Software Engineering Institute
Carnegie Mellon University

2002 CERT Incident Notes

CERT Division

http://www.sei.cmu.edu

REV-03.18.2016.0

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-2002-01: W32/Myparty Malicious Code

The CERT Coordination Center publishes incident notes to provide information about incidents to the Internet community. Release Date: January 28, 2002

A complete revision history can be found at the end of this file.

Systems Affected

Systems running Microsoft Windows

Overview

"W32/Myparty" is malicious code written for the Windows platform that spreads as an email file attachment. The malicious code makes use of social engineering to entice a user to execute it. The W32/Myparty payload is non-destructive.

As of 16:00 EST (UTC-0500) January 28, 2002 the CERT/CC has received reports of W32/Myparty from several dozen individual sites.

I. Description

Analysis of the W32/Myparty malicious code indicates that it is a Windows binary spreading via an email message with the following characteristics:

SUBJECT: `new photos from my party!`

BODY:

```
Hello!

My party... It was absolutely amazing!
I have attached my web page with new photos!
If you can please make color prints of my photos. Thanks!
```

ATTACHMENT: `www.myparty.yahoo.com`

The attached file name containing the malicious code, `www.myparty.yahoo.com`, was carefully chosen to entice the email recipient to open and (in most email clients) run the attachment. This social engineering exploits the fact that `.com` is both an executable file extension in Windows and a top-level domain (TLD).

We have seen two variants of `www.myparty.yahoo.com` as follows:

Filename = `www.myparty.yahoo.com`
MD5 checksum = `43fc3f274372f548b7e6c14af45e0746`
File size = `30172`

Filename = `www.myparty.yahoo.com`
MD5 checksum = `221c47432e70b049fce07a6ca85ca7dd`
File size = `29701`

Both files take the same actions when executed:

- the file `msstask.exe` is created in the current user's profile `Startup` folder (`\Start Menu\Programs\Startup`) and is immediately executed. It will also be executed every time the Windows user logs into the system.

  Filename = `msstask.exe`
  MD5 checksum = `cda312b5364bbaddcd2c2bf3ceb4e6cd`
  File size = `6144`

- on Windows 9x computers, a copy of `www.myparty.yahoo.com` is written to `C:\Recycled\REGCTRL.EXE`. On Windows NT computers, this copy is placed in either `C:\REGCTRL.EXE` or a newly created random directory in the `C:\Recycled` folder. This copy is subsequently executed.
- an email message is sent to a predefined address with a subject line of the folder where the W32/Myparty malicious code was stored on the victim machine. When sending this message, W32/Myparty will use the SMTP statement `HELO HOST` when identifying itself to the SMTP server.
- the current user's default SMTP server is retrieved from the following registry key:

  `HKEY_CURRENT_USER\Software\Microsoft\Internet Account Manager\Accounts\00000001`

- the hard drive is scanned for Windows Address Book (.WAB) files and Outlook Express inboxes and folders (.DBX) in order to harvest email addresses.
- copies of the malicious code are emailed to all the email addresses it could find.

Outside analysis indicates that this final step of mass mailing may be time-dependant. The code may only send itself if the clock on the victim machine is set to January 25-29. It is the experience of the CERT/CC that variants of malicious code often occur, so this time-trigger may not apply.

Other outside analysis also indicates that the default web browser may be launched to a particular URL under certain circumstances.

II. Impact

W32/Myparty may cause the default web browser to run unexpectedly. Likewise, the victim and targeted sites may experience an increased load on the mail server when the malicious code is propagating.

III. Solution

Run and maintain an anti-virus product

It is important for users to update their anti-virus software. Most anti-virus software vendors have released updated information, tools, or virus databases to help detect and recover from W32/Myparty. A list of vendor-specific anti-virus information can be found in Appendix A.

Many anti-virus packages support automatic updates of virus definitions. We recommend using these automatic updates when available.

Exercise caution when opening attachments

Exercise caution when receiving email with attachments. Users should be suspicious of unexpected attachments regardless of their origin. In general, users should also always scan files received through email with an anti-virus product.

The following section of the "Home Network Security" document provides advice on handling email attachments securely: http://www.cert.org/tech_tips/home_networks.html#IV-A-4.

