McAfee | Threat Analysis Report

File Name	e9ac2f8c5913c98be43f707e2a99f2374d0cc67bdebb0af42ccbe6adeca46e20	Threat Level	4 - High
Malware Name	Malware.Dynamic	Engine	Sandbox
File Submitted	2018-04-24 08:33:25	Processing Time	201 seconds
File Size	265,941 bytes	Sandbox Replication	168 seconds

Show More | Hash Values | File Details | Environment

MD5 Hash Identifier	C4F93C7F9B089E29B9527DFA6B8D7DA1
SHA-1 Hash Identifier	6C52BB1C24C45F6D0CA946C97E0E03DC8EF60A12
SHA-256 Hash Identifier	E9AC2F8C5913C98BE43F707E2A99F2374D0CC67BDEBB0AF42CCBE6ADECA46E20
Screenshots	16

Hide hash values

File Type	PE32 executable (GUI) Intel 80386
Digital Signature Verified	Unsigned
Publisher	Not Available
Description	Not Available
Product Name	Not Available
Version Info	Not Available
File version	Not Available
Strong Name	Not Available
Original Name	Not Available
Internal Name	Not Available
Copyright	Not Available
Comments	Not Available

Hide file details

Microsoft Windows 7 Enterprise Edition Service Pack 1 (build 7601, version 6.1.7601), 64-bit

Internet Explorer version: 8.0.7601.17514

Microsoft Office version: 2003

PDF Reader version: 9.0

Flash player version: 11.2.202.228

No Flash player plugin installed

Platform Version 4.4.0.9

Detection Package Version 4.4.0.180402

Hide environment

Baitexe activated but not infected

Behavior Classification

Behavior	Severity
Hiding, Camouflage, Stealthiness, Detection and Removal Protection	4 - High
Behaved like ransomware , encrypts victims files and demands for ransom to decrypt it	4 - High
Modified time attribute of the specified file after its creation	2 - Low
Manipulated an existing Windows service by its handle	2 - Low

Deleted itself after installation	2 - Low
Connected to a specific service provider	2 - Low
Uses the Microsoft Cryptographic APIs	1 - Informational
Set a filter function to supersede the top-level exception handler (http://msdn.microsoft.com/en-us/library/vstudio/x85tt0dd.aspx)	1 - Informational
Changed the protection attribute of the process	1 - Informational

Spreading — 4 - High

Behaved like ransomware , encrypts victims files and demands for ransom to decrypt it	4 - High
Wrote (injected) data to an area of a foreign process memory	3 - Medium
Created Office Document on a fly and executed it through shell application	3 - Medium
Hid content by modifying its attributes	2 - Low
Created new process through execution of Windows cmd application	2 - Low
Executed active content by Windows shell application	1 - Informational

Exploiting, Shellcode — 3 - Medium

Wrote (injected) data to an area of a foreign process memory	3 - Medium
Created and set up new security descriptor for the running process	2 - Low
Executed active content by Windows shell application	1 - Informational
Created instance of Windows Management Instrumentation (WMI) object	1 - Informational

Persistence, Installation Boot Survival — 2 - Low

Manipulated an existing Windows service by its handle	2 - Low
Deleted file after the machine restarts	1 - Informational

Security Solution / Mechanism bypass, termination and removal, Anti Debugging, VM Detection — 2 - Low

Updated security descriptor for newly created process	2 - Low
Modified Windows System Policy registry's settings	2 - Low
Manipulated an existing Windows service by its handle	2 - Low
Created new process through execution of Windows cmd application	2 - Low
Created named mutex object	2 - Low
Allowed the process to perform system-level actions that were not enabled previously	2 - Low
Allocated and initialized security descriptor for newly created process	2 - Low
Set a filter function to supersede the top-level exception handler (http://msdn.microsoft.com/en-us/library/vstudio/x85tt0dd.aspx)	1 - Informational
Obtained user's logon name	1 - Informational
Disabled attach/detach notifications from dynamic link library	1 - Informational
Contained long sleep	1 - Informational

