Global Information Assurance Certification Paper

Incident Report for GCIH
Capitol SANS, Washington DC, December 2000
Anees Mirza
February 16, 2001

Option 1 – Illustrate an Incident

Executive Summary

Incident handling generally means a response by a person or an organization to a systems security incident, such as, an intrusion or a virus attack. An organized and careful reaction to an incident can mean the difference between complete recovery and total disaster.

The information in this paper documents an incident that occurred in our organization during the month of January 1999. Unfortunately, I was not a part of the incident handling team at the time, and will only have the information from the incident report and interviews to quote from. Details of the incident have been heavily sanitized in order to comply with our organization's policy, which dictates that incident details are for official use only, and not for public dissemination.

Our organization's security policy includes the use of firewalls and Intrusion Detection Sensors (IDS). This incident unfolded as one of our Information Assurance personnel, whom we will call 'Mr. R', made his routine check of security logs. He noticed a very large number of recorded connections. Further analysis revealed that one of our own organization's IP address, address number 255.255.255.128, made approximately 99,000 connections to IP address 212.39.65.211. The connecting IP address happened to belong to a website in Bulgaria. The connections were made using multiple protocols, and appeared to be a probe for services, on Bulgarian machine.

As the events unfolded, it turned out that one of our users, named "Tom", received an email message that claimed to be from Microsoft. The email reads, in part:

As an user of the Microsoft Internet Explorer, Microsoft Corporation provides you with this upgrade for your web browser. It will fix some bugs found in your Internet Explorer. To install the upgrade, please save the attached file (ie0199.exe) in some folder and run it.

The unsuspicious user, "Tom", followed the instructions and ran the attached file. The email message contained an attached Trojan horse executable called ie0199.exe. After installation, this program made several modifications to the system and attempted to contact other remote systems.

This particular version of the attached Trojan horse used the victim's machine to launch Denial of Service (DoS) attacks against an entire website in Bulgaria.

A team consisting of two system administrators, one network engineer, and two information assurance personnel, spent numerous hours to identify, contain, eradicate, and recover from the attack.

Six Stages of Incident Handling

Incident handling, as taught in SANS courses, consists of a series of six steps or stages. Some of these stages may occur in parallel. A short description of each step follows:

1. **Preparation:** Preparation is the means of prior planning on how to respond to incidents. It involves creation and dissemination of a security policy, proper allocation of personnel, tools, and other requirements for incident handling. Examples include: backup software, safe binaries, safe means of communication, etc.

2. **Identification:** Identification includes the detection of anomalies, their severity, and threat levels. It is the detection of disparities and unauthorized changes to systems and networks. The detection can arise from reviews of network traffic, system and IDS logs, and help desk logs. The determination of the severity of the incident arises from this detection and the following investigation. To identify an incident requires that the event is found to be abnormal or deviation from everyday patterns. Once the full extent of the incident is known, the appropriate parties should be notified. Notification is the process of communicating relevant information to personnel on a need to know basis.

3. **Containment:** Containment is the effort to minimize damage that could result from an incident. Containment often results in isolation of affected systems or services. It is very important to keep the system pristine and if applicable, make a backup before making any changes.

4. **Eradication:** Eradication is composed of steps taken to eliminate new vulnerabilities and to remove the attacker's presence from your network. During this stage of incident handling further steps should be taken to prevent new attempts.

5. **Recovery:** Recovery means taking the necessary steps to alleviate adverse affects of the incident, and resume the normal operation or state of the system. At this point, affected systems are rebuilt and good backups are restored to allow for

normal operation to continue. It is also recommended to continue monitoring the system for a period of time.

6. **Follow-up:** Follow-up requires documentation of findings. An analysis of lessons learned, and enactment of procedures that may improve the security posture of the organization and better handling of incidents in the future.

The next section will present in detail how these six stages were applied to the aforementioned incident, summarized in the executive summary section above.

