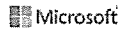


EXHIBIT 16



Account ▼ Sign in

# Malware Protection Center

Home Security software Malware encyclopedia Our research Help Developers

Follow:

TRANSLATE

## Win32/Neurevt

Summary

Technical information

### Threat behavior

#### Installation

When Neurevt gets to run, it drops itself into `%ProgramFiles%\common files` under a randomly named folder with a random file. For example:

- `%ProgramFiles%\common files\beta bot.(2227a280-3aea-1069-a2de-08002b30309d)\kbqipyzt.exe`
- `%ProgramFiles%\common files\chrome browser.(2227a280-3aea-1069-a2de-08002b30309d)\auaucdlve.exe`
- `%ProgramFiles%\common files\taksmgr\uwozkyfqm.exe`
- `%ProgramFiles%\common files\6b4074300\kbqipyzt.exe`
- `%ProgramFiles%\common files\adobeflash.(2227a280-3aea-1069-a2de-08002b30309d)\tjiujsrnb.exe`

It also creates the following registry entries, so that it automatically runs every time Windows starts:

In subkey: `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`

Sets value: "`<random phrase>`"

With data: "`%ProgramFiles%\common files\<random folder name>\<malware file name>.exe`"

For example:

In subkey: `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`

Sets value: "Beta Bot"

With data: "`%ProgramFiles%\common files\beta bot.(2227a280-3aea-1069-a2de-08002b30309d)\kbqipyzt.exe`"

In subkey: `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`

Sets value: "Chrome Browser"

With data: "`%ProgramFiles%\common files\chrome browser.(2227a280-3aea-1069-a2de-08002b30309d)\auaucdlve.exe`"

It disables exception validation for the dropped file by setting:

- Set "DisableExceptionChainValidation" = "" (Unknown), under key `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\<dropped_random_fileName>.exe`

It also creates the following registry entries, as part of its installation process:

In subkey: `HKCU\Software\Win7zip`

Sets value: "Uuid"

With data: "`<This is used to store Sha1 value of (WindowsDirectory, ComputerNameExW & VolumeSerialNumber)>`"

In subkey: `"HKCU\CLSID\{<CLSID>}\<Random_value>\CG1"`

Sets value: "HAL"

With data: "`<This is used to store threat specific state value>`"

In subkey: `"HKCU\CLSID\{<CLSID>}\<Random_value>\CG1"`

Sets value: "BID"

With data: "`<This is used to store SystemTime>`"

#### Payload

##### Connects to a remote server

Once connected, a remote attacker can do the following on your PC:

- Download and run arbitrary files
- Upload files
- Send its stolen data
- Spread through removable drives

### 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

This entry was first published on: Mar 21, 2013

This entry was updated on: Oct 29, 2014

This threat is also detected as:

Trojan.Win32.Jorik.Llac.pqz (Kaspersky)

Win32/Neurevt.A trojan (ESET)

Trojan.Win32.Neurevt (Ikarus)

Trojan.Neurevt!5156 (Rising AV)

- Start or stop programs
- Delete files

#### Disables security software

We have seen this threat disable some security products.

*Analysis by Karthik Selvaraj*

## Symptoms

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

- The presence of the following registry modification:
  - In subkey: *HKCU\Software\Win7zip*  
Value: "Uuid"
- Some security processes are not running as expected because of the following registry changes:
  - In subkey: *HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\vrstrui.exe*  
Sets value: "Debugger"  
With data: "<random characters>\_exe"
  - In subkey: *HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\hijackthis.exe*  
Sets value: "Debugger"  
With data: "<random characters>\_exe"
  - In subkey: *HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\spybotsd.exe*  
Sets value: "Debugger"  
With data: "<random characters>\_exe"
  - In subkey: *HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\housecalllauncher.exe*  
Sets value: "Debugger"  
With data: "<random characters>\_exe"
- "Protected mode" is disabled in Internet Explorer because of the following registry changes:
  - In subkey: *HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1*  
Sets value: "2500"  
With data: "3"
  - In subkey: *HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2*  
Sets value: "2500"  
With data: "3"
  - In subkey: *HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3*  
Sets value: "2500"  
With data: "3"
  - In subkey: *HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4*  
Sets value: "2500"  
With data: "3"

## Prevention







Take these steps to help prevent infection on your PC.

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](#)

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](#)