Software Engineering Institute
Carnegie Mellon University

2003 CERT Incident Notes

CERT Division

http://www.sei.cmu.edu

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

This report was prepared for the

SEI Administrative Agent
AFLCMC/AZS
5 Eglin Street
Hanscom AFB, MA 01731-2100

DM17-0052

Table of Contents

1 IN-2003-01: Malicious Code Propagation and Antivirus Software Updates

Release Date: July 2, 2003

Recent reports to the CERT/CC have highlighted two chronic problems:

- The speed at which viruses are spreading is increasing. This echoes the trend toward faster propagation rates seen in the past few years in self-propagating malicious code (i.e., worms). Beginning with the Code Red worm (CA-2001-19, CA-2001-23) in 2001 up through the Slammer worm (CA-2003-04) earlier this year, we have seen worm propagation times drop from hours to minutes.

  A similar trend from weeks to hours has emerged in the virus (i.e., non-self-propagating malicious code) arena. The effectiveness of antivirus software suffers as a result. Several recent malicious code incidents involving variants of W32/BugBear and W32/Sobig have achieved widespread propagation at rates significantly faster than many previous viruses. This increased speed is, unfortunately, also faster than many antivirus signatures can be identified and updated, regardless of the update method (including automated signature updates). The CERT/CC has received reports of successful W32/Sobig.E compromises from users whose signatures were up to date for the prior versions of W32/Sobig.

  Signature-based antivirus software is not the only type of antivirus software at risk: antivirus software that uses heuristics to determine malicious behavior may be circumvented by malicious code that employ new techniques. They should not be unconditionally trusted either, as they may not always block malicious code from executing. Additionally, we are aware of instances where corrupted antivirus software updates have caused the software to be disabled without the user's knowledge.

- In a number of the reports, users who were compromised may have been under the incorrect impression that merely having antivirus software installed was enough to protect them from **all** malicious code attacks. This is simply a mistaken assumption, and users must *always* exercise caution when handling email attachments or other code or data from untrustworthy sources.

In general, it is important to remember that while antivirus software vendors continue to improve the speed and reliability of their signature update mechanisms, there will always be some window of time when a system does not contain signatures to detect a particular worm or virus. Several recent research papers that have placed estimates on the magnitude of "worst-case scenario" malicious code propagation rates also illustrate the risk to systems during the window of time before signatures are available.[1][2]

Solutions

Apply "defense in-depth"

As mentioned above, it is not sufficient to rely solely on antivirus software for complete protection. Therefore, we recommend users apply a strategy of "defense in-depth" (where several layers of security or access controls are used) when considering ways to protect their computers from attackers. Although it may not be practical for all users, another way of achieving defense in-depth is to use diverse software and operating systems when possible. Some additional ways of improving security beyond the use of antivirus software follow.

In addition to following the steps outlined in this section, the CERT/CC encourages home users to review the "Home Network Security" and "Home Computer Security" documents.

Run and maintain an antivirus product

While an up-to-date antivirus software package cannot protect against all malicious code, for most users it remains the best first-line of defense against malicious code attacks.

Most antivirus software vendors release frequently updated information, tools, or virus databases to help detect and recover from malicious code, including W32/Bugbear.B and W32/Sobig.E. Therefore, it is important that users keep their antivirus software up to date. The CERT/CC maintains a partial list of antivirus vendors.

Many antivirus packages support automatic updates of virus definitions. The CERT/CC recommends using these automatic updates when available.

Do not run programs of unknown origin

Never download, install, or run a program unless you know it to be authored by a person or company that you trust. Email users should be wary of unexpected attachments, while users of Internet Relay Chat (IRC), Instant Messaging (IM), and file-sharing services should be particularly wary of following links or running software sent to them by other users, as these are commonly used methods among intruders attempting to build networks of distributed denial-of-service (DDoS) agents.

Disable or secure file shares

Best practice dictates a policy of least privilege. For example, if a Windows computer is not intended to be a server (i.e., share files or printers with others), "File and Printer Sharing for Microsoft Networks" should be disabled.

For computers that export shares, ensure that user authentication is required and that each account has a well-chosen password. Furthermore, consider using a firewall to control which computer can access these shares.