Filter the email or use a firewall

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

Appendix A. Vendor Information

Aladdin Knowledge Systems

http://www.esafe.com/home/csrt/valerts2.asp?virus_no=10102

Central Command, Inc.

http://support.centralcommand.com/cgi-bin/command.cfg/php/enduser/std_adp.php?p_refno=020128-000003

Command Software Systems

http://www.commandsoftware.com/virus/myparty.html

Computer Associates

http://www3.ca.com/solutions/collateral.asp?CT=65&ID=1323

F-Secure Corp

http://www.datafellows.com/v-descs/myparty.shtml

Frisk Software International

http://www.f-prot.com/f-prot/virusinfo/mypartya.html

McAfee

http://vil.mcafee.com/dispVirus.asp?virus_k=99332&

Norman Data Defense Systems

http://www.norman.com/virus_info/w32_myparty_a_mm.shtml

Panda Software

http://service.pandasoftware.es/servlet/panda.pandaInternet.EntradaDatosInternet?opera-cion=EV2FichaVirus&pestanaFicha=0&idioma=1&nombreVirusFicha=W32/Myparty@MM

Proland Software

http://www.pspl.com/virus_info/worms/myparty.htm

Sophos

http://www.sophos.com/virusinfo/analyses/w32mypartya.html

Symantec

http://securityresponse.symantec.com/avcenter/venc/data/pf/w32.myparty@mm.html

Trend Micro

http://www.antivirus.com/vinfo/virusencyclo/default5.asp?VName=WORM_MYPARTY.A

You may wish to visit the CERT/CC's Computer Virus Resources Page located at:
http://www.cert.org/other_sources/viruses.html

Authors: Roman Danyliw, Allen Householder

Revision History

Jan 28, 2002: Initial release

Jan 29, 2002: Modified feedback link

Feb 28, 2002: Added vendor link for Frisk Software International

2 IN-2002-02: W32/Gibe Malicious Code

The CERT Coordination Center publishes incident notes to provide information about incidents to the Internet community. Release Date: March 12, 2002
Last Updated: March 13, 2002

A complete revision history can be found at the end of this file.

Systems Affected Systems running Microsoft Windows

Overview

The CERT/CC has received numerous reports of a piece of malicious code, written for the Windows platform, commonly known as W32/Gibe. W32/Gibe spreads via email disguised as a Microsoft security bulletin and patch. A user must execute the attached file in order to be infected. The payload is non-destructive, but a backdoor is installed that may allow an intruder access to the system.

I. Description

W32/Gibe is a Windows binary executable written in Visual Basic that is spreading via email. The email appears to be from Microsoft; however, Microsoft does not distribute patches via email. The Microsoft software distribution policy can be viewed at http://www.microsoft.com/technet/security/policy/swdist.asp

The email appears as the following:

```
From: Microsoft Corporation Security Center <rdquest12@microsoft.com>
To: Microsoft Customer <'customer@yourdomain.com'>
Subject: Internet Security Update
Attachment: q216309.exe
```

Microsoft Customer,

> this is the latest version of security update, the "7 Mar 2002 Cumulative Patch" update which eliminates all known security vulnerabilities affecting Internet Explorer and MS Outlook/Express as well as six new vulnerabilities, and is discussed in Microsoft Security Bulletin MS02-005. Install now to protect your computer from these vulnerabilities, the most serious of which could allow an attacker to run code on your computer.
>
> Description of several well-know vulnerabilities:
>
> - "Incorrect MIME Header Can Cause IE to Execute E-mail Attachment" vulnerability. If a malicious user sends an affected HTML e-mail or hosts an affected e-mail on a Web

site, and a user opens the e-mail or visits the Web site, Internet Explorer automatically runs the executable on the user's computer.

- A vulnerability that could allow an unauthorized user to learn the location of cached content on your computer. This could enable the unauthorized user to launch compiled HTML Help (.chm) files that contain shortcuts to executables, thereby enabling the unauthorized user to run the executables on your computer.

- A new variant of the "Frame Domain Verification" vulnerability could enable a malicious Web site operator to open two browser windows, one in the Web site's domain and the other on your local file system, and to pass information from your computer to the Web site.

- CLSID extension vulnerability. Attachments which end with a CLSID file extension do not show the actual full extension of the file when saved and viewed with Windows Explorer. This allows dangerous file types to look as though they are simple, harmless files - such as JPG or WAV files - that do not need to be blocked.

System requirements:
Versions of Windows no earlier than Windows 95.

