W32.Flamer | Symantec

Archived: 2026-04-05 18:34:07 UTC

The Wayback Machine - https://web.archive.org/web/20190930124504/https://www.symantec.com/security-center/writeup/2012-052811-0308-99

Discovered: May 28, 2012
Updated: June 05, 2012 3:20:22 PM
Also Known As: WORM_FLAMER.A [Trend]
Type: Worm
Systems Affected: Windows
CVE References: CVE-2010-2729 | CVE-2010-2568

W32.Flamer is a worm that may attempt to spread when it receives instructions from a remote attacker. It also opens a back door and may steal information from the compromised computer.

For more information relating to this threat, please see the following resource:
Blog entries on W32.Flamer

Antivirus Protection Dates

- **Initial Rapid Release version** May 28, 2012 revision 009
- **Latest Rapid Release version** March 23, 2017 revision 037
- **Initial Daily Certified version** May 28, 2012 revision 017
- **Latest Daily Certified version** March 23, 2017 revision 041
- **Initial Weekly Certified release date** May 30, 2012

Click here for a more detailed description of Rapid Release and Daily Certified virus definitions.

Technical Description

W32.Flamer is a worm that has the ability to spread from one computer to another. However, the worm does not automatically spread, but instead it waits for instructions from the attackers. If required, it can spread using the following methods:

- Network shares using captured credentials, including Domain Administrator
- Microsoft Windows Print Spooler Service Remote Code Execution Vulnerability (CVE-2010-2729)
- Removable media using a specially crafted autorun.inf file
- Removable drives using a special folder that hides the files and can result in automatic execution on viewing the removable drive when combined with the Microsoft Windows Shortcut 'LNK/PIF' Files Automatic File Execution Vulnerability (CVE-2010-2568)

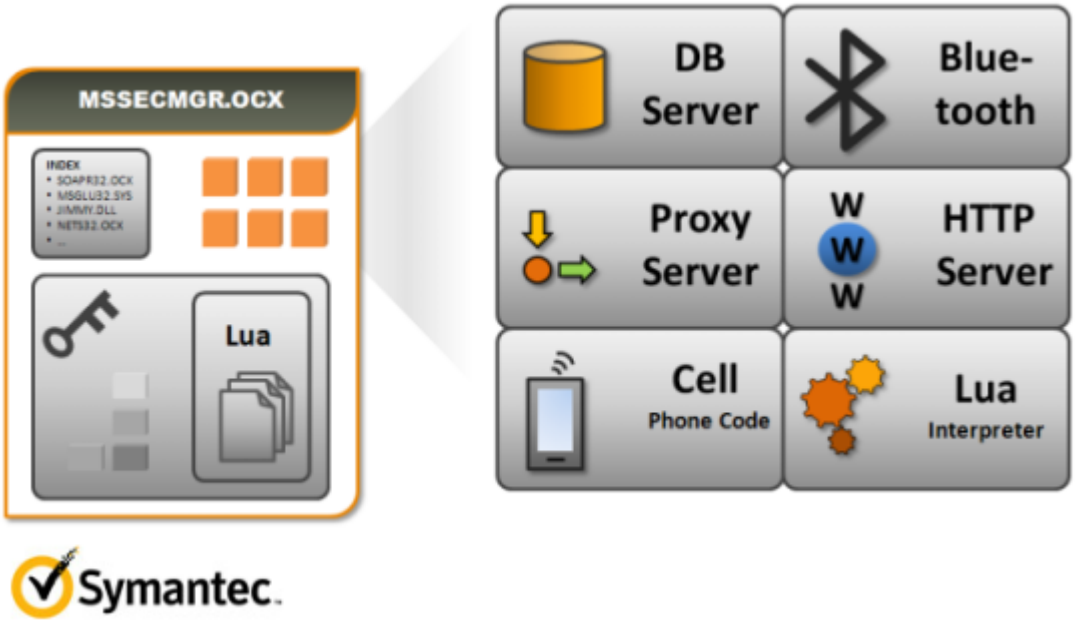
- Hijacking clients performing a Microsoft Windows update

When the worm executes, it may create the following files:

- %System%\boot32drv.sys
- %System%\ccalc32.sys
- %System%\csvde.exe
- %System%\msglu32.ocx
- %System%\mssecmgr.ocx
- %System%\nteps32.ocx
- %SystemDrive%\Program Files\Common Files\Microsoft Shared\MSAudio\audcache
- %SystemDrive%\Program Files\Common Files\Microsoft Shared\MSAudio\audfilter.dat
- %SystemDrive%\Program Files\Common Files\Microsoft Shared\MSAudio\dstrlog.dat
- %SystemDrive%\Program Files\Common Files\Microsoft Shared\MSAudio\lmcache.dat
- %SystemDrive%\Program Files\Common Files\Microsoft Shared\MSAudio\ntcache.dat
- %SystemDrive%\Program Files\Common Files\Microsoft Shared\MSAudio\wavesup3.drv
- %SystemDrive%\Program Files\Common Files\Microsoft Shared\MSAudio\wpgfilter.dat
- %Temp%\~a38.tmp
- %Temp%\~c34.tmp
- %Temp%\~DEB93D.tmp
- %Temp%\~dra53.tmp
- %Temp%\~HLV084.tmp
- %Temp%\~HLV084.tmp
- %Temp%\~HLV294.tmp
- %Temp%\~HLV473.tmp
- %Temp%\~HLV473.tmp
- %Temp%\~HLV751.tmp
- %Temp%\~HLV927.tmp
- %Temp%\~HLV927.tmp
- %Temp%\~KWI988.tmp
- %Temp%\~mso2a0.tmp
- %Temp%\~mso2a2.tmp
- %Temp%\~rf288.tmp
- %Temp%\~ZFF
- %Temp%\dat3C.tmp

