Answered by:

Noel D Paton

living :)

MCC, Partner

www.crashfixpc.co.uk

87,990 Points 6 7 13

Former MVP - 2002 to 2007

Noel D Paton's threads

View Profile

Top related threads

Trojan:Win32/Boaxxe.F

Is there any BPA for procedures ?

Trojan:Win32/Patched.L Can't be Removed

hi any other best way to write procedure

Any drawbacks of using PRINT in stored procedures?

Any procedure for Trojan:Win32/Sirefef.AH?

Windows 7 IT Pro forums > Windows 7 Security

Question

Please redirect to appropriate forum.

Dave Boston

0

Sign in to vote

Moved by Doug Neal Microsoft employee Wednesday, April 18, 2012 2:45 AM Not Related To MBSA (From:MBSA - Microsoft Baseline Security Analyzer)

Thursday, April 12, 2012 6:53 PM

Reply | Quote |

zzboston 0 Points

Answers

Both appear to be variants of the same Java-based exploits.

You should update your Java applications, and uninstall all old versions of the Java runtime.

It would be a good idea to go to a specialist malware-removal forum for asssistance, as such exploits often bring in other forms of malware, which may or may not be found by normal scans.

1

Sign in to vote

Noel Paton | Nil Carborundum Illegitemi | CrashFixPC | The Three-toed Sloth

Marked as answer by zzboston Saturday, April 14, 2012 8:20 PM

Saturday, April 14, 2012 8:05 PM

Reply | Quote |

Noel D Paton living :) (MCC, Partner) 87,990 Points

All replies

redirect what??

SO far you have told us nothing.

Noel Paton | Nil Carborundum Illegitemi | CrashFixPC | The Three-toed Sloth

0
Sign in to vote

Saturday, April 14, 2012 4:59 PM

Reply | Quote |

Noel D Paton living :) (MCC, Partner) 87,990 Points

Wasn't sure this was the correct forum for the question.

These two viruses kept reoccurring together, but scans showed no infections.

Trojan:Win32/Sirefef.AH and Trojan:Win32/Sirefef.AC

A subsequent update cleared them.

Sorry for the vagueness.

Dave Boston

0
Sign in to vote

Saturday, April 14, 2012 6:54 PM

Reply | Quote |

zzboston 0 Points

It still couldn't get much more vague.

What is your OS?

What AV were you using?

have you done scans with any other AV or anti-malware program? What symptoms were you seeing? Do you know how you got infected?

Noel Paton | Nil Carborundum Illegitemi | CrashFixPC | The Three-toed Sloth

0
Sign in to vote

Saturday, April 14, 2012 7:05 PM

Reply | Quote |

Noel D Paton living :) (MCC, Partner) 87,990 Points

Using Windows XP Pro Version 2002, 32 and Security Essentials AV with no other anti-malware.

These two viruses would set off an alert at regular intervals and security essentials would clean them. They showed up both on-line and off. On-line, I got redirected to mostly TV promotional announcements. They may have come from Yahoo 'sidebar' garbage that you can endlessly follow.

0
Sign in to vote

I went through Fix-It and did a Security Scan and they popped up during that and I think that triggered a Security Update that cleared the two. Maybe it was something else. I tried the mal-ware removal tool, but it found nothing.

That they kept reoccurring while off-line, yet the scans found nothing was the most puzzling.

Dave Boston

Saturday, April 14, 2012 7:50 PM

Reply | Quote |

zzboston 0 Points

Both appear to be variants of the same Java-based exploits.

You should update your Java applications, and uninstall all old versions of the Java runtime.

It would be a good idea to go to a specialist malware-removal forum for asssistance, as such exploits often bring in other forms of malware, which may or may not be found by normal scans.

1
Sign in to vote

Noel Paton | Nil Carborundum Illegitemi | CrashFixPC | The Three-toed Sloth

Marked as answer by zzboston Saturday, April 14, 2012 8:20 PM

Saturday, April 14, 2012 8:05 PM

Reply | Quote |

Noel D Paton living :) (MCC, Partner) 87,990 Points

Usually the normal anti-virus can't remove the latest viruses completely. Trojan:Win32/Sirefef.AH is one of them. That's because they are adding new characteristics all the time, so you can't detect by antivirus or antispyware software. In such circumstance, manual removal with expertise is required. If you're not professional with system files, you can search "computer expert online 24/7" from Google and get an online technician to help you fix it. Or if you're skillful enough, you can try this guide.

0
Sign in to vote

Edited by John_008 Saturday, April 21, 2012 12:17 AM

Saturday, April 21, 2012 12:16 AM

Reply | Quote |

John_008 0 Points

1
Sign in to vote

The Sirefef family of trojans often come bundled with rootkits, no easy matter to remove without expert trained help. The ZeroAccess rootkit is one of the variants of this malware.
Reference Trojan:Win32/Sirefef.AH
http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Trojan%3aWin32%2fSirefef.AH

It is safest to restore your system from a recent clean disk-mirror-image backup or to wipe the system and do a clean Windows install.

Free expert-guided help on malware removal may be obtained at specialty forums such as the following:
http://spywarehammer.com/simplemachinesforum/index.php?board=10.0
http://spywarehammer.com/simplemachinesforum/index.php?topic=87.0 (how to post guide)
http://aumha.net/viewforum.php?f=30
http://forum.malwareremoval.com/viewforum.php?f=11
http://www.bleepingcomputer.com/forums/forum22.html
http://www.spywareinfoforum.com/index.php?showforum=18
http://www.spywarewarrior.com/viewforum.php?f=5
http://forums.spybot.info/forumdisplay.php?f=22

Maurice Naggar ~ MS-MVP (Oct 2002 - Sept 2010) DTS-L

Saturday, April 21, 2012 10:53 AM

Reply | Quote |

Maurice N 155 Points

<waves> Hi, Maurice! - long time no see!

Noel Paton | Nil Carborundum Illegitemi | CrashFixPC | The Three-toed Sloth

0
Sign in to vote

Saturday, April 21, 2012 4:34 PM

Reply | Quote |

Noel D Paton living :) (MCC, Partner) 87,990 Points

{{ waves-back}} Hi, Noel !

Maurice Naggar ~ MS-MVP (Oct 2002 - Sept 2010) DTS-L

0
Sign in to vote

Saturday, April 21, 2012 5:45 PM

Reply | Quote |

Maurice N 155 Points