This update applies to:
Versions of Internet Explorer no earlier than 4.01
Versions of MS Outlook no earlier than 8.00
Versions of MS Outlook Express no earlier than 4.01

How to install
Run attached file q216309.exe

How to use
You don't need to do anything after installing this item.

For more information about these issues, read Microsoft Security Bulletin MS02-005, or visit link below.
http://www.microsoft.com/windows/ie/downloads/critical/default.asp
If you have some questions about this article contact us at rdquest12@microsoft.com

Thank you for using Microsoft products.

With friendly greetings,
MS Internet Security Center.

The email message created by W32/Gibe tries to convince users that the attached file is patch supplied by Microsoft. The attached file is in fact a copy of the malicious code.

The attached file has the following characteristics:

File name: q216309.exe
MD5: 739f917f746eb124514155cf36de5111
File size: 122880

When the attached file containing the malicious code is executed, it appears as though it is installing a Microsoft Security Update. It displays several dialog boxes during this process. The malicious code continues to execute regardless of the user's responses to the displayed dialog boxes. (Clicking "Cancel" will not stop the malicious code from executing.)

During execution, W32/Gibe creates the following files in the Windows root directory of the local system:

- Q216309.exe (a copy of the malicious code)
- Vtnmsccd.dll (a copy of the malicious code)
- BcTool.exe (mass-mailing component)
- WinNetW.exe (searches for email addresses)
- GFXacc.exe (backdoor trojan)

The worm also creates the file 02_N803.dat in the Windows directory to store email addresses collected from the Microsoft Outlook address book and various other files on the local system.

The following values are added to the registry to ensure that the backdoor and mass-mailing functions run each time the system restarts:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\

LoadDBackUp = C:\Windows\BcTool.exe

3Dfx Acc = C:\Windows\GFXacc.exe

W32/Gibe also creates the registry key:

HKEY_LOCAL_MACHINE\Software\AVTech\

Installed = ...by Begbie

Default Address = (default email address)

Default Server = (default SMTP server)

If the user runs the attached file again, it displays a dialog box indicating that the patch has already been applied.

II. Impact

W32/Gibe installs a backdoor (GFXacc.exe), which listens on port 12378/tcp. This may allow an intruder to gain access to the system and execute arbitrary commands.

In addition, W32/Gibe mass-mails copies of itself to addresses found on the victim host. The victim and targeted sites may experience an increased load on the mail server when the malicious code is propagating.

III. Solution

Remove infected files from the system

If the attached file has not been executed, it should be safe to simply delete the message and attachment from your email client.

If the malicious code has run, it's possible to get rid of W32/Gibe by deleting all of its components from an infected system. It should be noted that this is an incomplete process; it will not remove the entries in the system registry. If possible, it is best to run an anti-virus product to repair the system and remove the associated files.

Configure email clients to block executable attachments

Many email clients can be configured to prevent users from opening potentially malicious executable attachments while reading mail.

Run and maintain an anti-virus product

It is important for users to update their anti-virus software. Most anti-virus software vendors have released updated information, tools, or virus databases to help detect and recover from W32/Gibe. A list of vendor-specific anti-virus information can be found in Appendix A.

Many anti-virus packages support automatic updates of virus definitions. We recommend using these automatic updates when available.

Exercise caution when opening attachments

Exercise caution when receiving email with attachments. Users should be suspicious of unexpected attachments regardless of their origin. In general, users should also always scan files received through email with an anti-virus product.

The following section of the "Home Network Security" document provides advice on handling email attachments securely: http://www.cert.org/tech_tips/home_networks.html#IV-A-4

Filter the email or use a firewall

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

Appendix A: Vendor Information

Central Command, Inc.

http://support.centralcommand.com/cgi-bin/command.cfg/php/enduser/std_adp.php?p_sid=J2Rv5R9g&p_lva=&p_refno=020304-000001

Command Software Systems

http://www.commandsoftware.com/virus/gibe.html

Computer Associates

http://www3.ca.com/virus/virus.asp?ID=11468

F-Secure Corp

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

McAfee

http://vil.mcafee.com/dispVirus.asp?virus_k=99377&

Microsoft

The Microsoft PSS Security Response Team Alert for this issue can be found at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/virus/alerts/gibe.asp The alert also tells how to contact Microsoft for free support for this sort of issue.

