

Bobax.C

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2004-05/3270.html

From: MAP (*anonymous_at_discussions.microsoft.com*)

Date: 05/19/04

Date: Wed, 19 May 2004 14:23:25 -0700

>-----Original Message-----

>I cant seem to delete a file containing the W32.Bobax.c

>virus. The file is located in C:\Documents and

>Settings\User\Local Settings and is named ~9.tmp

>

>I have downloaded the recent updates from microsoft and

>semantec. Other files containing the virus have been

>deleted.

>

>Any ideas?

>

>

>.

>

Try it in safe mode?

Another reason to disable DCOM!

<http://grc.com/dcom/>

W32.Bobax.C

Discovered on: May 18, 2004

Last Updated on: May 19, 2004 11:58:26 AM

W32.Bobax.C is a worm that exploits both the LSASS vulnerability using port 445 (described in Microsoft Security Bulletin MS04-011) and the DCOM RPC vulnerability (first described in Microsoft Security Bulletin MS03-026) using TCP port 135.

Infected computers can become email relays.

W32.Bobax.C differs from W32.Bobax.A as follows:

- Uses a different, and variable, mutex name
- Has a different size and MD5
- Performs connection speed testing
- Has the ability to update itself
- Has the ability to report system information back to the author
- Takes advantage of the DCOM RPC vulnerability described in Microsoft Security Bulletin MS03-026

While this threat may execute on Windows 95/98/Me/Server 2003-based computers, it targets only Windows 2000/XP-based computers for exploitation.

Also Known As: W32/Bobax.worm.c [McAfee],
TrojanProxy.Win32.Bobax.c [Kaspersky]

Type: Worm
Infection Length: 22,528 bytes

Systems Affected: Windows 2000, Windows XP
Systems Not Affected: DOS, Linux, Macintosh, Novell
Netware, OS/2, UNIX, Windows 3.x, Windows 95, Windows 98,
Windows Me, Windows NT, Windows Server 2003
CVE References: CAN-2003-0533, CAN-2003-0352

Virus Definitions (Intelligent Updater) *
May 18, 2004

Virus Definitions (LiveUpdateT) **
May 18, 2004

*

Intelligent Updater definitions are released daily, but require manual download and installation.
[Click here to download manually.](#)

**

LiveUpdate virus definitions are usually released every Wednesday.
[Click here for instructions on using LiveUpdate.](#)

Wild:

Number of infections: 50 – 999

Number of sites: More than 10

Geographical distribution: Low

Threat containment: Easy

Removal: Moderate

Threat Metrics

Wild:

Low

Damage:

Medium

Distribution:

Medium

Damage

Payload Trigger: n/a

Payload: n/a

Large scale e-mailing: n/a

Deletes files: n/a

Modifies files: n/a

Degrades performance: Causes significant performance degradation.

Causes system instability: May cause the machine to reboot.

Releases confidential info: n/a

Compromises security settings: Allows unauthorized remote access.

Distribution

Subject of email: n/a

Name of attachment: n/a

Size of attachment: n/a

Time stamp of attachment: n/a

Ports: 445/tcp, 5000/tcp, random ports

Shared drives: n/a

Target of infection: Unpatched systems vulnerable to LSASS exploit – MS04-011.

When W32.Bobax.C is executed, it performs the following actions:

Creates a mutex "06:08:07:<random numbers>", where <random numbers> is a series of random numbers based on

the volume serial number of the infected system. This mutex ensures that only a single copy of the worm is present in memory.

Copies itself as %System%\<random_characters>.exe, where <random_characters> is a random number of random characters.

Note: %System% is a variable. The worm locates the System folder and copies itself to that location. By default, this is C:\Windows\System (Windows 95/98/Me), C:\Winnt\System32 (Windows NT/2000), or C:\Windows\System32 (Windows XP).

Adds the value

"<random_characters>" = "%System%\<random_characters>.exe"

to the following registry keys:

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

Attempts to delete all files in %temp% that begin with "~".

Drops a randomly named .tmp file into the %Temp% folder. This file is actually a .dll file that contains the worm's main functionality.

