

Fake Anti Virus Software

Trading Standards Officers are urging PC users to be wary of the growing problem of fake Anti Virus ("fake AV") products distributed online.

Often distributed using fictitious 'security alert/warning' pop-ups or advertisements, they use scare tactics to dupe users into believing their computers are infected with viruses or other malware. Usually pretending to scan the PC before reporting non-existent threats, they typically prompt users to download and install antivirus software.

However, the fake AV software is actually malware that will likely compromise the security of the PC and the user's personal information, or will generate annoying and intrusive alerts until a payment is made.

Over the past year, web security experts have seen a huge growth in such attacks, with variants growing from less than 1000 to over half a million. Many of the fake alerts appear very plausible, making use of familiar-looking operating system security messages and imagery (see the examples below).

Officers advise users to be vigilant and to protect themselves using reputable, regularly updated security software, and to ensure they are familiar with its operation and alerting methods. Users should be highly suspicious of any security warning messages that have not originated from the antivirus software currently installed on their PC and should not accept any unsolicited offers to scan their PC for malware. Users should verify any warning messages by initiating security scans from within their own antivirus software. **No genuine security warning will ask users to download and install any antivirus software.**

Effective online security is crucial, and in addition to running up-to-date anti-virus, anti-spyware and firewall software, users should ensure their operating systems are kept fully patched by installing published security updates promptly. Internet Explorer 6 users should upgrade their browsers without delay.

Even the best security software cannot protect against gullibility and ignorance, however, and must be supported by caution, user commonsense and awareness of Internet-based threats. For this reason, officers advise PC users to read up on online security via the www.getsafeonline.org. They also encourage email users to follow their advice for avoiding spam (<http://www.staffordshire.gov.uk/NR/ronlyres/3ECA6489-52AC-4A64-A48E-4E44743CB9CB/60121/MicrosoftWordAvoidingSpam.pdf>).

Produced: 23rd July 2010

All our alerts are available in a range of formats and languages, including large print. Please contact Community Development if this would be helpful to you, or to someone you know. Address: 14 Martin Street, Stafford, ST16 2LG



My computer Online Scan - Mozilla Firefox

http://mscussupport.microsoft.com/cussupport.microsoft5.client5.secureserver3.ccf

System Tasks

- View system information
- Add or remove programs
- Change a settings

Other Places

- My Network Places
- My Documents
- Shared Documents
- Control Panel

Details

My Computer System Folder

System scan progress

Shared Documents My Documents

7 trojans

Hard drives

Local Disk (C:) Local Disk (D:)

DVD

DVD-RAM Drive (E:)

Scan complete. 527 threats was found!

Your Computer is Infected!

Threats and actions:

Name	Risk level
Email-Worm.Win32.Net	Critical
Email-Worm.Win32.Myid	Critical
Trojan-Downloader.Win	Critical

Description:
This program is potentially dangerous for your system. Trojan-Downloader stealing passwords, credit cards and other personal information from your computer.

Advice:
You need to remove this threat as soon as possible!

Windows Security Alert

To help protect your computer, Windows Web Security has detected trojans and ready to remove them.

Detected spyware and adware on your computer:

Filename:	Filename:
<input checked="" type="checkbox"/> Address.Trojan	tpservice2.exe
<input checked="" type="checkbox"/> zserv.Transponder.Trojan	ZServ.dll
<input checked="" type="checkbox"/> Wstart.TrojanDownloader	wstart.dll

Remove all Cancel

Spyware is software, which can gather information from user's computer through Internet connection and send them to its creator. Gathered information can be passwords, e-mail addresses and all that data, which is important for you.

Full system cleanup

Total Security

Registration Update Support

System Scan

Protection

Privacy

Update

Settings

Get full real-time protection with Total Security

Total Security : System Scan

Type	Run Type	Name	Details
Trojan	C:/windows/syste...	Win32_Spamta.KG.worm	A multi-component mass-mail...
Trojan	C:/windows/syste...	Trojan.IRCBot.d	A worm that opens an IRC bac...
Trojan	C:/windows/syste...	Trojan.Dropper.MSWord.j	A Microsoft Word macro virus ...
Trojan	C:/windows/syste...	Win32.Clagger.C	This is small Trojan downloader...
Worm	C:/windows/system/	Worm.Bagle.CP	This is a "Bagle" mass-mailer ...
Worm	C:/windows/	Win32.BlackMail.xx	This dangerous worm will destr...
Trojan	hidden autorun	Trojan.Win32.Agent.ado	Trojan downloader that is sprea...
Trojan	autorun	Win32.Outsbot.u	A backdoor Trojan that is remo...
Spyware	autorun	Win32.PerFiler	Win32.PerFiler is designed to r...
Worm	hidden autorun	Win32.Mlevar.a	A Trojan Downloader that mas...
Trojan	C:/windows/	Trojan-Downloader.VBS.Small.oc	This Trojan downloads other fil...
Worm	autorun	Win32.Peacomm.dam	A Trojan Downloader that is sp...

