CERT Incident Note IN-2001-14: W32/BadTrans Worm

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

W32/BadTrans Worm

Release Date: November 27, 2001

Systems Affected

- Systems running Microsoft Windows 95, 98, ME, NT, and 2000

Overview

W32/BadTrans is a malicious Windows program distributed as an email file attachment. Because of a known vulnerability in Internet Explorer, some email programs, such as Outlook Express and Outlook, may execute the malicious program as soon as the email message is viewed.

Description

The W32/BadTrans worm attempts to use two known vulnerabilities to compromise systems and propagate.

The format of the MIME headers in an email containing W32/BadTrans attempts to exploit a vulnerability in Internet Explorer where certain MIME types can cause arbitrary code to be executed. For more information, including patch information, see

> CERT Vulnerability Note VU#980499
> http://www.kb.cert.org/vuls/id/980499

On systems that are patched for this vulnerability, the user may receive a confirmation message asking whether or not to execute the attachment. Running the attachment on these systems will still result in a compromise. Users should not execute programs in email attachments unless they exercise reasonable care to ensure that the attachments do not contain malicious code.

The filename in the email attachment of a W32/BadTrans infected email varies from message to message but always has two file extensions. By default, Windows may hide the true file extension from the user, as discussed in

> CERT Incident Note IN-2000-07
> http://www.cert.org/incident_notes/IN-2000-07.html

When the malicious program is executed, a copy is written as "Kernel32.exe" in the Windows directory.

```
C:\WINDOWS\Kernel32.exe
  MD5 checksum = 0bf5eaeed25da53f85086767bcd86e5e
  Filesize     = 29020 bytes
```

Kernel32.exe is executed and the originally executed file attachment is deleted from the system. Kernel32.exe may run as a system service on some versions of Windows, causing it to not be visible in the default system task list provided by Microsoft.

Kernel32.exe writes two additional files to disk in the Windows system directory.

```
C:\WINDOWS\SYSTEM\kdll.dll
  MD5 checksum = c7ceb9fb63edc7fb7c7767f899ff5491
  Filesize     = 5632 bytes

C:\WINDOWS\SYSTEM\cp_25389.nls
  MD5 checksum = varies
  Filesize     = varies
```

Reports indicate the "kdll.dll" file contains routines to record a user's keystrokes on the infected computer. The "cp_25389.nls" file contains logged keystrokes in encrypted form. Some reports indicate the contents of the log file are sent via email to a particular destination potentially causing sensitive information to be exposed.

Kernel32.exe sets a registry key to insure it is restarted when the computer restarts.

```
HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce\Kernel32  = "kernel32.exe"
```

While running, Kernel32.exe checks this registry value approximately every 10 seconds to insure that it is set.

Reports indicate that W32/BadTrans sends copies of itself via email to addresses found in unanswered email or in files found on the computer system. Email messages generated and sent by W32/BadTrans have some identifiable characteristics.

- During the SMTP conversation, the W32/BadTrans host will issue a "HELO AOL.COM" statement. This is generally visible in the resulting Received: header in the message.
- The address in the From: header will have a '_' prepended to the sender's email address.
- The MIME headers contain:

```
Mime-Version: 1.0
Content-Type: multipart/related;
    type="multipart/alternative";
    boundary="====_ABC1234567890DEF_====="
```

- The body of the MIME message contains:

```
--====_ABC1234567890DEF_====
Content-Type: multipart/alternative;
         boundary="====_ABC0987654321DEF_====="

--====_ABC0987654321DEF_====
Content-Type: text/html;
         charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable


<HTML><HEAD></HEAD><BODY bgColor=3D#ffffff>
<iframe src=3Dcid:EA4DMGBP9p height=3D0 width=3D0>
</iframe></BODY></HTML>
--====_ABC0987654321DEF_====--

--====_ABC1234567890DEF_====
Content-Type: audio/x-wav;
         name="filename.ext.ext"
Content-Transfer-Encoding: base64
Content-ID:
```

Some reports in public forums indicate that a backdoor is installed by W32/BadTrans, however the CERT/CC has been unable to confirm these reports in our own analysis.

Impact

The worm can execute arbitrary commands with the same privileges as the user who triggered it.

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

Solutions

Apply the appropriate patch from your vendor

If you are running a vulnerable version of Internet Explorer (IE), the CERT/CC recommends upgrading to at least version 5.0 since older versions are no longer officially maintained by Microsoft. Users of IE 5.0 and above are encouraged to apply patch for the "Automatic Execution of Embedded MIME Types" vulnerability available from Microsoft at

http://www.microsoft.com/technet/security/bulletin/MS01-020.asp

Note: IE 5.5 SP1 users should apply the patches discussed in
MS01-027

Run and maintain an antivirus product

It is important for users to update their anti-virus 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 anti-virus packages support automatic updates of virus definitions. We recommend using these automatic updates when available.

Don't open email attachments

The W32/BadTrans worm may arrive as an email attachment with a filename such as "file.ext1.ext2". Users should **not** open attachments of this nature. If an attachment of this type absolutely needs to be opened, the CERT/CC recommends exercising care to handle it in a way that allows it to be scanned for malicious code prior to execution.

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#26210]".

Appendix A. Vendor Information

Antivirus Vendor Information

Aladdin Knowledge Systems

http://www.ealaddin.com/home/csrt/valerts2.asp?virus_no=10093&cf=tl

Command Software Systems

http://www.commandcom.com/virus/badtrans.html

Computer Associates

http://www3.ca.com/Virus/Virus.asp?ID=10579

F-Secure Corp

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

McAfee

http://vil.mcafee.com/dispVirus.asp?virus_k=99069&

Norman Data Defense Systems

http://www.norman.com/virus_info/w32_badtrans_29090_mm.shtml

Panda Software

http://service.pandasoftware.es/servlet/panda.pandaInternet.EntradaDatosInternet?operacion=EV2FichaVirus&pestanaFicha=0&idioma=2&nombreVirusFicha=W32/Badtrans.B

P Software

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

Sophos

http://www.sophos.com/virusinfo/analyses/w32badtransb.html

Symantec

http://www.symantec.com/avcenter/venc/data/w32.badtrans.b@mm.html

Trend Micro

http://www.antivirus.com/vinfo/virusencyclo/default5.asp?VName=WORM_BADTRANS.B

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): Kevin Houle, Chad Dougherty

Revision History

November 27, 2001: Initial Release
November 28, 2001: Corrected incident number in reporting section
February 28, 2002: Removed extraneous text from F-Secure vendor link