PREPARATION

Comprehensively addressing the issue of security includes methods to prevent attacks as well as, how to respond to a successful one. In order to minimize the potential damage from an attack, some level of preparation is needed, which may include, but not limited to the following:

- Create a security policy and post warning banners
- Identify incident handling team members and organize a team
- Develop an emergency communications plan
- Conduct training for team members and keep them up-to-date
- Establish guidelines for interdepartmental cooperation
- Develop interfaces to law enforcement agencies and other computer incident response teams
- Back-up key data on a regular basis
- Keep software up-to-date and apply current patches
- Regularly monitor vendors' and security websites, along with mailing lists
- One key thing to remember is, know your systems i.e., know your system's/network's normal traffic patterns and behavior

In our organization most of these steps were implemented. "Tom's" computer had the following comprehensive warning banner:

This is a (organization's name) computer system. This computer system, including all related equipment, networks and network devices (specifically including internet access), are provided only for authorized company use. Computer systems may be monitored for all lawful purposes, including ensuring that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability and operational security. Monitoring includes active attacks by authorized entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed on or sent over this system may be monitored. Use of this computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution.

Evidence of unauthorized use collected during monitoring may be used for administrative, criminal or other adverse action. Use of this system constitutes consent to monitoring for these purposes.

Our organization has a systems security document, which is reviewed annually, and a computer use policy document, which every computer user signs as part of the process to obtain a network login account. Other policies require firewalls and intrusion detection systems to be in place, called for reporting of incidents to the information assurance office or to the help desk, and required local information systems security officers to have been appointed.

During my interview with the incident handler, "Mr. R", explained that he has a "jump kit" handy to deal with such situations. His kit includes a smart hub, cables, CD-ROM with trusted binaries, and also, static linked tools, a laptop, and a cell phone.

IDENTIFICATION

Identification is the first post-attack step of the incident handling process. It could become very complex, depending upon the sophistication of the attack.

Identification of this incident began when one morning "Mr. R" was scanning his firewall and IDS logs. He was alerted by a very large number of recorded connections. Further analysis revealed that IP address 255.255.255.128, in less than one day, had made approximately 99,000 connections to IP address 212.39.65.211, a website in Bulgaria. The first connection was recorded at 6:40 am and connections were made using multiple protocols and appeared to be a probe for services on Bulgarian machine.

The network system administrator of the particular machine, "Mr. G", was contacted to determine which user operates the machine in question, and why the connections were made. Meanwhile, an ISS scan of the system was conducted, which revealed that ports 135, 139, and 6050 were open and running. This was determined to be of no major vulnerability for this particular system. "Mr. G" reported that he inspected the machine and found no network scanning tools or any other suspicious software. He spoke with the user, who stated that the machine was on at the time of the incident, and he was doing a web search for a recipe. The user also stated that no new programs have been installed or removed from the machine. Further analysis of the IDS logs confirmed that the first syn packet was sent from 255.255.255.128. With that, "Mr. R" was convinced that the probe was initiated from within.

"Mr. R" started some sniffers on the DMZ to capture traffic from our host. He and his team then arrived at the location of the "infected" machine. His team looked thoroughly at the machine. It was running Windows NT 4.0 and appeared to be fully updated and patched according to the site's requirements. They examined all the services, applications, and start-up scripts and found nothing out of the ordinary. They killed several services and applications, and shut the system down a couple of times, to make

the changes made effective. They also went through much of the registry, looking for a sign of cause, but found nothing.

Further discussions with the user of the machine revealed that he received an email from Microsoft asking her to update her Internet Explorer web browser. He followed the instructions and ran the attached update file. The following message is the email that was still in his email inbox:

Date: xxx, xx Jan 1999 19:59:30 -0500 (EST)
From: Microsoft Internet Explorer Support <IEsupport@microsoft.com>
To: "Microsoft Internet Explorer User" <>
Subject: Please upgrade your Internet Explorer

Microsoft Corporation
1 Microsoft Way
Redmond, WA 98052
USA

Dear Sir/Madam

As an user of the Microsoft Internet Explorer, Microsoft Corporation provides you with this upgrade for your web browser. It will fix some bugs found in your Internet Explorer. To install the upgrade, please save the attached file (ie0199.exe) in some folder and run it.

