

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: **d24e3ea4473659cf53853c97eb1fd418**

MD5 Hash: **d24e3ea4473659cf53853c97eb1fd418**

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	YES	YES	NO	NO	NO	NO	NO	NO

Anti-Virus Tool	Result
McAfee+Artemis	Generic BackDoor
McAfee	Generic BackDoor
K7AntiVirus	Backdoor.Win32.Poison.wcs
VirusBuster	Worm.Autoit.TQ
NOD32	Win32/IRCBot.AGP
F-Prot	W32/BackdoorX.DMQX
a-squared	Backdoor.Win32.Poison!IK
Norman	W32/Smalldoor.dam
Avast	Win32:VB-LFH
ClamAV	Trojan.Poison-98
Kaspersky	Backdoor.Win32.Poison.wcs
Comodo	Backdoor.Win32.Poison.wcs
DrWeb	Trojan.Rent.14
AntiVir	TR/Dropper.Gen
TrendMicro	TROJ_AGMH.A
McAfee-GW-Edition	Trojan.Dropper.Gen
Sophos	Mal/Generic-A
Authentium	W32/BackdoorX.DMQX
Microsoft	Backdoor:Win32/Buzus.D
GData	Win32:Trojan-gen
VBA32	Backdoor.Win32.Poison.wcs
Sunbelt	Trojan.Win32.Generic!BT
PCTools	Backdoor.Poison.AMX
Ikarus	Backdoor.Win32.Poison
AVG	Generic_c.AUGB
Panda	Bck/Poison.F

VirusTotal link for: [d24e3ea4473659cf53853c97eb1fd418](https://www.virustotal.com/analysis/d24e3ea4473659cf53853c97eb1fd418)

Files created on the File System - Count: 5

[Back To Top](#)

File Name:	son.exe
File Path:	Documents and Settings/Administrator/Local Settings/Temp
MD5 Hash:	0e92f0a27b341a253c42256efc823008
SSDeep Hash:	6144:OIEpvVLxqermfw0oHnKhKI+xA4Ah7InjtNu+CTS15:OHvVLxXro5oFVxAdh71byO
File Name:	KB8888239.log
File Path:	WINDOWS
MD5 Hash:	1751f231b3514f9ab5c10ae7da84cc47
SSDeep Hash:	24:Wx+3zqeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee+:Wck

Files created on the File System - Count: 5

[Back To Top](#)

File Name:	cmsetac.dll
File Path:	WINDOWS
MD5 Hash:	2dbb52ae0e5d1e5aec756ce5ee1f537e
SSDeep Hash:	768:C+aoi6qZOpQB5ZpOc06HCMN9GT6RJ5BHUEy2YEZZEo:C+av6qZ4QxpP0AtNfRJ5BHxY
File Name:	mstwain32.exe
File Path:	WINDOWS
MD5 Hash:	0e92f0a27b341a253c42256efc823008
SSDeep Hash:	6144:OIEpvVLxqermfw0oHnKhKI+xA4Ah7InjtNu+CTS15:OHvVLxXro5oFVxAdh71byO
File Name:	ntdtcstp.dll
File Path:	WINDOWS
MD5 Hash:	67587e25a971a141628d7f07bd40ffa0
SSDeep Hash:	96:nPI4WiJu8aFwiFth01RI532eJWahK4oDIImBx:ndW0u8/Jh0DI532eJWao4i/

Files which were modified on the File System with the corresponding MD5SUM and Path - Count: 28

File Name:	NTUSER.DAT
File Path:	Documents and Settings/Administrator
MD5 Hash:	0ab75fe4704ff19e793ffd7d693058ce
File Name:	NTUSER.DAT
File Path:	Documents and Settings/LocalService
MD5 Hash:	507078a0769d740b067dfd28e22776e1
File Name:	NTUSER.DAT
File Path:	Documents and Settings/NetworkService
MD5 Hash:	cabf344e784d11e21837d7ed26d59f76
File Name:	RestorePointSize
File Path:	System Volume Information/_restore{307E7B41-0455-430D-B7AD-0176BCF9FE0E}/RP10
MD5 Hash:	b857c0221e06a8265c5fa75a07d9c856
File Name:	rp.log
File Path:	System Volume Information/_restore{307E7B41-0455-430D-B7AD-0176BCF9FE0E}/RP10
MD5 Hash:	a27848610b336d24f24374b2424e9cbc
File Name:	RestorePointSize
File Path:	System Volume Information/_restore{307E7B41-0455-430D-B7AD-0176BCF9FE0E}/RP11
MD5 Hash:	4ebd314ff332c7d5235a229ea4ceaebb
File Name:	rp.log
File Path:	System Volume Information/_restore{307E7B41-0455-430D-B7AD-0176BCF9FE0E}/RP11
MD5 Hash:	8cee4e990eecffd2b9b1b1121159185f
File Name:	RestorePointSize
File Path:	System Volume Information/_restore{307E7B41-0455-430D-B7AD-0176BCF9FE0E}/RP12
MD5 Hash:	f6ea513b7642390631ca299d3388ea52
File Name:	rp.log
File Path:	System Volume Information/_restore{307E7B41-0455-430D-B7AD-0176BCF9FE0E}/RP12
MD5 Hash:	958ac719393dfa9197b6ad16106ea952

Files which were modified on the File System with the corresponding MD5SUM and Path - Count: 28

