network security investigations

- Malware Analysis
- Forensics
- Intrusion Detection
- Incident Response
- (866) 221-6380
- Sales@netscty.com

This is a report from a file uploaded to our Sandbox. The data from our Sandbox has recently been updated to remove benign files and data, you will not see a list of all open ports or running processes, instead we are only listing those processes and files that are directly relevant to the binary (malware) that was uploaded on our website. We hope this make our reports easier to read and more useful to you.

We welcome your comments and suggestions; please send them to the email address above.

Report Contains Output Reference to file: **58da6e3221915e1947a7dd0ff6c2b7e7**
MD5 Hash: **58da6e3221915e1947a7dd0ff6c2b7e7**

Creates Files	Sniffer Capability	Botnet Activity	Beacons Out/Download Capable	Malware Downloaded	Key Logging Capability	Opens Listening Port	Creates SMTP Traffic	Modifies MBR	SQL Attack	FTP Remote Access	Attempts lateral connection	ADS
YES	NO	NO	YES	NO	NO	YES	NO	NO	NO	YES	NO	NO

Anti-Virus Tool	Result
NOD32	probably unknown NewHeur_PE
Norman	W32/Downloader
Kaspersky	Heur.Downloader
BitDefender	BehavesLike:Win32.Malware
F-Secure	BehavesLike:Win32.Malware
DrWeb	DLOADER.Trojan
AntiVir	HEUR/Malware
McAfee-GW-Edition	Heuristic.Malware
GData	BehavesLike:Win32.Malware
VBA32	suspected of Win32.Trojan.Downloader (http://...)
Rising	Trojan.DL.Win32.Downloader.GEN

VirusTotal link for: 58da6e3221915e1947a7dd0ff6c2b7e7

Files created on the File System - Count: 1

Back To Top

File Name:	fuckupspawn.txt
File Path:	fuckupspawn.txt
MD5 Hash:	af7071753e47c0a18f4e8fe1512817b9
SSDeep Hash:	12:fSL4L4L4L4L4L4L4L4L4L4L4L4L4L4L4L4L4L4L4L4L4L4L4L4L4L4L4L4L4L4L4Lh:fc

Files which were modified on the File System with the corresponding MD5SUM and Path - Count: 11

File Name:	NTUSER.DAT
File Path:	Documents and Settings/Administrator
MD5 Hash:	0d4a5b7d5461ebbf3bcd8c3c3f917beb
File Name:	NTUSER.DAT
File Path:	Documents and Settings/LocalService
MD5 Hash:	de067db881a2923abf4ae396e35d9674
File Name:	NTUSER.DAT
File Path:	Documents and Settings/NetworkService
MD5 Hash:	92174d1a84de7d673302e9cba57e5ccb

Files which were modified on the File System with the corresponding MD5SUM and Path - Count: 11

File Name:	AppEvent.Evt
File Path:	WINDOWS/system32/config
MD5 Hash:	badd5baf65170a3d893c5a2254c660b7
File Name:	default
File Path:	WINDOWS/system32/config
MD5 Hash:	8562b8d0218007ae9d315bd5faa34886
File Name:	SAM
File Path:	WINDOWS/system32/config
MD5 Hash:	6eb1e6ed8cd0c25ea33aad0770981da7
File Name:	SECURITY
File Path:	WINDOWS/system32/config
MD5 Hash:	274349eac7b77a6c69fb535aa486c604
File Name:	software
File Path:	WINDOWS/system32/config
MD5 Hash:	2d11316f1443a8b46d443ff79fec3ac9
File Name:	SysEvent.Evt
File Path:	WINDOWS/system32/config
MD5 Hash:	a831be89e31dfd25249e1b32233d5d34
File Name:	system
File Path:	WINDOWS/system32/config
MD5 Hash:	cbf69c6fc854e4970af4e38911c61b2b
File Name:	wbemess.lo_
File Path:	WINDOWS/system32/wbem/Logs
MD5 Hash:	66590dc0a28078691a71a61ed787e051