Scan progress

Scanning Stop

Path C:/WINDOWS/in/fppx.PNF

Infections 38

Save Report Remove

the knot unites



VirusDoctor - Online Protection - Mozilla Firefox [#]

File Edit View History Bookmarks Tools Help

http://antivirus-1-scanner.info/scan.php?campaign=mmb%5F783914071&landid=4&country=%COUNTRY%25&rs=6new=1

Most Visited Getting Started Latest Headlines http://keepvid.com/ Live Search Newegg.com - Compu... The Cassandra Page: ... VSubst...

VirusDoctor - Online Protection VirusDoctor - Online Protection VirusDoctor - Online Protection

System Tasks

- View system information
- Add or remove programs
- Change a settings

Other Places

- My Network Places
- My Documents
- Shared Documents
- Control Panel

Details

My Computer
System Folder

System folders

- Shared Documents **6 Viruses found**
- My Documents

Hard drive

- Hard drive (C:) **6 Viruses found**

Security

Windows Security

Checking: c:\...\Local Settings\Temporary Internet Files\Content.IE5\appmgr.dll

Your Computer is Infected **WARNING**

Name	Type	Threat level
Adware.Win32.Winad	Virus	Critical
AdvWare.Hotbar	Virus	High
Trojan-Downloader.Win32.Small.dge	Virus	High
Trojan Horse IRC/Backdoor.SdBot4.FRV	Virus	Medium
W32.Benjamin.Worm	Virus	High

Recommend: Click "Start Protection" button to erase all threats

Start Protection

Antivirus XP 2008

Registration Support

Scan

Start Scan Stop Scan Remove Viruses

Alert ! Your system is infected!

Infected: 1275

Virus Name	Description	Severity	Status
Win32/PSW.OnLine...	Trojan and viruses with keylogging and rootkit cap...	Medium	Infected
Win32/Adware.Seat...	Program is used to direct a browser to display pop...	High	Infected
Win32/IRCBot.AAH	The IRCBot.AAH malware family is a group of bot ...	High	Infected
Win32/IRCBot.AAH	The IRCBot.AAH malware family is a group of bot ...	High	Infected
Win32/IRCBot.AAH	The IRCBot.AAH malware family is a group of bot ...	High	Infected
Win32/Adware.Seat...	Program is used to direct a browser to display pop...	High	Infected
Win32/Adware.Seat...	Program is used to direct a browser to display pop...	High	Infected
Win32/Toolbar.Myw...	Toolbar which includes a search function that dre...	Critical	Infected
Win32/IRCBot.AAH	The IRCBot.AAH malware family is a group of bot ...	High	Infected
Win32/IRCBot.AAH	The IRCBot.AAH malware family is a group of bot ...	High	Infected
Virus Win.CIH	Dangerous virus. It destructs your computer BIOS ...	High	Infected
Win32/IRCBot.AAH	The IRCBot.AAH malware family is a group of bot ...	High	Infected
Win32/Adwe.Vitum...	Virus applications used to deliver advertisements t...	Low	Infected

Known viruses : 102563

Get Maximal Realtime Protection with Antivirus XP 2008

the knot unites



Windows Security Alert

To help protect your computer, Windows Web Security have detected Trojans and ready to remove them.

Detected spyware and adware:

- Adware.Win32.Look2me.ab
- Trojan.Qoologic - Key Logger
- W32.Yaha.B@mm
- AdvWare.Hotbar
- W32.Nimda.3@mm

Spyware is software, which can gather information from user's computer through Internet connection and send them to its creator. Gather information can be passwords, e-mail addresses and all that data, which is important for you.

Name	Type	Threat level
Adware.Win32.Look2me.ab	Wirus	Critical
Trojan.Qoologic - Key Logger	Wirus	High
W32.Yaha.B@mm	Wirus	Critical

Local Disc (C:) 57 trojans

Internet Antivirus Pro Warning!

Harmful and malicious software detected

Online Scanner detected program that may compromise your privacy or damage your computer.

Name	Type	Threat level
Trojan-IM.Win32.Fake	Wirus	Critical
Virus.Win32.Faker.a	Wirus	High
Trojan.PSW.BAT.Cunte	Wirus	Critical

Remove all

Opening setup_build7_195.exe

You have chosen to open

setup_build7_195.exe

which is a: Binary File

from: <http://musicscan-secure.com/>

Would you like to save this file?

Save File Cancel

Opening install14300.exe

You have chosen to open

install14300.exe

which is a: Binary File

from: <http://www.virnet.com/>

Would you like to save this file?

Save File Cancel

Remove All Ignore

Hardware and security errors

Hardware errors
Performance of your PC is low because of changes made by malware. Malicious software may be used by spyware to transfer your private information.

Privacy information errors
Spyware has stolen your personal information. You can see the contents of the information that was stolen.
Country: Philippines
City:
IP Address: 112.201.118.250

[#] The page at <http://antivirus-1-scanner.info> says: [#]

Warning! Your PC is at risk of virus and malware attack.

Your system requires immediate check!
System Security will perform a quick and free scan of your PC for viruses and malicious programs.

OK

