EXHIBIT 13

Microsoft
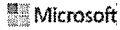
Malware Protection Center

Home   Security software   Malware encyclopedia   Our research   Help   Developers

Follow: ▢ ▢   TRANSLATE
                     b bing

Trojan:Win32/Lethic.I

Summary   Technical information

Microsoft security software detects and removes this threat.

This malware family can give a malicious hacker access and control of your PC.

Find out ways that malware can get on your PC.

What to do now

The following free Microsoft software detects and removes this threat:

- Microsoft Security Essentials or, for Windows 8, Windows Defender
- Microsoft Safety Scanner
- Microsoft Windows Malicious Software Removal Tool

Even if we've already detected and removed this particular threat, running a full scan might find other malware that is hiding on your PC.

You can also visit the Microsoft virus and malware community for more help.

Top

Provide feedback

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: 1.163.1876.0
Latest detected by definition: 1.207.1450.0 and higher
First detected on: Dec 13, 2013
This entry was first published on: Dec 19, 2013
This entry was updated on: Sep 15, 2014

This threat is also detected as:
No known aliases

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   Account ▾   Sign in

Malware Protection Center

Home   Security software   Malware encyclopedia   Our research   Help   Developers

Follow: ▢ ▢   TRANSLATE
                     ▷ bing

Trojan:Win32/Lethic.I

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

Summary   Technical information

Threat behavior

Installation

When it runs, Trojan:Win32/Lethic.I copies itself to *c:\documents and settings\administrator\application data\vfbu.exe*.

The malware modifies the following registry entry so that it runs each time you start your PC:

Adds value: *"Taskman"*
With data: *"c:\documents and settings\administrator\application data\vfbu.exe"*
To subkey: *HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon*

The malware utilizes code injection to hinder detection and removal. When Trojan:Win32/Lethic.I runs, it may inject code into running processes, including the following:

- *explorer.exe*

Payload

Contacts remote host

Trojan:Win32/Lethic.I can contact a remote host at *winsekurityupdat.co.cc* using port 443. Commonly, malware does this to:

- Report a new infection to its author
- Receive configuration or other data
- Download and run files, including updates or other malware
- Receive instruction from a remote hacker
- Upload data taken from your PC

This malware description was produced and published using our automated analysis system's examination of file SHA1 *d655a9a6576e749fcec8f79d44e6fb0429bda51f*.

Symptoms

System changes

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

- The presence of the following files:

  c:\documents and settings\administrator\application data\vfbu.exe

- You see these entries or keys in your registry:

  Adds value: *"Taskman"*
  With data: *"c:\documents and settings\administrator\application data\vfbu.exe"*
  To subkey: *HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon*

Prevention

Take these steps to help prevent infection on your PC.

Top

Alert level: Severe
First detected by definition: 1.163.1876.0
Latest detected by definition: 1.207.1450.0 and higher
First detected on: Dec 13, 2013
This entry was first published on: Dec 19, 2013
This entry was updated on: Sep 15, 2014

This threat is also detected as:
No known aliases

Provide feedback

Other Microsoft sites

Windows

Office

Surface

Windows Phone

Mobile devices

Xbox

Skype

MSN

Bing

Microsoft Store

Downloads

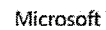Download Center

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   ©2015 Microsoft