Networking — 2 - Low

Modified INTERNET_OPTION_CONNECT_RETRIES: number of times that WinInet attempts to resolve and connect to a host	2 - Low
Downloaded data from a webserver	2 - Low

Connected to a specific service provider	2 - Low
Connected to a specific service provider	2 - Low
Altered Web Proxy Auto-Discovery Protocol (WPAD) for rerouting of the network traffic	2 - Low
Set a filter function to supersede the top-level exception handler (http://msdn.microsoft.com/en-us/library/vstudio/x85tt0dd.aspx)	1 - Informational
Cracks a URL into its component parts	1 - Informational

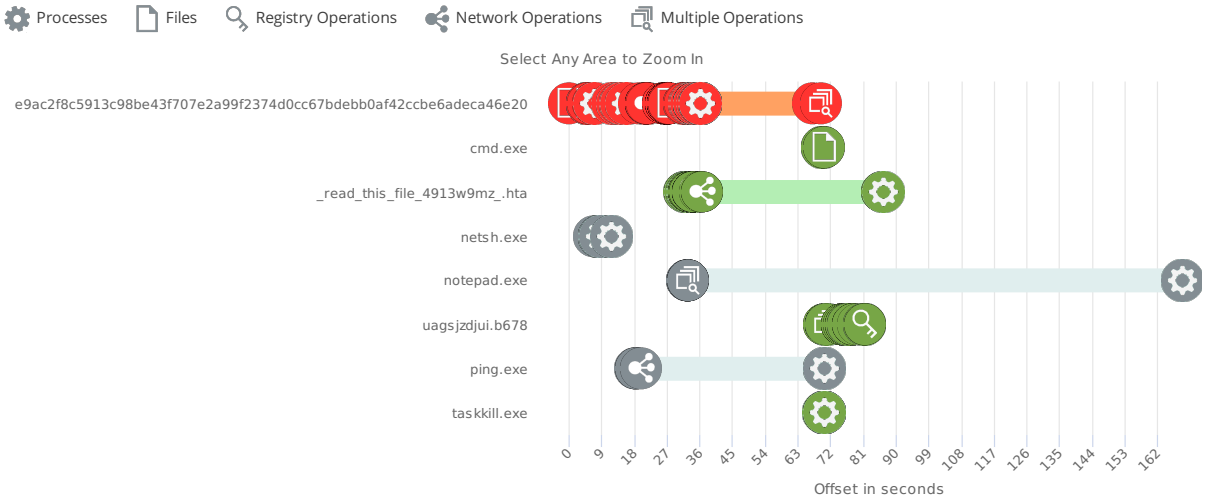
Data spying, Sniffing, Keylogging, Ebanking Fraud — 2 - Low

Set hook procedure to control system activities	2 - Low
Contained long sleep	1 - Informational

Processes Analyzed

Name	Reason	Severity
e9ac2f8c5913c98be43f707e2a99f2374d0cc67bdebb0af42ccbe6adeca46e20	loaded by MATD Analyzer	4 - High
cmd.exe	executed by e9ac2f8c5913c98be43f707e2a99f2374d0cc67bdebb0af42ccbe6adeca46e20	2 - Low
_read_this_file_4913w9mz_.hta	executed & dropped by e9ac2f8c5913c98be43f707e2a99f2374d0cc67bdebb0af42ccbe6adeca46e20	2 - Low
netsh.exe	executed by e9ac2f8c5913c98be43f707e2a99f2374d0cc67bdebb0af42ccbe6adeca46e20	Unverified
notepad.exe	executed by e9ac2f8c5913c98be43f707e2a99f2374d0cc67bdebb0af42ccbe6adeca46e20	1 - Informational
uagsjzdjui.b678	dropped by e9ac2f8c5913c98be43f707e2a99f2374d0cc67bdebb0af42ccbe6adeca46e20	2 - Low
ping.exe	executed by cmd.exe	Unverified
taskkill.exe	executed by cmd.exe	2 - Low

Timeline Activity



Timeline Activity Details

Time Offset	Event	Details
00:00:000	File Operations, miscellaneous	Obtained the unique volume name for a mount point