Outlook XP and Outlook 2000 and 98 with the Outlook Email Security Update are not vulnerable to this virus as they would automatically block the .exe attachment from being opened. More information on the Outlook Email Security Update can be found here: http://www.microsoft.com/office/ork/2000/journ/OutSecUpdate.htm

Norman Data Defense Systems

http://www.norman.com/virus_info/w32_gibe_a_mm.shtml

Panda Software

http://service.pandasoftware.es/servlet/panda.pandaInternet.EntradaDatosInternet?operacion=EV2FichaVirus&idVirusFicha=2627&pestanaFicha=1&idioma=2

Proland Software

http://www.pspl.com/virus_info/worms/gibe.htm

Sophos

http://www.sophos.com/virusinfo/analyses/w32gibea.html

Symantec

http://securityresponse.symantec.com/avcenter/venc/data/pf/w32.gibe@mm.html

Trend Micro

http://www.antivirus.com/vinfo/virusencyclo/default5.asp?VName=WORM_GIBE.A

You may wish to visit the CERT/CC's Computer Virus Resources Page located at:

http://www.cert.org/other_sources/viruses.html

Author(s): Brian B. King

Revision History

March 12, 2002: Initial release

March 13, 2002: Added statement from Microsoft

3 IN-2002-03: Social Engineering Attacks via IRC and Instant Messaging

The CERT Coordination Center publishes incident notes to provide information about incidents to the Internet community.

Release Date: March 19, 2002

A complete revision history can be found at the end of this file.

Systems Affected Systems running Internet Relay Chat (IRC) or Instant Messaging (IM) clients

Overview

The CERT/CC has received reports of social engineering attacks on users of Internet Relay Chat (IRC) and Instant Messaging (IM) services. Intruders trick unsuspecting users into downloading and executing malicious software, which allows the intruders to use the systems as attack platforms for launching distributed denial-of-service (DDoS) attacks. The reports to the CERT/CC indicate that tens of thousands of systems have recently been compromised in this manner.

I. Description

Reports received by the CERT/CC indicate that intruders are using automated tools to post messages to unsuspecting users of IRC or IM services. These messages typically offer the opportunity to download software of some value to the user, including improved music downloads, anti-virus protection, or pornography. Once the user downloads and executes the software, though, their system is co-opted by the attacker for use as an agent in a distributed denial-of-service (DDoS) network. Other reports indicate that Trojan horse and backdoor programs are being propagated via similar techniques.

Here is an example of one such message:

```
You are infected with a virus that lets hackers get into your machine and read ur files, etc. I suggest you to download [malicious url] and clean ur infected machine. Otherwise you will be banned from [IRC network].
```

This is purely a social engineering attack since the user's decision to download and run the software is the deciding factor in whether or not the attack is successful. Although this activity is not novel, the technique is still effective, as evidenced by reports of tens of thousands of systems being compromised in this manner. See IN-2000-08: Chat Clients and Network Security for additional information.

II. Impact

As with any DDoS tool installation, the impact is twofold. First, on systems that are compromised by users running untrusted software, intruders may

- exercise remote control
- expose confidential data
- install other malicious software
- change files
- delete files

These risks are not limited to the installation of DDoS agents. In fact, any time a user runs untrusted software these same dangers are present.

The secondary impact is to the sites targeted by the DDoS agents. Sites undergoing a DDoS attack may experience unusually heavy traffic volumes or high packet rates, resulting in degradation of services or loss of connectivity altogether.

III. Solutions

Home users

Run and maintain an anti-virus product

The malicious code being distributed in these attacks is under continuous development by intruders, but most anti-virus software vendors release frequently updated information, tools, or virus databases to help detect and recover from the malicious code involved in this activity. Therefore, it is important that users keep their their anti-virus software up to date. The CERT/CC maintains a partial list of anti-virus vendors at http://www.cert.org/other_sources/viruses.html#VI.

Many anti-virus 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. Users of IRC and IM services should be particularly wary of following links or running software sent to them by other users, as this is a commonly used method among intruders attempting to build networks of DDoS agents.

Understand the risks

Users are encouraged to review our "Home Network Security" tech tip, which provides an overview of risks and mitigation strategies for home users.

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

Sites

Site administrators are encouraged to review our report on denial of service attack technology trends, as well as our recommendations for managing the threat of denial-of-service attacks.

