EXHIBIT 19

Microsoft

Account ▾ Sign in

Malware Protection Center

Home Security software Malware encyclopedia Our research Help Developers

Follow: TRANSLATE bing

Worm:Win32/Kasidet.A

Summary Technical information

Microsoft security software detects and removes this threat.

This threat can send your sensitive information to a malicious hacker.

It spreads through infected removable drives, such as USB flash drives.

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 hidden malware.

Protect your sensitive information

This threat tries to steal your sensitive and confidential information. If you think your information has been stolen, see:

- What to do if you are a victim of fraud

You should change your passwords after you've removed this threat:

- Create strong passwords

Disable Autorun

This threat tries to use the Windows Autorun function to spread via removable drives, such as USB flash drives. You can disable Autorun to prevent worms from spreading:

- Disable Windows Autorun

Scan removable drives

Remember to scan any removable or portable drives. If you have Microsoft security software, see this topic on our software help page:

- How do I scan a removable drive, such as a USB flash drive?

Enable MAPS

Enable the Microsoft Active Protection Service (MAPS) on your system to protect your enterprise software security infrastructure in the cloud.

1. Check if MAPS is enabled in your Microsoft security product:
   i. Select **Settings** and then select **MAPS**.
   ii. Select **Advanced membership**, then click **Save changes**. With the MAPS option enabled, your Microsoft anti-malware security product can take full advantage of Microsoft's cloud protection service.
2. Join the Microsoft Active Protection Service Community.

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.

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: 1.175.1513.0
Latest detected by definition: 1.203.2809.0 and higher
First detected on: Jun 06, 2014
This entry was first published on: Jun 06, 2014
This entry was updated on: Jun 02, 2015

This threat is also detected as:
Agent4.BSGB (Avira)
TR/Kazy.361966 (AVG)

Worm:Win32/Kasidet.A

Summary Technical information

Threat behavior

Installation

This threat can create a file on your PC using the name of any of the files it finds in the *%SystemRoot%* directory. For example *explorer.exe*, *hh.exe*, or *isuninst.exe*. It creates this file in the following location:

- *%APPDATA% \<PC name>\<file name>*, for example *%APPDATA%\mymachine\explorer.exe*

It creates the following registry entry so that it runs each time you start your PC:

In subkey: *HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*
Sets value: "*%APPDATA%\<PC name>\<file name>*", for example "*%APPDATA%\mymachine\explorer.exe*"
With data: "*<file name>*", for example "explorer.exe"

Spreads through...

It can create the following copies on removable drives, such as USB flash drives:

- *<drive>:\WinUpdate.exe*

It also creates an *autorun.inf* file in the root folder of the removable drive. The file has instructions to launch the malware automatically when the removable drive is connected to a PC with the Autorun feature turned on.

This is a common way for malware to spread. However, *autorun.inf* files on their own are not necessarily a sign of infection; they are also used by legitimate programs.

Payload

Steals your sensitive information

This threat can collect the following information from your PC:

- PC name
- User name
- Operating system version
- Product ID
- Installed antivirus products
- Local IP address

It also checks to see what Windows version you are running and if you have administrator privileges.

Contacts a remote host

The stolen information is sent to the malware's command and control (C&C) server. We have seen it connect to the following servers:

- *abbeytraders.co.uk*
- *bungee-bumper.de*
- *hilarybateman.co.za*
- *lonehillbedandbreakfast.co.za*
- *merseysidedogshome.org*
- *project7.co.za*
- *safarisa.net*
- *xtronics.in*

Once connected to its C&C server the worm can also receive the following commands from a malicious hacker:

- Download and run files

Alert level: Severe
First detected by definition: 1.175.1513.0
Latest detected by definition: 1.203.2809.0 and higher
First detected on: Jun 06, 2014
This entry was first published on: Jun 06, 2014
This entry was updated on: Jun 02, 2015

This threat is also detected as:
Agent4.BSGB (Avira)
TR/Kazy.361966 (AVG)

- Record which keys you press
- Participate in DoS attacks
- Update itself
- Delete files and registry entries
- Find files on your PC
- Modify the system Hosts file
- Visit a URL using a hidden desktop
- Set the interval for retrieving commands from C&C

Additional information

Creates a mutex

This threat can create the following mutexes:

- *n3nmtx*
- *protected_n3utrino*

This can be an infection marker to prevent more than one copy of the threat running on your PC.

Analysis by Jasper Manuel

Symptoms

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

- You have these files:

  %APPDATA%\<PC name>\<file name>, for example *%APPDATA%\mymachine\explorer.exe*

- You see these entries or keys in your registry

  In subkey: *HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*
  Sets value: "*%APPDATA%\<PC name>\<file name>*", for example "*%APPDATA%\mymachine\explorer.exe*"
  With data: "*<file name>*", for example "explorer.exe"

Prevention

Take these steps to help prevent infection on your PC.

Top

Top

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

Microsoft

Contact Us Terms of Use Trademarks Privacy & Cookies About our ads