For more information, please visit our web site at www.microsoft.com/ie/

(c) 1995-1998 Microsoft Corporation. All Rights Reserved

The attached program 'ie0199.exe', in fact turned out to be, a Trojan horse denial of service program. Running the Unix strings program to see embedded strings in he program image, you see the following message left by the attackers:

---------- F u C k B T C ----------
----
t0zI BaCi1 E RaZrAb0tEn sPeCiA1N0 zA BTC
(bY1GaRsKaTa tE1Ek0mUnIkAcI0NnA K0MpAnIa)
Za dA ZaDrYsTi i1i p0nE Da zAbAwI WrYzKaTa
nA NaCi0nA1NiQ TiRaNiN (BTC) KaT0 gI F100D_I

P0St0qNn0 S TCP C0NnEcTi0n rEqUeSt_i. T0Wa
nE E Pr0sT0 hAkErSkA AtAkA SrEsHtU BTC A
0tMyShTeNiE I WyZmEzDiE. nIe, SyZdAtE1ItE Na
t0zI BaCi1 PrEdPrIeMaMe t0zI NaChIn nA B0RbA
S NaCi0nA1NiQ PrEsTyPnIk BTC s cE1 dA Mu
nAp0mNiM, cHe aK0 tQ E CaR Na tE1Ef0nItE I
K0MuNiKaCiItE W Bu1gArIa, T0 nIe sMe cArEtE
Na mReVaTa. I P0NeVe BTC pR0Dy1vAwA Da nI
0bIrA S 0gR0MnItE Si tAkSi zA "uS1UgItE",
NiE ShTe sE B0RiM SrEsHtU NeQ P0 INTERNET.
k0gAt0 Tq pReD10vI Na bY1GaRsKiQ NaR0D
N0RmA1Ni uS10vIq zA K0MuNiKaCiQ Na n0rMa1nI
CeNi,NiE ShTe sPrEm aTaKaTa. W Pr0gRaMaTa e
zA10vEm i mEhAnIzYm zA SpIrAnE, k0jT0 0BaChE
SaM0 nIe m0vEm dA ZaDaIsTwAmE. nIk0j nE M0Ve
dA Ni sPrE, zAsHt0t0 SmE FaNt0mI. nIk0j nE
M0Ve dA Ni hWaNe k0i sMe, ZaHsT0T0 nIk0j nE
Ni p0zNaWa, ZaShT0T0 nIk0j nE Ni e wIvDa1,
zAsHt0t0 NiE SmE HaKeRi, By1gArSkI
DeStRuKtIwNi hAkErI! t0wA E SaM0 nAcHa10T0.
A Pr0dY1VeNiEt0 ShTe e mN0G0 p0_GeNiA1N0.
NiE SmE ZaShTiTnIcI Na nAr0dA. nIe sMe b0rCi
zA NaCi0nA1Na sV0B0Da. NiE SmE B0RcI Za
iNf0rMaCi0nNa sV0B0Da. WiE, dRaGa BTC sTe
pReStYpNiCiTe. N0 i wIe sHtE WiDiTe p0nE Za
mA1K0 kAkW0 zNaChI Da nQmAsH INTERNET.
(-: P0-zDrAwI :-)

----------f U c K B T C ----------

... which roughly translates into English as:

This virus is worked out especially for the BTC (Bulgarian Telecommunications Company) for its audacity or [unclear] its amusing attempt at national tyranny [unclear] constantly with a TCP connection request. This is not simply a hacker attack against BTC, but an act of revenge. We the creators of this virus are taking this step in the battle with the federal criminal BTC with the purpose of informing it that as BTC is the tsar of the telephone and communications in Bulgaria, we are not the tsars of [unclear]. And since BTC is

extending this and collecting enormous fees for its "service," we wish to fight against it on the Internet. [unclear]the Bulgarian people normal conditions for communication for normal prices, we wish to attack. In the program is placed a mechanism for [unclear]....and so we are the phantoms. Nobody can say [unclear] who we are, and because of this nobody will recognize us, nobody has seen us, so we are hackers, Bulgarian destructive hackers! This is in itself the beginning. And the continuation [unclear] ingenious. We are the people's defenders. We are the fighters for national freedom. We are the fighters for freedom of information. You, dear BTC, are criminals. But you shall see how little the Internet means in [unclear]. Greetings.

