Win32/Opachki.A - Trojan that removes Zeus (but it is not benign)

contagiodump.blogspot.com/2009/11/win32opachkia-trojan-that-removes-zeus.html

Win32/Opachki.A --Virustotal-all antivirus names for it. The real tragedy is in those http://www.threatexpert.com/report.aspx?md5=87a2583de6f6fbb5104e0433e89b1bcf

nsrbgxod.bak created by Opachki http://www.threatexpert.com/report.aspx?md5=87a2583de6f6fbb5104e0433e89b1bcf and nsrbgxod.bak created by Zeus/ZBot http://www.threatexpert.com/report.aspx?md5=00f2fd5e2c125965c188754f04da576c

Different hash

SecureWorks Opachki Trojan Analysis
http://www.secureworks.com/research/threats/opachki

Threatexpert

Submission details:

Filename(s)

1 %Temp%\nsrbgxod.bak

0 bytes

MD5: 0xD41D8CD98F00B204E9800998ECF8427E
SHA-1: 0xDA39A3EE5E6B4B0D3255BFEF95601890AFD80709
2 %UserProfile%\protect.dll
%Programs%Startup\ChkDisk.dll
%System%\autochk.dll

[file and pathname of the sample #1]

24,064 bytes

MD5: 0x87A2583DE6F6FBB5104E0433E89B1BCF

SHA-1: 0x6048D36DB2207A1CEA877742C9403A816D711C6D

Mal/UnkPack-Fam
[Sophos]

TrojanDropper:Win32/Opachki.A

[Microsoft]

Trojan-Dropper.Win32.Opachki

[Ikarus]

3 %Programs%\Startup\ChkDisk.lnk

655 bytes

MD5: 0x6F61156F14AEED438770D31391E67EC9

SHA-1: 0x277B806CEC1AEDE9F9B934B7DD655D0BBB542597

Read more - Update March 2010