File Name:	RestorePointSize
File Path:	System Volume Information/_restore{307E7B41-0455-430D-B7AD-0176BCF9FE0E}/RP13
MD5 Hash:	37f4a55f6e658e6bafb0843e666b562d
File Name:	rp.log
File Path:	System Volume Information/_restore{307E7B41-0455-430D-B7AD-0176BCF9FE0E}/RP13
MD5 Hash:	18911fc4d08ea53ce0e0f328dc32de1c
File Name:	RestorePointSize
File Path:	System Volume Information/_restore{307E7B41-0455-430D-B7AD-0176BCF9FE0E}/RP14
MD5 Hash:	4a906308ad1802beb50a8138f9ec2e3a
File Name:	rp.log
File Path:	System Volume Information/_restore{307E7B41-0455-430D-B7AD-0176BCF9FE0E}/RP14
MD5 Hash:	8e9b4a390e23951ee1a56d6a02ad5394
File Name:	RestorePointSize
File Path:	System Volume Information/_restore{307E7B41-0455-430D-B7AD-0176BCF9FE0E}/RP15
MD5 Hash:	375688ce6dca64ba88c8263fb1aa21d2
File Name:	rp.log
File Path:	System Volume Information/_restore{307E7B41-0455-430D-B7AD-0176BCF9FE0E}/RP15
MD5 Hash:	e7a6446b38d3e54ebca3f162eef596eb
File Name:	RestorePointSize
File Path:	System Volume Information/_restore{307E7B41-0455-430D-B7AD-0176BCF9FE0E}/RP16
MD5 Hash:	8f2e9bc99ce5262ae84ff35455e34255
File Name:	rp.log
File Path:	System Volume Information/_restore{307E7B41-0455-430D-B7AD-0176BCF9FE0E}/RP16
MD5 Hash:	a05351d3622b43dad5ab7d3996baa6b3
File Name:	RestorePointSize
File Path:	System Volume Information/_restore{307E7B41-0455-430D-B7AD-0176BCF9FE0E}/RP9
MD5 Hash:	b7dc123efb930ae509005aa9cf14f58a
File Name:	rp.log
File Path:	System Volume Information/_restore{307E7B41-0455-430D-B7AD-0176BCF9FE0E}/RP9
MD5 Hash:	cf2730df8e940522f25e178682e75889
File Name:	AppEvent.Evt
File Path:	WINDOWS/system32/config
MD5 Hash:	ecbffb821fbac8870f68054f2484d660
File Name:	default
File Path:	WINDOWS/system32/config
MD5 Hash:	4bfcd5bc5669ed54fac3ed85bf6f5fd4
File Name:	SAM
File Path:	WINDOWS/system32/config
MD5 Hash:	d64cacab007403635f70d1248fee4b39
File Name:	SECURITY
File Path:	WINDOWS/system32/config
MD5 Hash:	60bfc2bba6ec8eda0d49fa41a413193b

Files which were modified on the File System with the corresponding MD5SUM and Path - Count: 28

File Name:	software
File Path:	WINDOWS/system32/config
MD5 Hash:	44214cfa248c0a3a15552e24f69b0cc4
File Name:	SysEvent.Evt
File Path:	WINDOWS/system32/config
MD5 Hash:	4a0f375eb7d84259406493d2810aae1d
File Name:	system
File Path:	WINDOWS/system32/config
MD5 Hash:	6fe2546010ffe11b0d82e470edd1324f
File Name:	Preferred
File Path:	WINDOWS/system32/Microsoft/Protect/S-1-5-18/User
MD5 Hash:	7bc2736a7375a2bbcce3257150d8d70a
File Name:	wbemess.lo_
File Path:	WINDOWS/system32/wbem/Logs
MD5 Hash:	f3e0f1d47465689064a81f01b72135b8

New Open and/or Listening Ports (MPORT) - Count: 1

[Back To Top](#)

Protocol	LocalIpPort	RemoteIpPort	Service	Status
10.10.10.7:1039	TCP	4.3.2.170:15963	ESTABLISHED	mstwain32.exe:360

New Open Sockets in Memory - Count: 1

[Back To Top](#)

Pid	Port	Proto
360	1039	6

New Processes in Memory - Count: 1

[Back To Top](#)

Pid	PPid	Name
360	1496	mstwain32.exe

New Connections in Memory - Count: 1

[Back To Top](#)

LocalIpPort	RemoteIpPort	Pid
10.10.10.7:1039	4.3.2.170:15963	360

New Opened files which were contained within Memory - Count: 5

[Back To Top](#)

Data

File \AsyncConnectHlp
File \AsyncSelectHlp
File \Documents and Settings\Administrator\Local Settings\Application Data\Microsoft\Portable Devices
File \System Volume Information_restore{307E7B41-0455-430D-B7AD-0176BCF9FE0E}\RP16\change.log
File \System Volume Information\tracking.log

Strings Command executed on Processes contained within Memory - Count: 6

[Back To Top](#)

Data

true
getftppasswords
http://www.turkojan.com
mailpasswords
webcoliq.no-ip.org
|rdr|\plug_ins\sendmail.api

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

[Back To Top](#)

Data

webcoliq.no-ip.org

Potentially Malicious Changes in NTUSER.DAT File - Count: 3

[Back To Top](#)

Data

"mstwain32"="C:\\WINDOWS\\mstwain32.exe"
"C:\\DOCUME~1\\ADMINI~1\\LOCALS~1\\Temp\\son.exe"=" "
"C:\\WINDOWS\\mstwain32.exe"=" "

Keylogger - Count: 1

[Back To Top](#)

Data

WINDOWS/KB8888239.log

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.