EXHIBIT 15

Microsoft

Account ▾ Sign in

Malware Protection Center

Home Security software Malware encyclopedia Our research Help Developers

Follow: TRANSLATE bing

Trojan:Win32/Necurs

Summary Technical information

Microsoft security software detects and removes this family of threats.

This family of malware work together to download other malware, including threats from the Win32/Sirefef and Win32/Medfos families. They can also give a malicious hacker backdoor access and control of your PC.

These threats can be installed at the same time as rogue security software, such as Rogue:Win32/Winwebsec. We have also seen them installed by variants of the Blacole family, the Win32/Beebone family, the Win32/Zbot family, and the Win32/Dorkbot family.

Find out ways that malware can get on your PC.

What to do now

Use the following free Microsoft software to detect and remove this threat:

- Windows Defender for Windows 10 and Windows 8.1, or Microsoft Security Essentials for Windows 7 and Windows Vista
- Microsoft Safety Scanner

You should also run a full scan. A full scan might find other, hidden malware.

Get more help

You can also visit our advanced troubleshooting page or search the Microsoft virus and malware community for more help.

If you're using Windows XP, see our Windows XP end of support page.

Top

I want to...

Get help

Remove difficult malware
Avoid tech support phone scams
See and search the latest threats
Find answers to other problems

Fix my software

Download and update

Submit a file

Alert level: Severe
First detected by definition: 1.139.525.0
Latest detected by definition: 1.207.1383.0 and higher
First detected on: Oct 24, 2012
This entry was first published on: Oct 24, 2012
This entry was updated on: Sep 01, 2014

This threat is also detected as:
Win32/TojanDownloader.Necurs.B (ESET)
Trojan-Dropper.Win32.Necurs.va (Kaspersky)

Provide feedback

Other Microsoft sites
Windows
Office
Surface
Windows Phone
Mobile devices
Xbox
Skype
MSN
Bing
Microsoft Store

Downloads
Download Center
Windows downloads
Office downloads

Support
Support home
Knowledge base
Microsoft community

About
The MMPC
Evaluating our protection
MMPC Privacy Statement
Microsoft
Careers
Citizenship
Company news
Investor relations
Site map

Popular resources
Security and privacy blogs
Security Response Center
Security Intelligence Report
Microsoft Safety & Security Center
Malware Protection Center
Security for IT Pros
Security for developers
Trustworthy Computing

Trojan:Win32/Necurs

Summary Technical information

Threat behavior

Installation

It is downloaded onto your PC via a drive-by download when you access compromised or infected websites.

It can be installed on its own or alongside rogue security software, such as Rogue:Win32/Winwebsec. We have also observed it being installed by variants of the Blacole family, the Win32/Beebone family, the Win32/Zbot family, and the Win32/Dorkbot family.

The malware downloads itself into the folder *%windir%\Installer\<random GUID>*, where <random GUID> is a unique number that identifies your PC, for example *%windir%\Installer\{df3d9e18-342c-8c07-8dab-13e76d8b4322}*.

In the wild, we have seen it use the name *syshost.exe* and one of the following icons:

The threat tries to install itself as an auto-starting Windows service to run automatically after your PC restarts.

If this service installation fails, Trojan:Win32/Necurs changes the following registry entry to ensure that its copy runs at each Windows start:

In subkey: *HKLM\Software\Microsoft\Windows\CurrentVersion\Run*
Sets value: "*syshost32*"
With data: "*%windir%\Installer\<random GUID>\syshost.exe*"

We have also seen some variants of Trojan:Win32/Necurs disabling your firewall.

Payload

Disables security software

Variants of the threat drop and run an additional component, detected as Trojan:WinNT/Necurs.A. This component prevents a large number of security applications from functioning correctly, including applications from the following companies:

- *Agnitum*
- *ALWIL*
- *Avira*
- *Beijing Jiangmin*
- *Beijing Rising*
- *BitDefender*
- *BullGuard*
- *Check Point Software Technologies*
- *CJSC Returnil*
- *Comodo Security Solutions*
- *Doctor Web*
- *ESET*
- *FRISK*
- *G DATA*
- *GRISOFT*
- *Immunet*

I want to...

