McAfee | Threat Analysis Report

File Name	1254deaf2281b55bf70bd20353e64138fd1b0229ff42392702f86fd01b17a43b	Threat Level	5 - Very High
Malware Name	Malware.Dynamic	Engine	Sandbox
File Submitted	2018-04-24 08:33:25	Processing Time	246 seconds
File Size	3,645,034 bytes	Sandbox Replication	78 seconds

Show More | Hash Values | File Details | Environment

MD5 Hash Identifier	B62AA7E5FDA9F8C86BDF843F38E7DD14
SHA-1 Hash Identifier	00215C11FA625D798E75146CA2688836B970985A
SHA-256 Hash Identifier	1254DEAF2281B55BF70BD20353E64138FD1B0229FF42392702F86FD01B17A43B
Screenshots	5

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

Behavior Classification

Behavior	Severity
Hiding, Camouflage, Stealthiness, Detection and Removal Protection	5 - Very High
Trojan Backdoor, allowed remote access to the infected system	5 - Very High
Behaved like file's infector malware	4 - High
Malicious Mutex created or opened	3 - Medium
	1 -

Created new PE file	Informational

Spreading — 5 - Very High

Infected Analyzer 'bait' application	5 - Very High
Dropped itself to the Windows root folder	3 - Medium
Created directory under Windows system folder	3 - Medium
Copied itself under system32 folder	3 - Medium
Created content under Windows system directory	2 - Low
Created executable content under Analyzer's temporary directory	1 - Informational

Networking — 5 - Very High

Trojan Backdoor, allowed remote access to the infected system	5 - Very High

Persistence, Installation Boot Survival — 3 - Medium

Malicious Mutex created or opened	3 - Medium
Copied itself under system32 folder	3 - Medium
Created content under Windows system directory	2 - Low