By default, Windows NT, 2000, and XP create certain hidden and administrative shares. See the HOW TO: Create and Delete Hidden or Administrative Shares on Client Computers for further guidelines on managing these shares.

Deploy a firewall

The CERT/CC also recommends using a firewall product, such as a network appliance or a personal firewall software package. In some situations, these products may be able to alert users to the fact that their machine has been compromised. Furthermore, they have the ability to block intruders from accessing backdoors over the network. However, no firewall can detect or stop all attacks, so it is important to continue to follow safe computing practices.

Recovering from a system compromise

If you believe a system under your administrative control has been compromised, please follow the steps outlined in Steps for Recovering from a UNIX or NT System Compromise.

References

1. Paxson, V., Staniford, S., Weaver, N. "How to 0wn the Internet in Your Spare Time" http://www.icir.org/vern/papers/cdc-usenix-sec02/index.html

2. Moore, D., Paxson, V., Savage, S., Shannon, S., Staniford, S., Weaver, N. "The Spread of the Sapphire/Slammer Worm" http://www.cs.berkeley.edu/~nweaver/sapphire/

Authors: Chad Dougherty and Allen Householder

This document is available from: http://www.cert.org/incident_notes/IN-2003-01.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/CC personnel answer the hotline 08:00-17:00 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.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from http://www.cert.org/CERT_PGP.key.

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our website: http://www.cert.org/.

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

---

2 IN-2003-02: W32/Mimail Virus

The CERT Coordination Center publishes incident notes to provide information about incidents to the Internet community. Release Date: August 2, 2003

Overview

On Friday, August 1st 2003 the CERT Coordination Center began to receive an increased number of reports of a new mass mailing virus, now referred to as W32/Mimail, spreading on the Internet.

Description

The W32/Mimail virus is a malicious file attachment containing a specially crafted MHTML file named 'message.html'. This file is delivered inside of a .ZIP archive file named 'message.zip'. Viewing the 'message.html' file on a vulnerable system will cause the malicious code to be installed and executed. The malicious code is a mass-mailer.

The email message may look like the following:

```
From: admin@<your domain>

Subject: <your account>             [random text]

Hello there,

I would like to inform you about important information regarding
your email address.  This email address will be expiring.

Please read attachment for details

---

Best regards,   Administrator

[random text]
```

The malicious code is installed and runs as %windowsroot%\videodrv.exe. The recipients are determined by scanning files in C:\Documents and Settings\{current_user}\ , C:\Program Files\ and C:\%windowsroot%\Fonts\ for the pattern %s@%s and it stores this information in %windowsroot%\eml.tmp.

Anti-virus vendors have developed signatures for W32/Mimail which can be found at:

> http://www.sarc.com/avcenter/venc/data/w32.mimail.a@mm.html
>
> http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_MIMAIL.A

http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=100523

The vulnerability which makes it possible for W32/Mimail to execute automatically once the .ZIP archive is opened is described in Vulnerability Note VU#208052 and Microsoft Security Bulletin MS03-014.

According to Microsoft security bulletin MS03-014:

MHTML is a standard for exchanging HTML content in e-mail, and, as a result, the MHTML URL Handler function has been implemented in Outlook Express. Internet Explorer can also render MHTML content. However, the MHTML function has not been implemented separately in Internet Explorer - it uses Outlook Express to render the MHTML content.

Thus, the MHTML format file 'message.html' file is exploiting a vulnerability in Outlook Express, but it poses a threat to any application that uses Internet Explorer (and thus Outlook Express) to render its contents.

Solutions

Apply the patch from Microsoft

The CERT/CC encourages sites to review Microsoft Security Bulletin MS03-014 and apply the Cumulative Patch for Outlook Express (330994).

Run and maintain an anti-virus product

While an up-to-date antivirus software package cannot protect against all malicious code, for most users it remains the best first-line of defense against malicious code attacks. Users may wish to read Incident Note IN-2003-01 for more information on anti-virus software and security issues.

Most antivirus software vendors release frequently updated information, tools, or virus databases to help detect and recover from malicious code, including W32/Mimail. Therefore, it is important that users keep their antivirus software up to date. The CERT/CC maintains a partial list of antivirus vendors.