New Open and/or Listening Ports (MPORT) - Count: 2

Back To Top

Protocol	LocalIpPort	RemoteIpPort	Service	Status
0.0.0.0:1044	TCP	0.0.0.0:2272	LISTENING	58da6e3221915e1947a7dd0ff6c2b7e7:1076
10.10.10.7:1042	TCP	4.3.2.230:21	ESTABLISHED	58da6e3221915e1947a7dd0ff6c2b7e7:1076

New Open Sockets in Memory - Count: 3

Back To Top

Pid	Port	Proto
1076	1042	6
1076	1034	17
1076	1044	6

New Processes in Memory - Count: 1

Back To Top

Pid	PPid	Name
1076	1780	58da6e3221915e1947a7dd0ff6c2b7e7

New Connections in Memory - Count: 2

Back To Top

LocalIpPort	RemoteIpPort	Pid
10.10.10.7:1038	4.3.2.91:80	1076
10.10.10.7:1042	4.3.2.230:21	1076

New Opened files which were contained within Memory - Count: 8

Back To Top

Data
File \AsyncConnectHlp
File \Documents and Settings\Administrator\Cookies\index.dat
File \Documents and Settings\Administrator\Local Settings\Application Data\Microsoft\Portable Devices
File \Documents and Settings\Administrator\Local Settings\History\History.IE5\index.dat
File \Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\index.dat
File \System Volume Information_restore{307E7B41-0455-430D-B7AD-0176BCF9FE0E}\RP16\change.log
File \System Volume Information\tracking.log
File \fuckupspawn.txt

Strings Command executed on Processes contained within Memory - Count: 4

Back To Top

Data
FtpPutFileA
c:\Documents and Settings\Rob\My Documents\Visual Studio 2008\Projects\FtpKeylogger\Release\FtpKeylogger.pdb
ftp.drivehq.com
http://xdl.x10hosting.com/svch0st.exe

Malicious DNS Queries, HTTP Traffic, and GET Commands, etc. - Count: 4

Back To Top

Data
xdl.x10hosting.com/svch0st.exe
ftp.drivehq.com
xdl.x10hosting.com
/svch0st.exe

Malicious FTP Traffic - Count: 11

Back To Top

Data
Connection from 10.10.10.7
USER publicowned
PASS secretpassword
Connection from 10.10.10.7
USER publicowned
PASS secretpassword
TYPE I
PASV
TYPE I
PORT 10,10,10,7,4,20
STOR Test.txt

Potentially Malicious Changes in System Registry File - Count: 2

Back To Top

Data
[system\ControlSet001\Services\Eventlog\Application\Microsoft H.323 Telephony Service Provider]
"EventMessageFile"="C:\\WINDOWS\\System32\\h323.tsp"

Potentially Malicious Changes in Software Registry File - Count: 1

Back To Top

Data
[software\Microsoft\DownloadManager]

This is an automated report provided free of charge, it was generated in part by a custom script and utilizes the following tools: the Reusable Malware Analysis Net (Truman*) server, Norton Anti-Virus, Malwarebytes Anti-malware*, Sysinternals Tools, Ngrep, Tcpdump, Sed Editor, Awk, Volatile Systems Volatitlity Framework, SSdeep, MD5sum, MS Office and Adobe Acrobat . If you would like a full forensic examination that would tell you more about how the malware was placed on the system and if additional malicious applications are still there please contact us. In some cases we can determine if data was exfiltrated, but data from your other network devices is sometimes necessary. (example: firewalls and IDS)

* TRUMAN: Authored by Mr. Joe Stewart under the General Public License.
* VirusTotal is a service developed by Hispasec Sistemas that analyzes suspicious files and URLs enabling the identification of viruses, worms, trojans and other kinds of malicious content detected by antivirus engines and web analysis toolbars.
* Ngrep: Authored by Jordan Ritter Norton Anti Virus: Product of Symantec Corp.
* Malwarebytes Anti-Malware, Product fo Malwarebytes Corporation Windows Sysinterals Tools, Sysinternals was created in 1996 by Mark Russinovich and Bryce Cogswell to host their advanced system utilities and technical information. Microsoft acquired Sysinternals in July, 2006
* Virus Total checks multiple AV products, here is a list of all the AV applications and versions they are currently using. If our report does not show an AV application above, it did not hit on the binary submitted.