It took "Mr. R" and his team a few minutes before they realized Microsoft does not send updates through email attachments! He recalls that one MCSE in his team was upset that he did not get the update notice from Microsoft but an ordinary user did! At this point they realized that this in fact was a malicious logic spread via Trojan horse and not a hack incident.

The incident handling team made a copy of the attached file and installed it on an isolated test system. They were able to replicate the behavior of the infected machine. They observed that when the user runs the Trojan horse program, they see an error message that claims, "*A required DLL was not found*" and nothing appears to happen. The program, however, has installed itself to and modified the Windows Registry so it will be run each time the computer is restarted.

Because the program appears to fail to run, and because it causes no problems initially, most users will assume this is normal Windows' behavior and just forget about it. When they next restart the system and it actually starts the denial of service attack, enough time will normally have lapsed so they are unlikely to associate the problem with the failed IE "upgrade". They will not know about the problem until someone in BTC sends email to their network contacts reporting an ongoing DoS attack.

When the actual attack portion of the program is invoked at system startup, it begins to send SYN packets to randomly chosen IP addresses in the BTC network address block.

A Summary of How This Exploit Works:

When ie0199.exe executes, it deletes sndvol32.exe from the %SystemRoot%\System32 directory, installs %SystemRoot%\System\sndvol.exe, creates a registry key value HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Default with a value of %SystemRoot%\System\sndvol.exe. This key causes the execution of sndvol.exe file after logging into the system. Registry key

HKCU\Software\Microsoft\Windows\CurrentVersion\Internetsettings.enableautodial also gets modified.

To remove the malicious logic you must terminate the running sndvol.exe process, delete %SystemRoot%\System\sndvol.exe file, remove the registry key created (i.e., HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Default); and restore %SystemRoot%\System32\sndvol32.exe, and also undo the changes made to the key HKCU\Software\Microsoft\Windows\CurrentVersion\Internetsettings.enableautodial if you have a modem connected to your machine.

CONTAINMENT

At this point, the attack was identified and now additional steps were needed to minimize the effects of the attack. Containment, being the next step in incident handling process, allows you to protect other users and networks from being infected and limits the damage.

"Mr. R" explained his method for containment of a confirmed exploit on a computer system. First he pulls the network connection of the infected system to prevent further use of the exploited software. He captures an image of the hard drives and creates a tape of the image to use as evidence if necessary. He seals this tape in a box, and the out side of the box has his, along with his supervisor's signatures. This box is placed in a safe with limited access for network security personnel only having the combination. Then he uses the hub in the jump kit and a "fishbowl" system that has the same OS and on the same subnet as the infected system and adds the message of the day "motd" service to state that there are network problems and connectivity can be problematic. Then by monitoring this system he can see if the hacker is still scanning for vulnerable systems. This may or may not lead to further activity from the intruder. Prosecution is determined by the extent of the damage and length of time from exploit to identification to containment.

Since this particular case was identified not as break-in but Trojan horse sent via email, "Mr. R" says he proceeded differently. First, all firewall and IDS logs were re-monitored to watch for any other suspicious traffic, and all the traffic to and from the Bulgarian website was blocked. Then "Mr. R's" office issued a warning message for every user in the organization to stop them from falling a victim of the Trojan horses. They also put the filters in their mail servers for suspicious mail attachments. The system administrator made a back up of the machine and verified that it was a good backup.

ERADICATION

Eradication consists of steps taken to eliminate new vulnerabilities inserted as a result of an incident. The extent of eradication required depends on the level of access, if any, achieved.