Many antivirus packages support automatic updates of virus definitions. The CERT/CC recommends using these automatic updates when available.

Do not run programs or open files of unknown origin

Email users should be wary of unexpected attachments or unusual links contained in email. Never download, install, run or open a program or file unless you know it to be authored by a person or company that you trust.

Filter the email

Sites can use email filtering techniques to delete messages known to contain this malicious code, or they can filter all attachments.

Author(s): Brian B. King, Kevin Houle

This document is available from: http://www.cert.org/incident_notes/IN-2003-02.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/CC personnel answer the hotline 08:00-17:00 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.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from http://www.cert.org/CERT_PGP.key.

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our website: http://www.cert.org/.

Conditions for use, disclaimers, and sponsorship information

Revision History

August 2, 2003: Initial Release

August 4, 2003: Corrected Microsoft patch number in Solutions section

3 IN-2003-03: W32/Sobig.F Worm

Release Date: August 22, 2003

Overview

The CERT/CC has been receiving a large volume of reports of a mass mailing worm, referred to as W32/Sobig.F, spreading on the Internet. New information indicates that this worm has additional capabilities that were not realized at the time it first began propagating.

Description

The W32/Sobig.F worm is an email-borne malicious program with a specially crafted attachment that has a .pif extension. The email messages may appear from random addresses and have a Subject: line such as

- Re: Thank You!
- Thank You!
- Your details
- Re: Details
- Re: Re: My details
- Re: Approved
- Re: Your application
- Re: Wicked screensaver
- Re: That movie

The following attachment names have been observed in email messages carrying the worm:

- your_document.pif
- document_all.pif
- thank_you.pif
- your_details.pif
- details.pif
- document_9446.pif
- application.pif
- wicked_scr.scr
- movie0045.pif

The worm requires a user to execute the malicious attachment either manually or by using an email client that will open the attachment automatically. Upon successful execution, the worm installs itself as `C:\%windir%\winppr.exe` and also creates the file `C:\%windir%\winstt32.dat`. An entry is also added to the Run registry key so that this executable will be run upon system restart. The key installed in HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run is ScanX with the value "`c:\winnt\winppr.exe /sinc`". The program then proceeds to scan files

with certain extensions (htm, html, dbx, hlp, mht, txt, wab) on the compromised system for valid email addresses, and it uses an internal SMTP engine to email itself to those addresses.

The worm uses the Network Time Protocol (NTP) to determine the current time. The worm also includes code that attempts to contact a list of 20 predefined IP addresses on port 8998/UDP on Fridays and Sundays between 1900 and 2200 UTC (starting at 1900 UTC on August 22, 2003). Is it believed that a location from which additional code can be downloaded is sent over this channel. The list of IP addresses appears as follows:

- 12.158.102.205
- 12.232.104.221
- 218.147.164.29
- 24.197.143.132
- 24.202.91.43
- 24.206.75.137
- 24.210.182.156
- 24.33.66.38
- 61.38.187.59
- 63.250.82.87
- 65.177.240.194
- 65.92.186.145
- 65.92.80.218
- 65.93.81.59
- 65.95.193.138
- 66.131.207.81
- 67.73.21.6
- 67.9.241.67
- 68.38.159.161
- 68.50.208.96

The worm is believed to have a programmed "shut down" date of September 10, 2003, at which time it is expected to stop propagating.

Anti-virus vendors have developed signatures for W32/Sobig.F:

http://securityresponse.symantec.com/avcenter/venc/data/w32.sobig.f@mm.html

http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_SOBIG.F

http://us.mcafee.com/virusInfo/default.asp?id=helpCenter&hcName=sobig

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

http://www.sophos.com/virusinfo/analyses/w32sobigf.html

Solutions

In addition to following the steps outlined in this section, the CERT/CC encourages home users to review the "Home Network Security" and "Home Computer Security" documents.

Run and maintain an anti-virus product

While an up-to-date antivirus software package cannot protect against all malicious code, for most users it remains the best first-line of defense against malicious code attacks. Users may wish to read IN-2003-01 for more information on anti-virus software and security issues.

Most antivirus software vendors release frequently updated information, tools, or virus databases to help detect and recover from malicious code, including W32/Sogib.F. Therefore, it is important that users keep their antivirus software up to date. The CERT/CC maintains a partial list of antivirus vendors.