Next, it creates the following registry entry so that it executes whenever Windows starts:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32\"wave9" = "%SystemDrive%\Program Files\Common Files\Microsoft Shared\msaudio\wavesup3.drv"

The mssecmgr.ocx file is the principal file in this threat and it is the first element of the threat that is executed on a compromised computer. The file contains a large number of sub-components that implement many of functions that this threat can perform.



For example, there are components that provide Web, Proxy and SSH services, manage databases, a component to handle Bluetooth, and there is even a component that is a script engine for the Lua scripting language .

Lua is a lightweight and fast scripting language that has multiple uses including video games. It is particularly suited for embedding within executable files allowing for functionality to be scripted quickly. Much of the functionality contained within W32.Flamer is implemented using the embedded Lua scripts.

Most sub-components, including various scripts, are stored in an encrypted resource embedded in the mssecmgr.ocx file. Several standalone executable DLL files are also included. The sub-components include some of the following files:

- %CurrentFolder%\00006411.dll
- %CurrentFolder%\advnetcfg.ocx
- %CurrentFolder%\boot32drv.sys
- %CurrentFolder%\jimmy.dll
- %CurrentFolder%\msglu32.ocx
- %CurrentFolder%\nteps32.ocx
- %CurrentFolder%\soapr32.ocs

W32.Flamer has built-in modules to gather information from compromised computers, including:

System information:

- Computer name
- Drive properties, e.g. size
- Printer information
- Registered devices
- Removable media properties
- Running processes

- Services
- System code page
- System drive letter
- Time and time zone information

System network information:

- DHCP information
- DNS information
- Gateway settings
- Host file
- Internet connection information
- IP addresses
- Mail server configuration
- Network adapters and interfaces
- Open ports
- Proxy settings
- Routing table
- Wi-fi network name and profiles

Profiles and cached credentials:

- CoreFTP
- CuteFTP
- EmFTP
- FTP Explorer
- Local computer credentials
- Microsoft Outlook
- Mssh
- NetserveFTP
- RAdmin
- Remote AccessServices
- RoboFTP
- Softx FTP
- South River WebDrive
- TeamViewer
- VNC

Files:

- AutoCAD design data
- Images, including the following formats: BMP, GIF, JPEG, PNG, and TIFF
- Microsoft Office documents, including: Access, Excel, PowerPoint, Publisher, and Word
- Outlook details, including: appointments, emails, meeting requests, and notes

- PDF documents
- URL shortcuts
- Visio diagrams

Files with the following extensions:

- .CSV
- .LNK
- .ORA
- .RDP
- .RTF
- .SSH
- .SSH2
- .TXT

Other information:

- File metadata
- Installed applications
- Network traffic monitoring
- User data and environment

Recommendations

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

- Use a firewall to block all incoming connections from the Internet to services that should not be publicly available. By default, you should deny all incoming connections and only allow services you explicitly want to offer to the outside world.
- 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.
- Ensure that programs and users of the computer use the lowest level of privileges necessary to complete a task. When prompted for a root or UAC password, ensure that the program asking for administration-level access is a legitimate application.
- Disable AutoPlay to prevent the automatic launching of executable files on network and removable drives, and disconnect the drives when not required. If write access is not required, enable read-only mode if the option is available.
- Turn off file sharing if not needed. If file sharing is required, use ACLs and password protection to limit access. Disable anonymous access to shared folders. Grant access only to user accounts with strong passwords to folders that must be shared.
- Turn off and remove unnecessary services. By default, many operating systems install auxiliary services that are not critical. These services are avenues of attack. If they are removed, threats have less avenues of attack.

- If a 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.
- Configure your email server to block or remove email that contains file attachments that are commonly used to spread threats, such as .vbs, .bat, .exe, .pif and .scr files.
- Isolate compromised computers quickly to prevent threats from spreading further. 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.
- If Bluetooth is not required for mobile devices, it should be turned off. If you require its use, ensure that the device's visibility is set to "Hidden" so that it cannot be scanned by other Bluetooth devices. If device pairing must be used, ensure that all devices are set to "Unauthorized", requiring authorization for each connection request. Do not accept applications that are unsigned or sent from unknown sources.
- For further information on the terms used in this document, please refer to the Security Response glossary.

Source: https://web.archive.org/web/20190930124504/https:/www.symantec.com/security-center/writeup/2012-052811-0308-99