Trends in Denial of Service Attack Technology

http://www.cert.org/archive/pdf/DoS_trends.pdf

Managing the Threat of Denial-of-Service Attacks

http://www.cert.org/archive/pdf/Managing_DoS.pdf

Author(s): Allen D. Householder

Revision History

March 19, 2002: Initial release

4 IN-2002-04: Exploitation of Vulnerabilities in Microsoft SQL Server

The CERT Coordination Center publishes incident notes to provide information about incidents to the Internet community.

Release Date: May 22, 2002
Last Updated: May 23, 2002

A complete revision history can be found at the end of this file.

Systems Affected

- Systems running Microsoft SQL Server or Microsoft SQL Server 2000 installed with mixed mode security enabled
- Systems running Microsoft Data Engine 1.0 (MSDE 1.0) or Microsoft SQL Server 2000 Desktop Engine (MSDE 2000) installed with mixed mode security enabled
- Systems running Tumbleweed's Secure Mail (MMS) versions 4.3, 4.5, and 4.6

Overview

The CERT/CC has received reports of systems being compromised through the automated exploitation of null or weak default *sa* passwords in Microsoft SQL Server and Microsoft Data Engine. This activity is accompanied by high volumes of scanning, and appears to be related to recently discovered self-propagating malicious code, referred to by various sources as Spida, SQLsnake, and Digispid.

I. Description

Reports received by the CERT/CC indicate that the Spida worm scans for systems listening on port 1433/tcp. Once connected, it attempts to use the `xp_cmdshell` utility to enable and set a password for the guest user.

If successful, the worm then

1. assigns the guest user to the local Administrator and Domain Admins groups
2. copies itself to the victim system
3. disables the guest account
4. sets the *sa* password to the same password as the guest account
5. executes the copy on the victim system

Once the local copy is executing on the victim system, the worm begins scanning for other systems to infect. It also attempts to send a copy of the local password (SAM) database, network configuration information, and other SQL server configuration information to a fixed email address (ixtld@postone.com) via email.

The attack used by the Spida worm is similar to that used by the Kaiten malicious code described in IN-2001-13. Additional information on null default *sa* passwords in Microsoft SQL Server can be found in VU#635463.

II. Impact

The scanning activity of the Spida worm may cause denial-of-service conditions on compromised systems, and it has been reported to cause high traffic volumes even on networks with no compromised hosts.

Information about the victim system's configuration and accounts may be compromised by the email the worm attempts to send.

By leveraging a default null password, an attacker may execute arbitrary commands on the system in the security context in which the Microsoft SQL Server services are running. While site-specific configurations may vary, the SQL Server is typically run with system-level privileges.

III. Solutions

Detection

During the course of the Spida worm's execution, a number of files are created on the victim system. These include

- %SystemRoot%\System32\drivers\services.exe
- %SystemRoot%\System32\sqlexec.js
- %SystemRoot%\System32\clemail.exe
- %SystemRoot%\System32\sqlprocess.js
- %SystemRoot%\System32\sqlinstall.bat
- %SystemRoot%\System32\sqldir.js
- %SystemRoot%\System32\run.js
- %SystemRoot%\System32\timer.dll
- %SystemRoot%\System32\samdump.dll
- %SystemRoot%\System32\pwdump2.exe

The presence of any of these files on the system indicates compromise.

Scanning for other systems on port 1433/tcp or attempts to send email to ixtld@postone.com may also indicate a compromised system.

Response

If you believe a system under your administrative control may have been compromised, please refer to Steps for Recovering from a UNIX or NT System Compromise.

Protection

Set a password on the *sa* account

Following best practices, passwords should never be left with a null or easily guessed value. Ensure that a password has been assigned to the *sa* account on Microsoft SQL Servers under your control.

Note that when installing Microsoft SQL 2000 Server, the application prompts for an *sa* password. If a null password is entered, a warning will be displayed, but the application will permit a null password to be used.