Note: %Temp% is a variable. The worm locates the temporary folder and copies itself to that location. By default, this is C:\Windows\TEMP (Windows 95/98/Me/XP) or C:\WINNT\Temp (Windows NT/2000).

Injects the .dll file into Explorer.exe and then ends its own <random_characters>.exe process.

Note: Explorer.exe may crash as a result.

Attempts to download one of several files from various websites to gauge the speed of the internet connection of the host computer.

Attempts to contact a remote Web server with a unique ID code, and some information about the infected host, as notification of infection. The worm parses the response for commands to activate, which include the following:

Sending spam mail

Sending system information to the author

Stopping and restarting scanning

Downloading and running a specified executable

Updating itself

Scans randomly generated IP addresses, attempting to connect to them on TCP port 5000. This will determine whether the system is a Windows XP-based system (see Microsoft Security Bulletin MS01-059). The worm then probes port 135 of the remote computer to verify that the RPC DCOM interface is available.

If the worm determines that the remote system is running Windows XP, it performs the following operations:

Sends shell code to the host on TCP port 445, attempting to exploit the Microsoft Windows LSASS Buffer Overrun Vulnerability, which is described in Microsoft Security Bulletin MS04-011.

If this exploit does not succeed, the worm sends data to TCP port 135 in an attempt to exploit the DCOM RPC vulnerability.

If either exploit is successful, the code that is executed on the remote computer uses HTTP to force a connection to the host computer on a random port.

Downloads the worm from the host computer and saves it on the remote computer as Svc.exe.

The worm is executed on the remote computer.

If the worm determined the remote computer was running Windows 2000, it would only attempt to exploit the DCOM RPC vulnerability, as in steps b through e.

Notes:

A side effect of this exploit is that it eventually crashes the LSASS process, forcing the computer to restart. This is similar to the effect of W32.Sasser.Worm.

Due to the random nature of how the worm constructs the exploit data, this may cause the RPC service to crash if it receives incorrect data. This may manifest as Svchost.exe, generating errors as a result of the incorrect data. If the RPC service crashes, the default procedure under Windows XP and Windows Server 2003 is to restart the computer. To disable this feature, see step 1 of the Removal Instructions.

10. Opens a number of randomly selected ports and awaits incoming connections. The worm runs its own SMTP server routine on these ports, leaving the infected computer open to be used as a spam relay.

Symantec Security Response encourages all users and administrators to adhere to the following basic security "best practices":

Turn off and remove unneeded services. By default, many operating systems install auxiliary services that are not critical, such as an FTP server, telnet, and a Web server. These services are avenues of attack. If they are removed, blended threats have less avenues of attack and you have fewer services to maintain through patch updates.

If a blended threat exploits one or more network services, disable, or block access to, those services until a patch is applied.

Always keep your patch levels up-to-date, especially on computers that host public services and are accessible through the firewall, such as HTTP, FTP, mail, and DNS services.

Enforce a password policy. Complex passwords make it difficult to crack password files on compromised computers. This helps to prevent or limit damage when a computer is compromised.

Configure your email server to block or remove email that contains file attachments that are commonly used to spread viruses, such as .vbs, .bat, .exe, .pif and .scr files.

Isolate infected computers quickly to prevent further compromising your organization. Perform a forensic analysis and restore the computers using trusted media.

Train employees not to open attachments unless they are expecting them. Also, do not execute software that is downloaded from the Internet unless it has been scanned for viruses. Simply visiting a compromised Web site can cause infection if certain browser vulnerabilities are not patched.

Before you begin: If you are running Windows 2000 or XP and you have not yet applied the patch for the vulnerability described in Microsoft Security Bulletin MS04-011, you must do so. If you do not do so, it is likely that your computer will continue to be reinfected.

What to do if the computer shuts down before you can apply the patch
This threat can cause Windows to keep shutting down and restarting. This can prevent you from installing the Microsoft patch.

Notes:

You may have to try this several times because you have only about 20 seconds to do steps 3 through 6.
This will not work on Windows 2000.

To prevent the shutdown
Disconnect the computer from the network/Internet connection. Disconnect the cable, if necessary.
Restart the computer.
As soon as Windows opens and you see the Windows desktop, click Start > Run.
Type cmd and press Enter.
Type shutdown -i and press Enter.
In the Remote Shutdown dialog box, do the following:
Click Add, type your computer name in the Add Computers dialog box, and then click OK.
In the "Display warning for" field, type 9999
In the Comment box, type the following text:

Delay Lsass.exe shutdown.

