Software Engineering Institute
Carnegie Mellon University

2004 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.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

This report was prepared for the

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

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

DM17-0052

Table of Contents

1 IN-2004-01: W32/Novarg.A Virus

Release Date: January 27, 2004
Last Updated: January 30, 2004

Overview

The CERT/CC has been receiving reports of a new mass-mailing virus known as W32/Novarg.A, W32/Shimg, or W32/Mydoom that has been reported to open a backdoor to the compromised system and possibly launch a denial-of-service attack at a fixed time in the future.

Description

The W32/Novarg.A virus attempts to do the following:

- Modify various Windows registry values so that the virus is run again upon reboot
- Open a listening TCP port in the range of 3127-3198, suggesting remote access capabilities
- Install a copy of itself in the `C:\Program Files\KaZaA\My Shared Folder\` folder, which will be available for download by KaZaA users

The virus arrives as an email message with a 22,528-byte attachment that has a random filename with a file extension of `.cmd`, `.pif`, `.scr`, `.exe`, or `.bat`. The attachment may also arrive as a ZIP archive.

Some messages containing the virus have had the following characteristics:

```
Subject: <random>
From: <spoofed>
To: <email address>

Body: (The body has been reported to contain one of the following
three messages.)

"The message cannot be represented in 7-bit ASCII encoding and has
been sent as a binary attachment."

"The message contains Unicode characters and has been sent as a bi-
nary attachment."

"Mail transaction failed. Partial message is available."
```

In addition to the backdoor capabilities, the virus is also believed to have the capability to launch a distributed denial-of-service attack against a specific web site beginning on February 1, 2004. As with other malicious code having mass-mailing capabilities, W32/Novarg.A may cause "collateral" denial-of-service conditions in networks where either (a) multiple systems are infected, or (b) large volumes of infected mail are received.

The CERT/CC is continuing to analyze the malicious code and we will update this Incident Note as more information is confirmed.

Anti-virus vendors have developed signatures for W32/Novarg.A:

http://www.sarc.com/avcenter/venc/data/w32.novarg.a@mm.html

http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_MIMAIL.R

http://us.mcafee.com/virusInfo/default.asp?id=mydoom

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

http://www.sophos.com/virusinfo/analyses/w32mydooma.html

http://www3.ca.com/virusinfo/virus.aspx?ID=38102

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/Novarg.A. 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

Reports to CERT/CC indicate that the virus opens a listening TCP port in the range of 3127-3198. 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 virus as CERT#25304. Relevant artifacts or activity can be sent to cert@cert.org with the appropriate CERT# in the subject line.

Authors: Marty Lindner, Damon Morda, and Chad Dougherty

This document is available from: http://www.cert.org/incident_notes/IN-2004-01.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.

NO WARRANTY
Any material furnished by Carnegie Mellon University and the Software Engineering Institute is furnished on an "as is" basis. Carnegie Mellon University makes no warranties of any kind, either expressed or implied as to any matter including, but not limited to, warranty of fitness for a particular purpose or merchantability, exclusivity or results obtained from use of the material. Carnegie Mellon University does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

Conditions for use, disclaimers, and sponsorship information

Revision History

January 27, 2004: Initial Release

January 30, 2004: Changed worm references

2 IN-2004-02: W32/Netsky.B Virus

Release Date: February 18, 2004
Last Updated: --

Overview

The CERT/CC has been receiving reports of a new mass-mailing virus known as W32/Netsky.B.

Description

The W32/Netsky.B virus propagates either as an attachment to an email message or by automatically copying itself to Windows network shares. Upon successful execution, the virus attempts to

- modify various Windows registry values so that the virus is run again upon reboot.
- install a copy of itself in the `%Windir%\services.exe`, where `%Windir%` is a variable pointing to the root of the Windows directory on the host.
- collect target email addresses from files with specific extensions on the local system.
- copy itself to particularly-named files within non-CDROM local drives or mapped network shares.
- remove registry keys that were added as a likely result of successful compromise via other recent malicious code, including W32/Novarg.A and W32/MyDoom.B.

When spreading via email, the virus arrives as an email message with a 22,016-byte attachment that has a filename selected randomly from a fixed list and a double-extension of one of the following combinations:

- `.txt`
- `.rtf`
- `.doc`
- `.htm`

and

- `.com`
- `.pif`
- `.scr`
- `.exe`

The attachment may also arrive as a ZIP (`.zip`) archive.

Some messages containing the virus have had the following characteristics:

`Subject:` `(one of the following)`

- `stolen`
- `fake`

- `unknown`
- `something for you`
- `read it immediately`
- `warning`
- `information`

From: `<spoofed>`
To: `<email address>`

Body:
`(The body has been reported to contain a short message selected randomly from a fixed list.)`

When spreading via the filesystem, the virus searches non-CDROM drives C: through Z:, including mapped network shares, for any folders containing "Share" or "Sharing" in their name. The virus then copies itself into these folders as a filename selected randomly from a fixed list and containing a double-extension.

As with other malicious code having mass-mailing capabilities, W32/Netsky.B may cause "collateral" denial-of-service conditions in networks where either (a) multiple systems are infected, or (b) large volumes of infected mail are received.

The CERT/CC is continuing to analyze the malicious code and we will update this Incident Note as more information is confirmed.

Anti-virus vendors have developed signatures for and information about W32/Netsky.B:

> http://www.sarc.com/avcenter/venc/data/w32.netsky.b@mm.html
>
> http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_NETSKY.B
>
> http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=101034
>
> http://www.f-secure.com/v-descs/netsky_b.shtml
>
> http://www.sophos.com/virusinfo/analyses/w32netskyb.html
>
> http://www3.ca.com/virusinfo/virus.aspx?ID=38332

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/Netsky.B. 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.

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 virus as CERT#23032. Relevant artifacts or activity can be sent to cert@cert.org with the appropriate CERT# in the subject line.

Authors: Chad Dougherty

This document is available from: http://www.cert.org/incident_notes/IN-2004-02.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/.

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

NO WARRANTY
Any material furnished by Carnegie Mellon University and the Software Engineering Institute is furnished on an "as is" basis. Carnegie Mellon University makes no warranties of any kind, either expressed or implied as to any matter including, but not limited to, warranty of fitness for a particular purpose or merchantability, exclusivity or results obtained from use of the material. Carnegie Mellon University does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

Conditions for use, disclaimers, and sponsorship information

Revision History

February 18, 2004: Initial Release

February 18. 2004: Clarify information about filesystem propagation