Having successfully contained the incident and determining that the extent of the exploit was limited to this particular host, efforts were focused on removing all traces of the attack without unnecessarily destroying the user data. In this case however, "Mr. R" and his team, decided to scrub the system and reinstall from scratch.

RECOVERY

A complete system backup for the host was unfortunately, not available. The system administrator and the user, both agreed to reinstall the operating system and apply the necessary patches.

FOLLOW-UP and LESSONS LEARNED

One of the lessons learned from this incident is that email should not be trusted until such time as cryptographic mechanisms are standardized and implemented, such that you can be assured the message comes from the person claimed. Another lesson learned was that it is very important to teach computer users about social engineering, Trojan horse programs, and security problems associated with them. This incident also raised the awareness of Denial of Service attacks along with importance and benefits of Egress Filtering on your networks. To learn more about Egress Filtering please visit SANS web site at the following URL:
http://www.sans.org/y2k/egress.htm

One key thing to remember is, know your systems i.e., know your system's/network's normal traffic patterns and behavior.

This incident was prelude to many similar incidents to come, as evident by the following CERT advisory (what follows is an abbreviated version of the advisory, for full advisory please go to this URL : http://www.cert.org/advisories/CA-1999-02.html):

> *CERT® Advisory CA-1999-02 Trojan Horses*
> *Original issue date: February 5, 1999*
> *Last revised: March 8, 1999*
> *Minor typograhical corrections*
>
> *A complete revision history is at the end of this file.*
>
> *Systems Affected*

Any system can be affected by Trojan horses.

Overview

Over the past few weeks, we have received an increase in the number of incident reports related to Trojan horses. This advisory includes descriptions of some of those incidents (Section II), some general information about Trojan horses (Sections I and V), and advice for system and network administrators, end users, software developers, and distributors (Section III).

Few software developers and distributors provide a strong means of authentication for software products. We encourage all software developers and distributors to do so. This means that until strong authentication of software is widely available, the problem of Trojan horses will persist. In the meantime, users and administrators are strongly encouraged to be aware of the risks as described in this document.

I. Description

A Trojan horse is an "apparently useful program containing hidden functions that can exploit the privileges of the user [running the program], with a resulting security threat. A Trojan horse does things that the program user did not intend" [Summers].

Trojan horses rely on users to install them, or they can be installed by intruders who have gained unauthorized access by other means. Then, an intruder attempting to subvert a system using a Trojan horse relies on other users running the Trojan horse to be successful.

II. Recent Incidents

Incidents involving Trojan horses include the following:

False Upgrade to Internet Explorer

Recent reports indicate wide distribution of an email message which claims to be a free upgrade to the Microsoft Internet Explorer web browser. However, we have confirmed with Microsoft that they do not provide patches or upgrades via electronic mail, although they do distribute security bulletins by electronic mail.

The email message contains an attached executable program called

Ie0199.exe. After installation, this program makes several modifications to the system and attempts to contact other remote systems. We have received conflicting information regarding the modifications made by the Trojan horse, which could be explained by the existence of multiple versions of the Trojan horse.

At least one version of the Trojan horse is accompanied by a message which reads, in part:

> *As an user of the Microsoft Internet Explorer, Microsoft Corporation provides you with this upgrade for your web browser. It will fix some bugs found in your Internet Explorer. To install the upgrade, please save the attached file (ie0199.exe) in some folder and run it.*

The above message is not from Microsoft.

We encourage you to refer to the Microsoft Internet Explorer web site at the following location:

> *http://www.microsoft.com/windows/ie/security/default.asp*

Please refer to the Section III below for general solutions to Trojan horses.