Many antivirus packages support automatic updates of virus definitions. The CERT/CC recommends using these automatic updates when available.

Do not run programs of unknown origin

Never download, install, or run a program unless you know it to be authored by a person or company that you trust. Email users should be wary of unexpected attachments, while users of Internet Relay Chat (IRC), Instant Messaging (IM), and file-sharing services should be particularly wary of following links or running software sent to them by other users since these are commonly used methods among intruders attempting to build networks of distributed denial-of-service (DDoS) agents.

Filter network traffic

Sites are encouraged to block network access to the following relevant ports at network borders. This can minimize the potential of denial-of-service attacks originating from outside the perimeter. The specific services that should be blocked include

- 123/UDP
- 995/UDP
- 996/UDP
- 997/UDP
- 998/UDP
- 999/UDP
- 8998/UDP

Sites should consider blocking both inbound *and* outbound traffic to these ports, depending on network requirements, at the host and network level.

If access cannot be blocked for all external hosts, the CERT/CC recommends limiting access to only those hosts that require it for normal operation. As a general rule, the CERT/CC recommends filtering **all** types of network traffic that are not required for normal operation.

Recovering from a system compromise

If you believe a system under your administrative control has been compromised, please follow the steps outlined in Steps for Recovering from a UNIX or NT System Compromise.

Reporting

The CERT/CC is tracking activity related to this worm as CERT#30979. Relevant artifacts or activity can be sent to cert@cert.org with the appropriate CERT# in the subject line.

Authors: Chad Dougherty and Brian King

This document is available from: http://www.cert.org/incident_notes/IN-2003-03.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/CC personnel answer the hotline 08:00-17:00 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.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from http://www.cert.org/CERT_PGP.key.

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our website: http://www.cert.org/.

To subscribe to the CERT mailing list for advisories and bulletins, send email to majordomo@cert.org. Please include in the body of your message

```
subscribe cert-advisory
```

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

Revision History

August 22, 2003: Initial Release

4 IN-2003-04: Exploitation of Internet Explorer Vulnerability

Original release Date: October 1, 2003
Last revised: October 4, 2003

Overview

The CERT/CC has received reports indicating that attackers are actively exploiting the Microsoft Internet Explorer vulnerability described in VU#865940.

Description

Reports to the CERT/CC indicate that attackers are leveraging the vulnerability described in VU#865940 to cause victim systems to perform various tasks. These attacks include the installation of tools for launching distributed denial-of-service (DDoS) attacks, reading sensitve information from the Windows registry, and the use of the victim system's modem to dial pay-per-minute services thereby incurring significant expense to users. Another attack known as "QHosts" misdirects network traffic by modifying Domain Name System (DNS) settings. By convincing a user running a vulnerable version of Microsoft Internet Explorer (IE) to view an HTML document (e.g., a web page or HTML email), a remote attacker could execute arbitrary code with the privileges of the user.

The vulnerability described in VU#865940 exists due to an interaction between IE's MIME type processing and the way it handles HTML application (HTA) files embedded in OBJECT tags. When an HTA file is referenced by the DATA attribute of an OBJECT element, and the web server returns the Content-Type header set to `application/hta`, IE may execute the HTA file directly, without user intervention. The HTML used to reference the HTA file can be created in at least three ways:

1. The HTML can be static
2. The HTML can be generated by script
3. The HTML can be generated by Data Binding an XML source to an HTML consumer

The extension of the HTA file does not affect this behavior, for example `<OBJECT DATA="somefile.jpg">` (where somefile.jpg is a text file containing HTML code). IE security zone settings for ActiveX controls may prevent an HTA from being executed in this manner.

Additional details on VU#865940 can be found in the Vulnerability Note.

Any program that uses the WebBrowser ActiveX control or the IE HTML rendering engine (MSHTML) may be affected by this vulnerability. Outlook and Outlook Express are affected, however recent versions of these programs open mail in the Restricted sites zone where ActiveX controls and plug-ins are disabled by default.