Instructions to change the SQL Server password are located at

> http://msdn.microsoft.com/library/default.asp?url=/library/en-us/ modadmin/html/deconchangingsqlserveradministratorlogin.asp
>
> http://msdn.microsoft.com/library/default.asp?url=/library/en-us/ adminsql/ad_1_server_5un8.asp

Instructions to change the MSDE password can be found at

> http://support.microsoft.com/default.aspx?scid=kb;en-us;Q322336

Additional information on securing Microsoft SQL Server can be found at

> http://www.microsoft.com/sql/techinfo/administration/2000/security.asp

Limit access to the SQL Server port

Packet filtering should be performed at network borders to prohibit externally initiated inbound connections to non-authorized services. With regards to SQL Server, ingress filtering of port 1433/tcp could prevent attackers outside of your network from scanning or infecting vulnerable Microsoft SQL servers in the local network that are not explicitly authorized to provide public SQL services.

Filtering packets destined for other services that are not explicitly required can also prevent intruders from connecting to backdoors on compromised systems.

Egress filtering

Egress filtering manages the flow of traffic as it leaves a network under your administrative control. There is typically limited need for machines providing public services to initiate outbound connections to the Internet. In the case of the Spida worm, employing egress filtering to disallow outbound connections to port 1433/tcp at your network border can help prevent systems on your network from attacking systems elsewhere. This is only effective against systems that are already infected with the Spida worm.

Block outgoing email to ixtld@postone.com

As mentioned in the Description section above, the worm attempts to send configuration information and the local password database to ixtld@postone.com. Blocking email to this address can reduce the risk of confidential information being exposed by the Spida worm. However, as with the egress filtering recommendation above, this only blocks systems that are already infected, so it is not sufficient to block the email without taking other precautionary steps as described above.

IV. Additional protection

Apply a patch from Microsoft

Microsoft Corporation has released Microsoft Security Bulletin MS02-020, which announces the availability of a cumulative patch to address a variety of problems. While this patch does not address null *sa* passwords, it does fix a number of serious security issues. We strongly encourage you to read this bulletin and take the appropriate corrective measures. MS02-020 is available at

> http://www.microsoft.com/technet/ treeview/default.asp?url=/technet/security/bulletin/MS02-020.asp

Reporting

The CERT/CC is interested in receiving reports of this activity. If machines under your administrative control are compromised, please send mail to cert@cert.org with the following text included in the subject line: "[CERT#38873]".

Author(s): Chad Dougherty and Allen Householder

Revision History

May 22, 2002: Initial release

May 23, 2002: Updated systems affected, added link for MSDE password change to Solutions

5 IN-2002-05: W32/Frethem Malicious Code

The CERT Coordination Center publishes incident notes to provide information about incidents to the Internet community.

Release Date: July 17, 2002

Systems Affected

- Systems running Microsoft Windows

Overview

The CERT/CC has received a number of reports of malicious code known as W32/Frethem. It affects systems running Microsoft Windows with unpatched versions of Internet Explorer and mail clients that use IE's HTML rendering engine (including Outlook and Outlook Express). Patched systems (or systems that do not use IE's HTML rendering engine for mail) may also be affected if a user manually executes the malicious code. A number of variants of this code have been identified.

I. Description

W32/Frethem is a malicious Windows program with an internal SMTP mail delivery agent. W32/Frethem arrives as an email message containing three MIME parts (`multipart/alternative; boundary=L1db82sd319dm2ns0f4383dhG`) with the subject "Re: Your password!" The body of the message is contained in the first MIME part and includes a specially crafted IFRAME tag that will cause the malicious attachment to be executed when this part is rendered in a vulnerable mail user agent (as described below). The body also contains the following text:

> **ATTENTION!**
>
> You can access
> **very important**
> information by
> this password
>
> **DO NOT SAVE**
> password to disk
> use your mind
>
> now press
> **cancel**

The next two MIME parts are the attachments, `decrypt-password.exe` and `password.txt`. In samples received by the CERT/CC, the `password.txt` file contains the text "Your password is W8dqwq8q918213", but it does not contain any executable code. The malicious code is contained in the `decrypt-password.exe` file. We have received variants of `decrypt-password.exe` with the following MD5 checksums:

`decrypt-password.exe`

file size: 48,640 bytes md5: 5412f64b6d2279d2da89a43be9e1a001

file size: 48,640 bytes md5: cc695e7e531c18843baa0731a38e969b

file size: 35,840 bytes md5: ded90e8bd58aaab9d864cce245c57ba2

file size: 35,840 bytes md5: e4858975a01a614f08b22dc4069f6360

In the variants we have received, `decrypt-password.exe` appears as an attachment flagged as a MIME content type `audio/x-midi`, which allows W32/Frethem to exploit the vulnerability described in VU#980499 and run automatically if the message is viewed on a vulnerable system. Even if the system has been patched for this vulnerability, a user can still trigger infection by opening the attachment directly.

