CVE-2010-2568 keylogger Win32/Chymine.A

contagiodump.blogspot.com/2010/07/cve-2010-2568-keylogger-win32chyminea.html


EXTRAEXPLOIT

EVERYTHING OR NOTHING

TUESDAY, JULY 27, 2010

Win32/Chymine.A

Reading something about this trojan, which use the CVE-2010-2568 as spreading vector, I found that
the binary is located at hxxxp://205.209.171.119/bin.exe. The process try to

CONTACTS

email: extraexploit(at) gmail.com

CVE-2010-2568 - Win32/Chymine.A

Windows Shell in Microsoft Windows XP SP3, Server 2003 SP2, Vista SP1 and SP2, Server 2008 SP2 and R2, and Windows 7 allows local users or remote attackers to execute arbitrary code via a crafted (1) .LNK or (2) .PIF shortcut file, which is not properly handled during icon display in Windows Explorer, as demonstrated in the wild in July 2010, and originally reported for malware that leverages CVE-2010-2772 in Siemens WinCC SCADA systems

The credit for this post goes to Extraexploit from extraexploit.blogspot.com. See additional details on his blog


EXTRAEXPLOIT

EVERYTHING OR NOTHING

TUESDAY, JULY 27, 2010

Win32/Chymine.A

Reading something about this trojan, which use the CVE-2010-2568 as spreading vector, I found that
the binary is located at hxxxp://205.209.171.119/bin.exe. The process try to

CONTACTS

email: extraexploit(at) gmail.com


Download bin.exe as a password protected archive (contact me if you need the password)

ESET New malicious LNKs: here we go…

> "At the time of analysis, this threat downloads and install a key stroke logger which we detect as Win32/Spy.Agent.NSO trojan. The server used to deliver the components used in this attack is presently located in the US, but the IP is assigned to a customer in China. "

F-Secure Win32/Chymine-A

Result: 30/41 (73.18%)
http://www.virustotal.com/analisis/96ec6dc227b3110807d1dd183e802aa4f1271f79cdeaa50e9172065fd5c311f2-1280489604
Antivirus Version Last Update Result
AhnLab-V3 2010.07.30.00 2010.07.29 Dropper/Win32.Chymine
AntiVir 8.2.4.32 2010.07.30 TR/Dldr.Tiny.cmq
Antiy-AVL 2.0.3.7 2010.07.30 Trojan/Win32.Tiny.gen
Avast 4.8.1351.0 2010.07.30 Win32:Malware-gen
Avast5 5.0.332.0 2010.07.30 Win32:Malware-gen
AVG 9.0.0.851 2010.07.30 PSW.Generic8.GRF
BitDefender 7.2 2010.07.30 Trojan.Autorun.ATB
Comodo 5586 2010.07.30 TrojWare.Win32.AntiAV.~G
DrWeb 5.0.2.03300 2010.07.30 Trojan.KeyLogger.8141
Emsisoft 5.0.0.34 2010.07.30 Trojan-Downloader.Win32.Tiny!IK
F-Secure 9.0.15370.0 2010.07.30 Trojan-Spy:W32/Chymine.A
Fortinet 4.1.143.0 2010.07.30 W32/Tiny.CMQ!tr.dldr
GData 21 2010.07.30 Trojan.Autorun.ATB
Ikarus T3.1.1.84.0 2010.07.30 Trojan-Downloader.Win32.Tiny
Jiangmin 13.0.900 2010.07.29 TrojanSpy.KeyLogger.cqyg
Kaspersky 7.0.0.125 2010.07.30 Trojan-Downloader.Win32.Tiny.cmq
McAfee 5.400.0.1158 2010.07.30 Generic Downloader.x!eas
McAfee-GW-Edition 2010.1 2010.07.30 Heuristic.BehavesLike.Win32.CodeInjection.H
Microsoft 1.6004 2010.07.30 Trojan:Win32/Chymine.A
NOD32 5325 2010.07.30 Win32/Spy.Agent.NSO
nProtect 2010-07-30.02 2010.07.30 Trojan.Autorun.ATB
Panda 10.0.2.7 2010.07.29 Trj/ChymineLNK.A
PCTools 7.0.3.5 2010.07.30 Net-Worm.SillyFDC
Rising 22.58.04.05 2010.07.30 Trojan.Win32.Generic.52214029
Sophos 4.56.0 2010.07.30 Mal/Chymin-A
Sunbelt 6663 2010.07.30 Trojan.Win32.Generic!BT
Symantec 20101.1.1.7 2010.07.30 W32.SillyFDC
VBA32 3.12.12.7 2010.07.30 Trojan-Downloader.Tiny.cmq
ViRobot 2010.7.30.3963 2010.07.30 Trojan.Win32.S.Downloader.131584
VirusBuster 5.0.27.0 2010.07.29 Trojan.DL.Tiny.DPT
Additional information
File size: 131584 bytes
MD5...: 3515b1f2ae991fcd64ff4e3b664625c0