blank password on the Administrator or other user accounts. This misconfiguration is an extremely high risk vulnerability, and should be corrected immediately.

This vulnerability is typically detected on a computer where there is also no minimum password length required. If the Guest account has a blank password, it allows anyone to log in with any username and a blank password. If the file and registry permissions are not very tightly restricted, this situation can give any attacker the ability to access sensitive information and systems.

Remedy:

3.5 Recovery

During this phase, a two stage approach was taken, the first was to continue testing for and seeking signs of infection of the Worm followed by testing of business applications by the business owners and the IT operations group.

Monitoring and testing took a proximally twelve hours, which occurred after business hours to ensure that no further signs of the Worm was present. After that period if was agreed that no further signs were found. Also damaged appeared limited and no restores of data were needed. The IT Operations group gave the final approval for their resumption of normal day-to-day activities.

Senior management was briefed on the resolution of the situation and end users were sent a follow up e-mail regarding the situation along with basic e-mail security tips.

3.6 Lessons Learned

During a review of the events, which lead to the infestation of the Worm, it was identified that several key issues had surfaced. A great deal was learned about the internal weaknesses and lack of controls of both the IT infrastructure is policies and procedures. The following is a listing of lessons learned from this incident by this company.

- The need for a plan

The first and foremost lesson learned was the lack of a specific plan to deal with IT emergency's specifically ones that impact the business. During this scenario a Disaster recovery plan was modified to assist the team but it was realized that an overall plan as well as practices were needed to quickly address any problem, which effected or impacted the business. This also included establishing lines of communications - creating conference call in numbers, and producing and distributing printed copies of an emergency plan.

Another area found to be an issue during the incident was the lack of proper documentation from network topology maps to run books of applications. Had adequate information been available and at the disposal of the team it would have saved time in resolving the crisis.

- Policies, Procedures and Enforcement

Although there were some basic IT policies in the organization, they policies did not have the backing of the senior management. Rather, the existing polices were utilized as an attempt by the IT organization to gather some of basic controls over the environment. What were really needed were some corporate sponsored approved and communicated Information security

policies. Along with the need for better IT polices were guidelines and procedures for security, not to mention IT best practices.

The final step in this area to resolve a real need was to develop an enforcement mechanism and escalation path within the organization to identify security violations and enforce company policy.

- IT Security Training

Along with the need for better policies and procedures, there was the need to communicate those polices to in a clear and concise manner to end-users. A greater awareness of information security awareness was needed badly; many users were simply ignorant to many of today's Information Security concerns.

This was especially true for users who may be conditioned to open attachments from any sender despite multiple warnings from the Information technology department to beware of such tactics from hackers and virus writers.

- Standardization of PC's builds

It was identified that one of the areas, which allowed for the rapid spread of the Worm was the fact that many PC's had either no antiviral software or that it was not properly configured. Also many PC's had open shares with anonymous read and write capability.

In addition may end users PC had either no or weak local administrator passwords on the machines. In some cases many of the machines had the end user as in the local administrator group allowing the user to install any software he or she wanted.

- Improvements to Security Systems and Procedures

Many of the Networks Control and Detection devices were in place yet much of the IT staff had limited knowledge or hands on experience in using. The IDS for example was running but was not being administered, Firewall and server logs were being captured but no one ever reviewed the logs.

- E-mail polices and Security

It was identified that e-mail security was a major issue; there was no filtering for attachments of e-mail until the incident occurred. Also antiviral software for the e-mail servers was not well monitored.

The issue of not blocking certain attachments coming into the organizations network was based on an unsupported argument. This argument was that many groups in the company believed that it would hinder business needs. Rather than research this issue further Information technology had conceded to this issue and all attachments were allowed to pass

into the organizations e-mail system.

- Administrator privilege and responsibility

Poor choices by a staff member who had administrator rights were one of the causes of the Incident. A review of those who should have administrator rights and reasons for having administrator privileges was proposed.

This proposal included an inventory and quarterly review of all administrators and root privilege accounts to for all computing devices on the network. The review was to include a comparison of the inventory to a current payroll listing of all employees as well to ensure that only active employees had access and any terminated users were removed.

- Creation of segregated for test networks

Finally the initial entry point of the Worm was an ill protected software lab. This lab, which was really a collection of machines to test software and applications and had an unauthorized modem acted as a beachhead for the Worm.

A suggestion was made to management to create and allow for only approved test and lab environments. This would not only assist in protecting the network but was also beneficial in the Change Management area as well in establishing good development controls.

Conclusion

Many hard learned lessons were learned during this event. It should be noted that the root causes were identified after the event and shared with both IT and Senior Management during a debriefing and detailed report.

Unfortunately, progress remained slow to correct many of the issues which led to the attack, this was much to the dismay of the newly formed incident handling team.

References

---

[1] http://www.cert.org/advisories/CA-2003-08.html

[2] http://www.securityspace.com/smysecure/catid.html?id=2123&ctype=sid

[3] http://www.securityfocus.com/bid/7385/discussion/

[4] http://www.securityfocus.com/bid/7385/info/

[5] http://vil.nai.com/vil/content/v_100072.htm

[6] http://www.viruslist.com/eng/index.html?tnews=1001&id=59665

[7] http://www.iss.net

[8] http://www.pantek.com/library/general/lists/snort.org/snort-sigs/msg00427.html

[9] http://securityresponse.symantec.com/avcenter/venc/data/w32.hllw.lovgate.d@mm.html