

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: **767cfbc1723c44aad9131caf8fd7c628**

MD5 Hash: **767cfbc1723c44aad9131caf8fd7c628**

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

Anti-Virus Tool	Result
McAfee+Artemis	Artemis!767CFBC1723C
TheHacker	Trojan/Mebroot.bo
NOD32	a variant of Win32/Mebroot.BO
F-Prot	W32/Sinowal.B.gen!Eldorado
a-squared	Backdoor.Win32.Sinowal!IK
Avast	Win32:Sinowal-FZ
BitDefender	Backdoor.Sinowal.CV
F-Secure	Trojan:W32/Mebroot.gen!A
DrWeb	Trojan.Packed.2447
AntiVir	TR/PWS.Sinowal.Gen
McAfee-GW-Edition	Heuristic.LooksLike.Trojan.PWS.Sinowal.I
Sophos	Mal/Generic-A
Authentium	W32/Sinowal.B.gen!Eldorado
Microsoft	PWS:Win32/Sinowal.gen!M
GData	Backdoor.Sinowal.CV
VBA32	Malware-Cryptor.Win32.Kefir
Sunbelt	Trojan.Win32.Mebroot!Generic (v)
PCTools	Trojan.Mebroot
Ikarus	Backdoor.Win32.Sinowal
Fortinet	PossibleThreat
AVG	PSW.Sinowal.W
Panda	Suspicious file

VirusTotal link for: [767cfbc1723c44aad9131caf8fd7c628](https://www.virustotal.com/analysis/767cfbc1723c44aad9131caf8fd7c628)

**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: 7581b3a5cd8f5a8c9963b89edbe12a91

File Name: NTUSER.DAT  
 File Path: Documents and Settings/LocalService  
 MD5 Hash: c13b1b5c3e7ab7887f964d517391ee33

File Name: NTUSER.DAT  
 File Path: Documents and Settings/NetworkService  
 MD5 Hash: 0854baea0cf17ba2d14db001c9241360

**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:	0565d6676daf2aac8e7b481cde4d7649
File Name:	default
File Path:	WINDOWS/system32/config
MD5 Hash:	d98e8fe789bc464fc7b0b69e616efe8d
File Name:	SAM
File Path:	WINDOWS/system32/config
MD5 Hash:	beab31379840ba0b7907b9a845df8502
File Name:	SECURITY
File Path:	WINDOWS/system32/config
MD5 Hash:	f9e84c95ed06a12dd9b880a4a98ff3aa
File Name:	software
File Path:	WINDOWS/system32/config
MD5 Hash:	72a9865fd186f686d019183b421d267c
File Name:	SysEvent.Evt
File Path:	WINDOWS/system32/config
MD5 Hash:	e561c28b9100a0a50c674490a9644e95
File Name:	system
File Path:	WINDOWS/system32/config
MD5 Hash:	09691c669143b67ecc34c43270abb72c
File Name:	wbemess.lo_
File Path:	WINDOWS/system32/wbem/Logs
MD5 Hash:	304fdc2a976fc079d21a233572e33b81

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

[Back To Top](#)

**Data**

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

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.