Get help

Remove difficult malware
Avoid tech support phone scams
See and search the latest threats
Find answers to other problems

Fix my software

Download and update

Submit a file

Alert level: Severe
First detected by definition: 1.139.525.0
Latest detected by definition: 1.207.1383.0 and higher
First detected on: Oct 24, 2012
This entry was first published on: Oct 24, 2012
This entry was updated on: Sep 01, 2014

This threat is also detected as:
Win32/TojanDownloader.Necurs.B (ESET)
Trojan-Dropper.Win32.Necurs.va (Kaspersky)

- *K7 Computing*
- *Kaspersky Lab*
- *Microsoft*
- *NovaShield*
- *Panda*
- *PC Tools*
- *Quick Heal Technologies*
- *Sunbelt*
- *Symantec*
- *VirusBuster*

The component can run on both 32-bit and 64-bit systems.

Contacts remote hosts

Trojan:Win32/Necurs contacts a remote host for command and control instructions via HTTP port 80.

The malware's authors frequently update the list of hosts, however we have seen it trying to connect to the following URLs:

- *hxxp://pbmwtovcjeyvnauw.in/cgi-bin/auth.cgi*
- *hxxp://dnsplast.com/cgi-bin/auth.cgi*

Commonly, malware might contact a remote host for the following purposes:

- To confirm Internet connectivity
- To report a new infection to its author
- To receive configuration or other data
- To download and run arbitrary files (including updates or additional malware)
- To receive instruction from a remote attacker
- To upload data taken from the affected PC, including:
  - The version of Windows you are using
  - Information about the region and language settings of your PC
  - Information about Trojan:Win32/Necurs's installation or configuration

In older variants Trojan:Win32/Necurs can be used to download rogue security software, such as Rogue:Win32/Winwebsec.

Newer variants have been observed receiving and loading a malicious DLL component from the remote host for the purpose of sending spam emails via Gmail.

Trojan:Win32/Necurs saves a copy of the component as *<random GUID>.tmps* to the %TEMP% folder, for example *%TEMP%\7ea7a638-d659-97f6-31a1-3ce2eaf08942.tmps*.

The component gets your PC's external IP address which it sends back to the remote host.

The component then receives information from the remote host which it uses to send spam emails via Gmail.

Additional information

Some variants of Trojan:Win32/Necurs can inject code into all running processes. The injected code is known as a "dead byte"; certain system processes will cause your PC to restart if they are injected with this code.

When dropping the Trojan:WinNT/Necurs.A component on a 64-bit PC, Trojan:Win32/Necurs bypasses kernel patch protection (commonly known as "PatchGuard").

All data sent and received by Trojan:Win32/Necurs is encrypted and signed with an MD5 or SHA1 encryption key.

Related encyclopedia entries

Rogue:Win32/Winwebsec

Trojan:WinNT/Necurs.A

Win32/Sirefef

Win32/Medfos

Blacole

Win32/Beebone

Win32/Dorkbot

Win32/Zbot

Analysis by Tim Liu

Symptoms

System changes

The following could indicate that you have this threat on your PC:

- The presence of the following files:

  %windir%\Installer\<random GUID>\syshost.exe
  %TEMP%\<random GUID>.tmps

  where <random GUID> is a unique number that identifies your PC, for example *{df3d9e18-342c-8c07-8dab-13e76d8b4322}*

- The presence of a file using one of the following icons:

- The presence of the following registry modification:

  In subkey: *HKLM\Software\Microsoft\Windows\CurrentVersion\Run*
  Sets value: *"syshost32"*
  With data: *"%windir%\Installer\<random GUID>\syshost.exe"*

- Your installed security application does not run correctly or does not run at all

Prevention

Take these steps to help prevent infection on your PC.

Top
