

Provide feedback

Microsoft						Account → Sign in		
Malwar	e Prote	ction Center				ρ		
	rity software	Malware encyclopedia	Our research	Help	Develope			
Home Seco	nty software	mamare encyclopedia	Our research	Help	Develope			
						Follow: TRANSLATE		
Win32/I	Veurev	†				I want to		
VVIII 152/1	vearev	C				Get help		
	Summary		Technical info	ormatio	n	Remove difficult malware Avoid tech support phone scams See and search the latest threats Find answers to other problems		
		and removes this threat. or PC settings and steal you	r sensitive information	n. It can also	give a	Fix my software		
malicious hacker a Find out ways that	ccess to your PC.					Download and update		
,-		,				Submit a file		
What to o		ire detects and removes this	s threat:			Alert level: Severe This entry was first published on: Mar 21, 2013		
 Windows Defer and Windows \ Microsoft Safet 	/ista	s 10 and Windows 8.1, or M	licrosoft Security Esse	ntials for Wir	ndows 7	This entry was updated on: Oct 29, 2014 This threat is also detected as: Trojan.Win32.Jorik.Llac.pqz (Kaspersky)		
		Ill scan might find other hid	lden malware.			Win32/Neurevt.A trojan (ESET)		
Protect your	sensitive in	nformation				Trojan.Win32.Neurevt (Ikarus) Trojan.Neurevt!5156 (Rising AV)		
		ive and confidential informa	ation. If you think you	· information	ı has			
What to do if y	ou are a victim o	f fraud						
-		after you've removed this	threat:					
Create strong p	oasswords							
Additional re	emediation	steps						
		es to your PC configuration on returning your PC to its p						
		tings for Internet Explorer						
 View hidden an 	d/or system files							
 For Window For Window 								
For other support	ort and help relat	ed articles, go to:						
Windows 8.	1							
 Windows 7 Windows Vi 	sta							
	ecurity TechNet (Center			•			
Get more he	lp							
		ubleshooting page or search	h the Microsoft virus a	and malware				
community for mo		· Windows XP end of suppo	ert page.					
Тор								
10-7-contractor for the distribution of the State Stat		المنظمة المنظمة المنظمة المنظمة						

Mice	osoft				Account 🗸 Sign in		
Malv	ware Protec	ction Cente	r		٥		
Home	Security software	Malware encyclopedia	Our research He	elp Develo	pers		
					Follow: TRANSLATE		
\\/in	22/Nourovd	L			I want to		
Win32/Neurevt					Get help		
	Summary		Technical inform	ation	Remove difficult malware Avoid tech support phone scams See and search the latest threats Find answers to other problems		
Threa	at behavior				•		
Installati	ion				Fix my software Download and update		
	revt gets to run, it drops a a random file. For exam		6\common files under a rand	omly named	Submit a file		
• %Prog.	ramFiles% \common files\ dlve.exe	chrome browser.{2227a28	1069-a2de-08002b30309d)\i 0-3aea-1069-a2de-08002b30		Alert level: Severe This entry was first published on: Mar 21, 2013 This entry was updated on: Oct 29, 2014		
	ramFiles% \ common files ramFiles% \ common files				This threat is also detected as:		
 %ProgramFiles% \ common files\6b4074300\kbqiypzyt.exe %ProgramFiles% \ common files\adobeflash.(2227a280-3aea-1069-o2de-08002b30309d)\tjiujsnjb.exe 				l}\tjiujsnjb.exe	Trojan.Win32Jorik.Llac.pqz (Kaspersky)		
It also creates the following registry entries, so that it automatically runs every time Windows starts: In subkey: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run					Win32/Neurevt.A trojan (ESET)		
					Trojan.Win32.Neurevt (Ikarus) Trojan.Neurevt!5156 (Rising AV)		
Sets value:	:" <random phrase="">" "%ProgramFiles%\comm</random>		omkan ame>\ <malware file="" name="">.</malware>	exe"			
Sets value:	"Beta Bot" "%ProgramFiles%\comm	oft\Windows\CurrentVersi on files\beta bot.{2227a28(on\Run 0-3aea-1069-a2de-08002b30	0309d}			
	HKLM\SOFTWARE\Micros "Chrome Browser"	oft\Windows\CurrentVersi	on\Run				

In subkey: "HKCU\CLSID\{<CLSID>}\<Random_value>\CG1" Sets value: "HAL"

Sets value: "Uuid"

VolumeSerialNumber)>"

\auaucdlve.exe"

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

It disables exception validation for the dropped file by setting:

Options\<dropped_random_fileName>.exe

In subkey: HKCU\Software\Win7zip

Set "DisableExceptionChainValidation" = "" (Unknown), under key
 HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution

With data: "<This is used to store Sha1 value of (WindowsDirecotry, ComputerNameExW &

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

With data: "%ProgramFiles%\common files\chrome browser.{2227a280-3aea-1069-a2de-08002b30309d}

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

Sets value: "BID"
With data: "<This is used to store SystemTime>"

Payload

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

- · 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\rstrui.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"

 $In \ subkey: \textit{HKCU} \ Software \ Microsoft \ Windows \ Current \ Version \ Internet \ Settings \ Zones \ 2$

Sets value: *2500*

With data: "3"

In subkey: HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 Sets value: "2500"

With data: "3"

 $In \ subkey: HKCU \ Software \ Microsoft \ Windows \ Current Version \ Internet \ Settings \ Zones \ 4$

Sets value: "2500"

With data: "3"

Prevention

Take these steps to help prevent infection on your PC.

Тор

Provide feedback

Win32/Neurevt Page 3 of 3

Other Microsoft sites	Downloads	About	Popular resources
Windows Office Surface	Download Center Windows downloads Office downloads	The MMPC Evaluating our protection MMPC Privacy Statement Microsoft	Security and privacy blogs Security Response Center Security Intelligence Report
Windows Phone Mobile devices Xbox Skype	Support Support home Knowledge base Microsoft community	Careers . Citizenship Company news Investor relations Site map	Microsoft Safety & Security Center Malware Protection Center Security for IT Pros Security for developers
MSN Bing Microsoft Store			Trustworthy Computing .

Microsoft

Contact Us Terms of Use Trademarks Privacy & Cookies About our ads ©2015 Microsoft

Win32/Neurevt Page 2 of 2

Other Mici	rosoft sites	Downloads	About -	Popular resources
₽₽ Wind	dows	Download Center	The MMPC	Security and privacy blogs
		Windows downloads	Evaluating our protection	Security Response Center
Offic	e	Office downloads	MMPC Privacy Statement	
☐, Surfa	ice		Microsoft	Security Intelligence Report
Wind	lows Phone		Careers	Microsoft Safety & Security Center
п		Support	Citizenship	14th - P - 1 - 2 - 2 - 2
∐ Mob	ile devices	Support home	Company news	Malware Protection Center
Xbox	:	Knowledge base	Investor relations	Security for IT Pros
Skyp	e	Microsoft community	Site map	Security for developers
MSN	ı			Trustworthy Computing
Bing				
Micro	osoft Store		,	

Microsoft

Contact Us Terms of Use Trademarks Privacy & Cookies About our ads ©2015 Microsoft