McAfee | Threat Analysis Report

File Name	15f5cb94b851289d0218f333e06372e43b2a55d241c530d4f61aad3b89f68b91	Threat Level	5 - Very High
Malware Name	Malware.Dynamic	Engine	Sandbox
File Submitted	2018-04-24 08:33:25	Processing Time	213 seconds
File Size	67,584 bytes	Sandbox Replication	180 seconds

Show More | Hash Values | File Details | Environment

MD5 Hash Identifier	C3294C90474063DFB0D28EF8A693A6CB
SHA-1 Hash Identifier	F339B703192A562DDE82596319E8720C30AAA5ED
SHA-256 Hash Identifier	15F5CB94B851289D0218F333E06372E43B2A55D241C530D4F61AAD3B89F68B91
Screenshots	1

Hide hash values

File Type	PE32 executable (GUI) Intel 80386
Digital Signature Verified	Unsigned
Publisher	Not Available
Company	SynapticosSoft, Corporation.
Description	kCkZn
Product Name	rLORrMGmF
Version Info	16,2,5,16
File version	16,2,5,16
MachineType	SynapticosSoft, Corporation.
Binary Version	16,2,5,16
Strong Name	Not Available
Original Name	uZlQSDe.exe
Internal Name	Not Available
Copyright	Copyright 1990 - 2001
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
Spreading	5 - Very High
Infected Analyzer 'bait' application	5 - Very High

Behaved like ransomware , encrypts victims files and demands for ransom to decrypt it	4 - High
Behaved like Ransomware family	4 - High
Created Office Document on a fly and executed it through shell application	3 - Medium
Created new process through execution of Windows cmd application	2 - Low
Executed active content by Windows shell application	1 - Informational

Hiding, Camouflage, Stealthiness, Detection and Removal Protection — 4 - High

Deleted shadow copies of a specified volume	4 - High
Behaved like ransomware , encrypts victims files and demands for ransom to decrypt it	4 - High
Behaved like Ransomware family	4 - High
Created new PE file	1 - Informational

Persistence, Installation Boot Survival — 4 - High

Malicious behavior: set application name into auto-run registry entry and executed it by system shell	4 - High
Dissabled recovery mode	4 - High
Behaved like Ransomware family	4 - High
Altered auto-run registry entry that executed at next Windows boot	3 - Medium

Exploiting, Shellcode — 4 - High

Malicious behavior: set application name into auto-run registry entry and executed it by system shell	4 - High
Executed active content by Windows shell application	1 - Informational

Security Solution / Mechanism bypass, termination and removal, Anti Debugging, VM Detection — 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
Obtained user's logon name	1 - Informational
Disabled attach/detach notifications from dynamic link library	1 - Informational
Contained long sleep	1 - Informational

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

Contained long sleep	1 - Informational

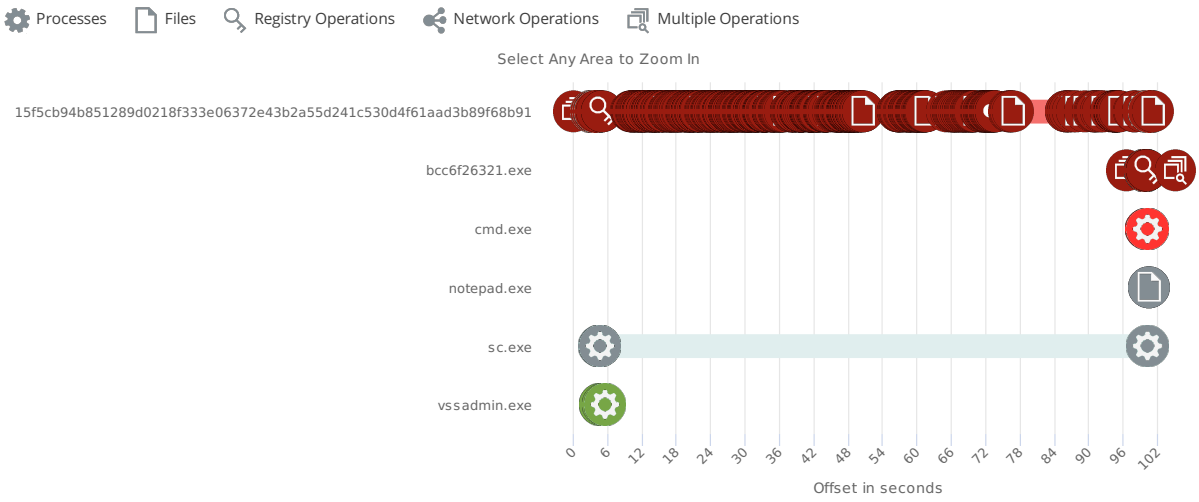
Networking — Unverified

Processes Analyzed

Name	Reason	Severity
15f5cb94b851289d0218f333e06372e43b2a55d241c530d4f61aad3b89f68b91	dropped by 15f5cb94b851289d0218f333e06372e43b2a55d241c530d4f61aad3b89f68b91 & loaded by MATD Analyzer	5 - Very High
bcc6f26321.exe	dropped by 15f5cb94b851289d0218f333e06372e43b2a55d241c530d4f61aad3b89f68b91	5 - Very High
cmd.exe	executed by 15f5cb94b851289d0218f333e06372e43b2a55d241c530d4f61aad3b89f68b91	4 - High

	& executed by bcc6f26321.exe	
notepad.exe	executed by 15f5cb94b851289d0218f333e06372e43b2a55d241c530d4f61aad3b89f68b91	1 - Informational
sc.exe	executed by cmd.exe	Unverified
vssadmin.exe	executed by cmd.exe	2 - Low

Timeline Activity



Timeline Activity Details

Time Offset	Event	Details
00:00:000	File Operations, miscellaneous	Obtained the current directory for the current process
00:00:000	Process Operations, miscellaneous	Disabled the DLL_THREAD_ATTACH and DLL_THREAD_DETACH notifications for the dynamic-link library
00:00:000	Others	Obtained the system metric or system configuration setting
00:03:328	Process Created	{871C5380-42A0-1069-A2EA-08002B30309D}
00:03:344	Process Created	{1F486A52-3CB1-48FD-8F50-B8DC300D9F9D}
00:03:344	Process Created	{7B8A2D94-0AC9-11D1-896C-00C04FB6BFC4}
00:03:344	Process Operations, miscellaneous	Initialized COM library for the current thread and set it in the concurrency mode
00:03:750	Process Created	c:\windows\system32\cmd.exe "c:\windows\system32\cmd.exe" /c sc stop vvs
00:03:766	Process Opened	CMD/c sc stop vvs
00:03:828	Process Opened	CMD/c vssadmin.exe delete shadows /all /quiet
00:03:828	Process Created	c:\windows\system32\cmd.exe "c:\windows\system32\cmd.exe" /c vssadmin.exe delete shadows /all /quiet
00:03:921	Process Opened	CMD/c bcdedit /set {default} recoveryenabled no
00:03:921	Process Created	c:\windows\system32\cmd.exe "c:\windows\system32\cmd.exe" /c bcdedit /set {default} recoveryenabled no