> *http://www.cert.org/advisories/CA-90.11.Security.Probes.html*

III. Impact

Trojan horses can do anything that the user executing the program has the privileges to do. This includes

- *deleting files that the user can delete*
- *transmitting to the intruder any files that the user can read*
- *changing any files the user can modify*
- *installing other programs with the privileges of the user, such as programs that provide unauthorized network access*
- *executing privilege-elevation attacks; that is, the Trojan horse can attempt to exploit a vulnerability to increase the level of access beyond that of the user running the Trojan horse. If this is successful, the Trojan horse can operate with the increased privileges.*
- *installing viruses*

- *installing other Trojan horses*

If the user has administrative access to the operating system, the Trojan horse can do anything that an administrator can. The Unix 'root' account, the Microsoft Windows NT 'administrator' account, or any user on a single-user operating system has administrative access to the operating system. If you use one of these accounts, or a single-user operating system (e.g., Windows 95 or MacOS), keep in mind the potential for increased impact of a Trojan horse.

A compromise of any system on your network, including a compromise through Trojan horses, may have consequences for the other systems on your network. Particularly vulnerable are systems that transmit authentication material, such as passwords, over shared networks in cleartext or in a trivially encrypted form. This is very common. If a system on such a network is compromised via a Trojan horse (or another method), the intruder may be able to install a network sniffer and record usernames and passwords or other sensitive information as it traverses the network.

Additionally, a Trojan horse, depending on the actions it takes, may implicate your site as the source of an attack and may expose your organization to liability.

IV. How Trojan Horses Are Installed

Users can be tricked into installing Trojan horses by being enticed or frightened. For example, a Trojan horse might arrive in email described as a computer game. When the user receives the mail, they may be enticed by the description of the game to install it. Although it may in fact be a game, it may also be taking other action that is not readily apparent to the user, such as deleting files or mailing sensitive information to the attacker. As another example, an intruder may forge an advisory from a security organization, such as the CERT Coordination Center, that instructs system administrators to obtain and install a patch.

Other forms of "social engineering" can be used to trick users into installing or running Trojan horses. For example, an intruder might telephone a system administrator and pose as a legitimate user of the system who needs assistance of some kind. The system administrator might then be tricked into running a program of the intruder's design.

Software distribution sites can be compromised by intruders who replace legitimate versions of software with Trojan horse versions. If the distribution site is a central distribution site whose contents are mirrored by other distribution sites, the Trojan horse may be downloaded by many sites and

spread quickly throughout the Internet community.

Because the Domain Name System (DNS) does not provide strong authentication, users may be tricked into connecting to sites different than the ones they intend to connect to. This could be exploited by an intruder to cause users to download a Trojan horse, or to cause users to expose confidential information.

Intruders may install Trojan horse versions of system utilities after they have compromised a system. Often, collections of Trojan horses are distributed in toolkits that an intruder can use to compromise a system and conceal their activity after the compromise, e.g., a toolkit might include a Trojan horse version of ls which does not list files owned by the intruder. Once an intruder has gained administrative access to your systems, it is very difficult to establish trust in it again without rebuilding the system from known-good software. For information on recovering after a compromise, please see

http://www.cert.org/tech_tips/root_compromise.html

A Trojan horse may be inserted into a program by a compiler that is itself a Trojan horse. For more information about such an attack, see [Thompson].

Finally, a Trojan horse may simply be placed on a web site to which the intruder entices victims. The Trojan horse may be in the form of a Java applet, JavaScript, ActiveX control, or other form of executable content.

This document is available from: http://www.cert.org/advisories/CA-1999-02.html

---

CERT/CC Contact Information
Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:
CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.
CERT personnel answer the hotline 08:00-20:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

NO WARRANTY

To learn more about this exploit please visit the following URLs:

http://www.microsoft.com/windows/ie/security/default.asp
http://www.cert.org/advisories/CA-1999-02.html
http://www.ciac.org/ciac/notes/Notes99-01.shtml
http://www.prioritydata.ie/articles/bugwatch-apr99.htm

REFERENCES:

The CERT Coordination Center at http://www.cert.org

Computer Incident Advisory Capability at http://www.ciac.org

SANS Global Incident Analysis Center http://www.sans.org/y2k/egress.htm

SANS Computer and network hacker exploits: Step-by-Step, Part 1, Eric Cole, Book 4.2, GIAC GCIH Certification program.

SANS Hacker Exploits Workshop, Eric Cole, Book 4.4, Track 4, GIAC GCIH Certification program.