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

Created named mutex object	2 - Low
Contained long sleep	1 - Informational

Data spying, Sniffing, Keylogging, Ebanking Fraud — 1 - Informational

Contained long sleep	1 - Informational

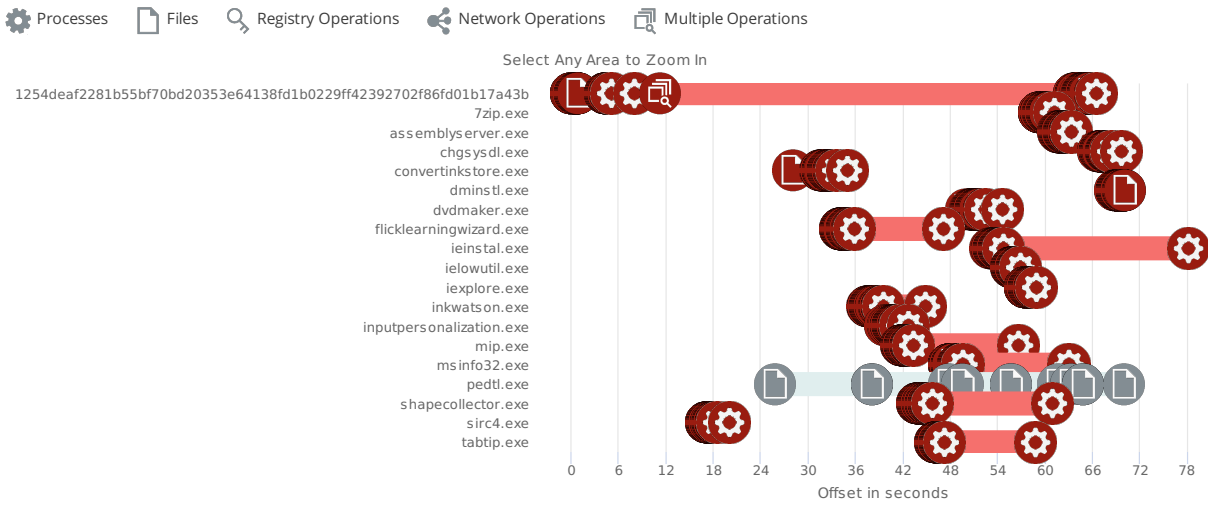
Exploiting, Shellcode — Unverified

Processes Analyzed

Name	Reason	Severity
1254deaf2281b55bf70bd20353e64138fd1b0229ff42392702f86fd01b17a43b	loaded by MATD Analyzer	5 - Very High
7zip.exe	dropped by 1254deaf2281b55bf70bd20353e64138fd1b0229ff42392702f86fd01b17a43b	5 - Very High
assemblyserver.exe	dropped by 1254deaf2281b55bf70bd20353e64138fd1b0229ff42392702f86fd01b17a43b	5 - Very High
chgsysdl.exe	dropped by 1254deaf2281b55bf70bd20353e64138fd1b0229ff42392702f86fd01b17a43b	5 - Very High
convertinkstore.exe	dropped by 1254deaf2281b55bf70bd20353e64138fd1b0229ff42392702f86fd01b17a43b	5 - Very High
dminstl.exe	dropped by 1254deaf2281b55bf70bd20353e64138fd1b0229ff42392702f86fd01b17a43b	5 - Very High
dvdmaker.exe	dropped by 1254deaf2281b55bf70bd20353e64138fd1b0229ff42392702f86fd01b17a43b	5 - Very High
flicklearningwizard.exe	dropped by 1254deaf2281b55bf70bd20353e64138fd1b0229ff42392702f86fd01b17a43b	5 - Very High
ieinstal.exe	dropped by 1254deaf2281b55bf70bd20353e64138fd1b0229ff42392702f86fd01b17a43b	5 - Very High
ielowutil.exe	dropped by 1254deaf2281b55bf70bd20353e64138fd1b0229ff42392702f86fd01b17a43b	5 - Very High
iexplore.exe	dropped by 1254deaf2281b55bf70bd20353e64138fd1b0229ff42392702f86fd01b17a43b	5 - Very High
	dropped by	5 - Very

inkwatson.exe	1254deaf2281b55bf70bd20353e64138fd1b0229ff42392702f86fd01b17a43b	High
inputpersonalization.exe	dropped by 1254deaf2281b55bf70bd20353e64138fd1b0229ff42392702f86fd01b17a43b	5 - Very High
mip.exe	dropped by 1254deaf2281b55bf70bd20353e64138fd1b0229ff42392702f86fd01b17a43b	5 - Very High
msinfo32.exe	dropped by 1254deaf2281b55bf70bd20353e64138fd1b0229ff42392702f86fd01b17a43b	5 - Very High
pedtl.exe	dropped by 1254deaf2281b55bf70bd20353e64138fd1b0229ff42392702f86fd01b17a43b	1 - Informational
shapecollector.exe	dropped by 1254deaf2281b55bf70bd20353e64138fd1b0229ff42392702f86fd01b17a43b	5 - Very High
sirc4.exe	dropped by 1254deaf2281b55bf70bd20353e64138fd1b0229ff42392702f86fd01b17a43b	5 - Very High
tabtip.exe	dropped by 1254deaf2281b55bf70bd20353e64138fd1b0229ff42392702f86fd01b17a43b	5 - Very High
baitexe.exe	loaded by MATD Analyzer & dropped by 1254deaf2281b55bf70bd20353e64138fd1b0229ff42392702f86fd01b17a43b	5 - Very High

Timeline Activity



Timeline Activity Details

Time Offset	Event	Details
00:00:000	File Operations, miscellaneous	Obtained the path of the Windows system directory
00:00:000	File Operations, miscellaneous	Retrieved the full path for the module
00:00:016	File Operations, miscellaneous	Searched a directory for the name: C:*.*
00:00:016	Files Modified	C:\marijuana.txt 0 0
00:00:016	Files Modified	C:\marijuana.txt 0 128
00:00:016	Files Modified	C:\marijuana.txt 106 106
00:00:016	Files Modified	C:\marijuana.txt 128 128
		C:\marijuana.txt