Although Microsoft released a cumulative patch for Internet Explorer (see MS03-032) that stops HTAs from executing in one case in which static HTML is used to create an OBJECT element

referencing the HTA, the patch did **not** prevent HTAs from executing in the cases when the requisite HTML is generated by script or by Data Binding. We have confirmed reports of attackers exploiting the Data Binding method. Microsoft has subsequently released security bulletin MS03-040 which supercedes MS03-032 and references a patch (828750) that purportedly fixes the cases where the HTML is generated by script or Data Binding.

Solutions

The CERT/CC is unaware of a complete solution for this vulnerability.

Apply patch

The cumulative patch (822925) referenced in Microsoft Security Bulletin MS03-032 (released on 2003-08-20) stops HTAs from executing in one case in which static HTML is used to create an OBJECT element referencing the HTA (1). The patch does **not** prevent HTAs from executing in at least two other cases in which the requisite HTML is generated by script (2) or by Data Binding (3). Microsoft has since released a new cumulative patch (828750), referenced in Microsoft Security Bulletin MS03-040 that fixes the latter cases. The CERT/CC recommends that users and administrators apply the patches from MS03-040 and consider taking the additional steps outlined below.

Additional steps for users

Disable ActiveX controls and plug-ins

It appears that disabling the "Run ActiveX controls and plug-ins" setting will prevent OBJECT elements from being instantiated, thus preventing exploitation of this vulnerability. Disable "Run ActiveX controls and plug-ins" in the Internet zone and any zone used to read HTML email. Note that there may be other attack vectors that are not governed by the "Run ActiveX controls and plug-ins" setting.

Apply the Outlook Email Security Update

Another way to effectively disable ActiveX controls and plug-ins in Outlook is to install the Outlook Email Security Update. The update configures Outlook to open email messages in the Restricted Sites Zone, where Active scripting is disabled by default. In addition, the update provides further protection against malicious code that attempts to propagate via Outlook. The Outlook Email Security Update is available for Outlook 98 and Outlook 2000. The functionality of the Outlook Email Security Update is included in Outlook 2002 and Outlook Express 6.

Maintain updated antivirus software

Antivirus software with updated virus definitions may identify and prevent some exploit attempts. Variations of exploits or attack vectors may not be detected. Do not rely on antivirus software to defend against this vulnerability. The CERT/CC maintains a partial list of antivirus vendors.

Additional steps for system administrators

The following steps are recommended for system administrators and advanced users.

Unmap HTA MIME type

Deleting or renaming the following registry key prevents HTAs from executing in the three cases listed above:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\MIME\Database\Content Type\application/hta
```

Note that there may be other attack vectors that do not rely on this MIME setting.

Block Content-Type headers

Use an application layer firewall, HTTP proxy, or similar technology to block or modify HTTP Content-Type headers with the value "application/hta". This technique may not work for encrypted HTTP connections and it may break applications that require the "application/hta" Content-Type header.

Block mshta.exe

Use a host-based firewall to deny network access to the HTA host: %SystemRoot%\system32\mshta.exe. Examining network traces of known attack vectors, it seems that the exploit HTML/HTA code is accessed three times, twice by IE and once by mshta.exe. The HTA is instantiated at some point before the third access attempt. Blocking mshta.exe prevents the third access attempt, which appears prevent the exploit code from being loaded into the HTA. There may be other attack vectors that circumvent this workaround. For example, a vulnerability that allowed data in the browser cache to be loaded into the HTA could remove the need for mshta.exe to access the network. This technique may break applications that require HTAs to access the network. Also, specific host-based firewalls may or may not properly block mshta.exe from accessing the network.

Recovering from a system compromise

If you believe a system under your administrative control has been compromised, please follow the Steps for Recovering from a UNIX or NT System Compromise.

Reporting

The CERT/CC is tracking activity related to this vulnerability as CERT#35432. Relevant artifacts or reports can be sent to cert@cert.org with the appropriate CERT# in the subject line.

Authors: Allen Householder, Art Manion, and Chad Dougherty

This document is available from: http://www.cert.org/incident_notes/IN-2003-04.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/CC personnel answer the hotline 08:00-17:00 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.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from http://www.cert.org/CERT_PGP.key.

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our website: http://www.cert.org/.

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

Revision History

October 1, 2003: Initial release

October 4, 2003: Added information pertaining to MS03-040, noted registry and QHosts attacks