When `decrypt-password.exe` is run, it creates the `IEXPLORE_MUTEX_AABBCCDDEEFF` mutex to ensure that only one copy will run at a time. It also gathers the current user's default SMTP server, email address, and display name from the registry keys located at

HKCU\Software\Microsoft\Internet Account Manager\Accounts\00000001

It uses these in conjunction with its built-in SMTP engine in order to propagate. It harvests email addresses from the Windows Address Book as well as any other files with .wab, .dbx, .mbx, .mdb, and .eml extensions.

W32/Frethem attempts to install itself locally so it will run again whenever Windows restarts. In some variants, it does this by placing a copy of itself in the `Start Menu\Programs\Startup` folder as `setup.exe`. A more recent variant accomplishes this by copying itself to `%WinDir%/taskbar.exe` and adding a registry key named 'Task Bar' to

HKCU\Software\Microsoft\Windows\CurrentVersion\Run

with a value of `%WinDir%/taskbar.exe`

II. Impact

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

III. Solution

Update Internet Explorer

Users are encouraged to install the patches detailed in MS01-020. (Note: MS01-020 has been superseded by MS02-023, so users should consider installing the appropriate patches from MS02-023 if possible) Microsoft has published additional recommendations for protecting against W32/Frethem at

> http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/virus/alerts/frethem.asp

Run and maintain an anti-virus product

It is important for users to update their anti-virus software. Most anti-virus software vendors have released updated information, tools, or virus databases to help detect and recover from W32/Frethem. A list of vendor-specific anti-virus information can be found in Appendix A.

Many anti-virus packages support automatic updates of virus definitions. We recommend using these automatic updates when available.

Exercise caution when opening attachments

Exercise caution when receiving email with attachments. Users should be suspicious of unexpected attachments, regardless of their origin. In general, users should also always scan files received through email with an anti-virus product.

The following section of the "Home Network Security" document provides advice on handling email attachments securely: http://www.cert.org/tech_tips/home_networks.html#IV-A-4.

Filter the email or use a firewall

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

Appendix A. Vendor Information

Aladdin Knowledge Systems

> http://www.esafe.com/home/csrt/valerts2.asp?virus_no=10228

Central Command, Inc.

> http://support.centralcommand.com/cgi-bin/command.cfg/php/enduser/std_adp.php?p_refno=020612-000007

Command Software Systems

http://www.commandsoftware.com/virus/frethem.html

Computer Associates

http://www3.ca.com/virusinfo/virus.asp?ID=12569

F-Secure Corp

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

McAfee

http://vil.mcafee.com/dispVirus.asp?virus_k=99565&

Microsoft

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/virus/alerts/frethem.asp

Norman Data Defense Systems

http://www.norman.com/virus_info/w32_frethem_k_mm.shtml

Proland Software

http://www.pspl.com/virus_info/worms/fretheme.htm

Sophos

http://www.sophos.com/virusinfo/analyses/w32frethemfam.html

Symantec

http://securityresponse.symantec.com/avcenter/venc/data/w32.frethem.k@mm.html

Trend Micro

http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_FRETHEM.K

You may wish to visit the CERT/CC's Computer Virus Resources Page located at: http://www.cert.org/other_sources/viruses.htm.

Author(s): Kevin Houle and Allen D. Householder

6 IN-2002-06: W32/Lioten Malicious Code

Release Date: December 4, 2001

Systems Affected

- Systems running Microsoft Windows with Microsoft Outlook installed
- Systems running Microsoft Windows with Microsoft Office and ICQ installed

Overview

W32/Goner is a malicious Windows program distributed as an email file attachment and via ICQ file transfers. To a user, the file (gone.scr) appears to be a Windows screen saver. W32/Goner infects a system when a user executes file "gone.scr".

Description

Late this morning, the CERT/CC began receiving reports of a new piece of malicious code known as W32/Goner. Since that time, the CERT/CC has received an increasing number of reports of this code circulating on the Internet.

