

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: **dwm.exe**
 MD5 Hash: **49c390df183a139f3d4abf3b850e0898**

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
NO	YES	NO	YES	NO	NO	NO	NO	NO	NO	NO	NO	NO

Anti-Virus Tool	Result
nProtect	Trojan-Proxy/W32.Agent.69632.M
CAT-QuickHeal	TrojanProxy.Agent.clv
McAfee	Generic.dx!tjc
K7AntiVirus	Proxy-Program
TheHacker	Trojan/Proxy.Agent.clv
VirusBuster	Trojan.PR.Agent!O3wQM4HdGp4
NOD32	probably unknown NewHeur_PE
F-Prot	W32/MalwareF.HIFV
Symantec	Backdoor.Trojan
Norman	W32/Suspicious_Gen2.DTXFO
TrendMicro-HouseCall	TROJ_PROXY.ALE
Avast	Win32:Malware-gen
Kaspersky	Trojan-Proxy.Win32.Agent.clv
BitDefender	Trojan.Agent.23063
ViRobot	Trojan.Win32.S.Proxy.69632.A
Sophos	Troj/Agent-NLL
Comodo	Heur.Suspicious
F-Secure	Trojan.Agent.23063
VIPRE	BehavesLike.Win32.Malware.rwx (mx-v)
AntiVir	TR/Agent.23063
TrendMicro	TROJ_PROXY.ALE
McAfee-GW-Edition	Generic.dx!tjc
Emsisoft	Trojan-Proxy.Win32.Agent!IK
Jiangmin	TrojanProxy.Agent.cku
Antiy-AVL	Trojan/Win32.Agent.gen
Microsoft	Trojan:Win32/Orsam!rts
Prevx	Medium Risk Malware
GData	Trojan.Agent.23063
Commtouch	W32/MalwareF.HIFV
AhnLab-V3	Win-Trojan/Agent.69632.AJG
VBA32	TrojanProxy.Agent.clv
PCTools	Backdoor.Trojan
Ikarus	Trojan-Proxy.Win32.Agent
Fortinet	W32/Agent.NLL!tr
AVG	Proxy.AKRX
Panda	Trj/CI.A
Avast5	Win32:Malware-gen

VirusTotal link for: [49c390df183a139f3d4abf3b850e0898](https://www.virustotal.com/49c390df183a139f3d4abf3b850e0898)

Files which were modified on the File System with the corresponding MD5SUM and Path - Count: 10

File Name:	NTUSER.DAT
File Path:	Documents and Settings/Administrator
MD5 Hash:	78daac887ac23a0af88d55492a8ac39c
File Name:	NTUSER.DAT
File Path:	Documents and Settings/LocalService
MD5 Hash:	48bab7f41778e291410b1795958ff99b
File Name:	NTUSER.DAT
File Path:	Documents and Settings/NetworkService
MD5 Hash:	aeec5802bec9277b02218b4260db725
File Name:	AppEvent.Evt
File Path:	WINDOWS/system32/config
MD5 Hash:	8a2284820583dec097428f7c60c136be
File Name:	default
File Path:	WINDOWS/system32/config
MD5 Hash:	c0bc8de6f0a80cd0498787bc9536db56
File Name:	SAM
File Path:	WINDOWS/system32/config
MD5 Hash:	c94567cc83c97ad0affe6d31d7234df7
File Name:	SECURITY
File Path:	WINDOWS/system32/config
MD5 Hash:	d6407db033f1ada3ee4f8f04db415631
File Name:	software
File Path:	WINDOWS/system32/config
MD5 Hash:	c4475f9af118eb88f078d888d6f18410
File Name:	SysEvent.Evt
File Path:	WINDOWS/system32/config
MD5 Hash:	aaa68b00e6f01bd8cbd0cf201ca82ce7
File Name:	system
File Path:	WINDOWS/system32/config
MD5 Hash:	dd07c839c7af700fdacd98be30160df7

New Open Sockets in Memory - Count: 1

[Back To Top](#)

Pid	Port	Proto
908	0	0

New Processes in Memory - Count: 1

[Back To Top](#)

Pid	PPid	Name
908	1856	dwm.exe

New Connections in Memory - Count: 3

[Back To Top](#)

LocalIpPort	RemotelpPort	Pid
10.10.10.7:1037	62.122.73.222:5689	908
10.10.10.7:1041	62.122.73.222:5689	908
10.10.10.7:1038	62.122.73.222:5689	908

New Opened files which were contained within Memory - Count: 2

[Back To Top](#)

Data

File \0
 File \Documents and Settings\Administrator\Local Settings\Application Data\Microsoft\Portable Devices

Potentially Malicious Changes in Software Registry File - Count: 1

[Back To Top](#)

Data

"dmw"="C:\\WINDOWS\\system32\\dwm.exe"

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 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.