Click OK.

Reconnect the network/Internet connection.
Connect to the Internet, and obtain the patch file.

Note: After you have patched the computer and removed the

threat, you may re-enable the 20-second default warning.

Continue with the following steps.

The following instructions pertain to all current and recent Symantec antivirus products, including the Symantec AntiVirus and Norton AntiVirus product lines.

Summary steps:

Disable System Restore (Windows XP).

Update the virus definitions.

Restart the computer in Safe mode or VGA mode.

Run a full system scan, and delete all files that are detected as W32.Bobax.C.

Delete the value that was added to the registry.

For specific details on each of these steps, read the following instructions.

1. To disable System Restore (Windows XP)

If you are running Windows XP, we recommend that you temporarily turn off System Restore. Windows Me/XP uses this feature, which is enabled by default, to restore the files on your computer in case they become damaged. If a virus, worm, or Trojan infects a computer, System Restore may back up the virus, worm, or Trojan on the computer.

Windows prevents outside programs, including antivirus programs, from modifying System Restore. Therefore, antivirus programs or tools cannot remove threats in the System Restore folder. As a result, System Restore has the potential of restoring an infected file on your computer, even after you have cleaned the infected files from all the other locations.

Also, a virus scan may detect a threat in the System Restore folder even though you have removed the threat.

For instructions on how to turn off System Restore, read your Windows documentation, or the Symantec Knowledge Base document "How to turn off or turn on Windows XP System Restore."

Note: When you are completely finished with the removal procedure and are satisfied that the threat has been removed, re-enable System Restore by following the instructions in the aforementioned documents.

2. To update the virus definitions

Symantec Security Response fully tests all the virus definitions for quality assurance before they are posted to our servers. There are two ways to obtain the most recent virus definitions:

Running LiveUpdate, which is the easiest way to obtain virus definitions

These virus definitions are posted to the LiveUpdate servers once each week (usually on Wednesdays), unless there is a major virus outbreak. To determine whether definitions for this threat are available by LiveUpdate, refer to the Virus Definitions (LiveUpdate).

Downloading the definitions using the Intelligent Updater
The Intelligent Updater virus definitions are posted on U.S. business days (Monday through Friday). You should download the definitions from the Symantec Security Response Web site and manually install them. To determine whether definitions for this threat are available by the Intelligent Updater, refer to the Virus Definitions (Intelligent Updater).

The Intelligent Updater virus definitions are available:
Read "How to update virus definition files using the Intelligent Updater" for detailed instructions.

3. To restart the computer in Safe mode or VGA mode

Shut down the computer, and turn off the power. Wait for at least 30 seconds, and then restart the computer in Safe mode or VGA mode.

In Windows 95, 98, Me, 2000, or XP, restart the computer in Safe mode.

For instructions, read the document "How to start the computer in Safe Mode."

In Windows NT 4, restart the computer in VGA mode.

4. To scan for and delete the infected files

Start your Symantec antivirus program, and make sure that it is configured to scan all files.

For Norton AntiVirus consumer products

Read the document, "How to configure Norton AntiVirus to scan all files."

For Symantec AntiVirus Enterprise products

Read the document "How to verify that a Symantec Corporate antivirus product is set to scan all files."

Run a full system scan.

If any files are detected as infected with W32.Bobax.C, click Delete.

5. To delete the value from the registry

WARNING: Symantec strongly recommends that you back up the registry before making any changes to it. Incorrect changes to the registry can result in permanent data loss or corrupted files. Modify the specified keys only. Read the document "How to make a backup of the Windows registry" for instructions.

Click Start, and then click Run. (The Run dialog box appears.)

Type regedit

Then click OK. (The Registry Editor opens.)

Navigate to each of the following keys:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\

RunServices

In the right pane, delete the following values:

"random_characters" = "%System%\<random_characters>.exe"

Exit the Registry Editor.

Revision History:

May 19, 2004: Added information pertaining to use of DCOM RPC exploit.