Analysis indicates that this code is spreading via email with the following characteristics:

```
Subject:        Hi!

Body:   How are you ?

When I saw this screen saver, I immediately thought about you I am
in a harry, I promise you will love it!

Attachment:gone.scr
```

Several anti-virus vendors have stated that this code may also propogate via the ICQ messaging program. W32/Goner is believed to initiate a file transfer with any "online" users in the infected user's contact list. If the user on the receiving end approves the transfer, the worm sends a copy of itself.

When the file "gone.scr" is executed, the worm displays a splash screen and a false error message in an attempt to fool the user into thinking the program is a legitimate screen saver. It copies itself to the Windows system folder (usually C:\WINDOWS\SYSTEM32\scr.exe or C:\WINNT\SYSTEM32\scr.exe) and modifies the Windows registry to execute itself upon reboot by adding the following key:

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

W32/Goner propagates by sending itself to all addresses listed in the Microsoft Outlook address book and all online users in the ICQ contacts list.

In addition, the worm looks for and terminates processes associated with many popular antivirus and security programs. The following processes/files are targeted by this malicious code:

APLICA32.EXE
ZONEALARM.EXE
ESAFE.EXE
CFIADMIN.EXE
CFIAUDIT.EXE
CFINET.EXE
PCFWallIcon.EXE
FRW.EXE
VSHWIN32.EXE
VSECOMR.EXE
WEBSCANX.EXE
AVCONSOL.EXE
VSSTAT.EXE
PW32.EXE
VW32.EXE
VP32.EXE
VPCC.EXE
VPM.EXE
_AVP32.EXE
_AVPCC.EXE
_AVPM.EXE
AVP32.EXE
AVPCC.EXE
AVPM.EXE
AVP.EXE
LOCKDOWN2000.EXE
ICLOAD95.EXE
ICMON.EXE
ICSUPP95.EXE
ICLOADNT.EXE
ICSUPPNT.EXE
TDS2-98.EXE
TDS2-NT.EXE
FEWEB.EXE
SAFEWEB.EXE

If W32/Goner finds any of these programs running, the process is terminated and all files in the directory containing that executable are deleted. If the worm is unable to delete the files immediately, it creates a file called WININIT.INI, which deletes the files upon reboot.

There is also some evidence that W32/Goner may install denial of service scripts for the mIRC Internet Relay Chat client.

Impact

The worm may disable anti-virus and security software installed on the system.

During propagation, sites may experience residual denial of service conditions on hosts or email systems through which the worm is sent.

Solutions

Run and maintain an antivirus product

It is important for users to update their antivirus software. Most antivirus software vendors have released updated information, tools, or virus databases to help detect and partially recover from this malicious code. A list of vendor-specific antivirus information can be found in Appendix A.

Many antivirus packages support automatic updates of virus definitions. We recommend using these automatic updates when available.

Don't open email attachments

The W32/Goner worm may arrive as an email attachment (gone.scr). Users should **not** open attachments of this nature. In general, users should use caution when opening any email attachment by first scanning it with an anti-virus product.

Don't open files received via instant messaging applications

The W32/Goner worm may arrive via an ICQ file transfer. ICQ users should exercise caution when opening files received via a file transfer just as they would with email attachments.

Filter email attachments

System administrators may install filters on mail servers to prevent potentially harmful files (.exe, .vbs, .bat, .scr, etc.) from being spread via email. In this case filters could be used to prevent the spread of "gone.scr".

Reporting

The CERT/CC is interested in receiving reports of this activity. If machines under your administrative control are compromised, please send mail to cert@cert.org with the following text included in the subject line: "[CERT#27693]".

Appendix A. Vendor Information

Antivirus Vendor Information

Computer Associates

http://www3.ca.com/solutions/collateral.asp?CT=65&ID=1212

F-Secure Corp

http://www.fsecure.com/v-descs/goner.shtml

McAfee

http://vil.nai.com/vil/virusSummary.asp?virus_k=99272

Norman Data Defense Systems

http://www.norman.com/virus_info/w32_goner_a_mm.shtml

Sophos

http://www.sophos.com/virusinfo/analyses/w32gonera.html

Symantec

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

Trend Micro

http://www.antivirus.com/vinfo/virusencyclo/default5.asp?VName=WORM_GONE.A

In addition to these specific vendors, you may wish to visit the CERT/CC's computer virus resources page located at

http://www.cert.org/other_sources/viruses.html

Author(s): Brian B. King, John Shaffer, Robert Hanson

Revision History

December 4, 2001: Initial Release