File Name	1b12dcb58fe25a803ebb10b39bace2e87c0752d6a997ecffd6ec666e59e0fd34	Threat Level	5 - Very High
Malware Name	Malware.Dynamic	Engine	Sandbox
File Submitted	2018-04-24 08:33:25	Processing Time	212 seconds
File Size	272,896 bytes	Sandbox Replication	121 seconds

Show More Hash Values File Details Environment

MD5 Hash Identifier	DC499C928B3347F9F43AEA2786B48420
SHA-1 Hash Identifier	43D4B470E9450FD92918FB7B8F180509AB6BE8EB
SHA-256 Hash Identifier	1B12DCB58FE25A803EBB10B39BACE2E87C0752D6A997ECFFD6EC666E59E0FD34
Screenshots	2

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
Security Solution / Mechanism bypass, termination and removal, Anti Debugging, VM Detection	5 - Very High
Injected code into processes using Dynamic Forking method	5 - Very High
Manipulated an existing Windows service by its handle	2 - Low
Created named mutex object	2 - Low
Allowed the process to perform system-level actions that were not enabled previously	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
Enumerated all running system's processes in the snapshot	1 - Informational
Spreading	5 - Very High

Injected code into processes using Dynamic Forking method	5 - Very High
Infected Analyzer 'bait' application	5 - Very High
Injected into a different process memory and changes the access protection of the committed pages	4 - High
Dropped files into various system folders	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
Hid content by modifying its attributes	2 - Low

Persistence, Installation Boot Survival — 4 - High

Dropped files into various system folders	4 - High
Altered auto-run registry entry that executed at next Windows boot	3 - Medium
Manipulated an existing Windows service by its handle	2 - Low
General activities from kernel level, see http://en.wikipedia.org/wiki/Ring_(computer_security)	1 - Informational

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

Injected into a different process memory and changes the access protection of the committed pages	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
Modified time attribute of the specified file after its creation	2 - Low
Modified file's time creation attributes	2 - Low
Manipulated an existing Windows service by its handle	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
Created new PE file	1 - Informational
Changed the protection attribute of the process	1 - Informational

Exploiting, Shellcode — 4 - High

Injected into a different process memory and changes the access protection of the committed pages	4 - High
Wrote (injected) data to an area of a foreign process memory	3 - Medium

Networking — 2 - Low

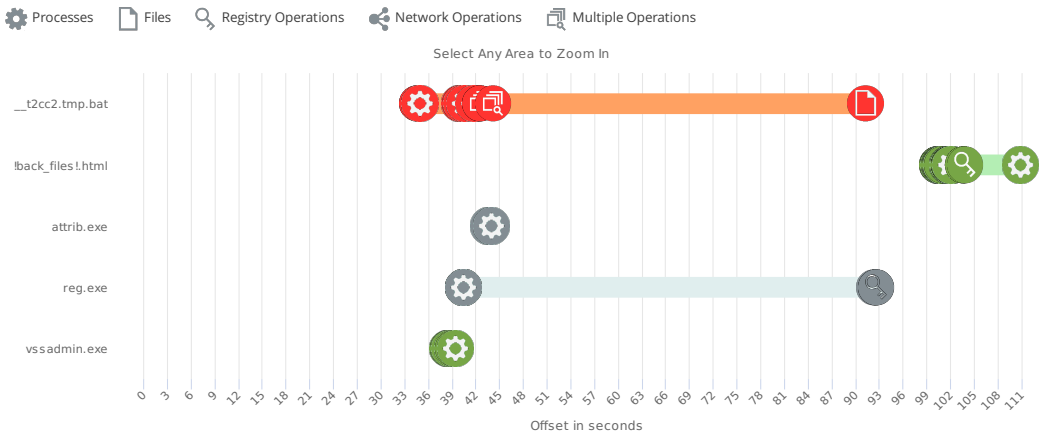
Altered Web Proxy Auto-Discovery Protocol (WPAD) for rerouting of the network traffic	2 - Low
Set a filter function to supersede the top-level exception handler (http://msdn.microsoft.com/en-us/library/vstudio/x85tt0dd.aspx)	1 - Informational

Data spying, Sniffing, Keylogging, Ebanking Fraud — Unverified

Processes Analyzed

Name	Reason	Severity
1b12dcb58fe25a803ebb10b39bace2e87c0752d6a997ecffd6ec666e59e0fd34	loaded by MATD Analyzer	5 - Very High
__t2cc2.tmp.bat	executed & dropped by 1b12dcb58fe25a803ebb10b39bace2e87c0752d6a997ecffd6ec666e59e0fd34	4 - High
!back_files!.html	dropped by 1b12dcb58fe25a803ebb10b39bace2e87c0752d6a997ecffd6ec666e59e0fd34	2 - Low
attrib.exe	executed by __t2cc2.tmp.bat	Unverified
reg.exe	executed by __t2cc2.tmp.bat	Unverified
vssadmin.exe	executed by __t2cc2.tmp.bat	2 - Low

Timeline Activity



Timeline Activity Details

Time Offset	Event	Details
00:00:000	File Operations, miscellaneous	Retrieved the full path for the module
00:00:000	Process Operations, miscellaneous	Enabled an application to supersede the top-level exception handler
00:33:030	Process Operations, miscellaneous	Changed the protection attribute of process address: 0x3d5b60, new attribute: Execute_ReadWrite
00:33:047	File Operations, miscellaneous	Obtained a set of FAT file system attributes for a file or directory
00:33:234	Process Operations, miscellaneous	Retrieved the context of the specified thread
00:33:234	Process Created	c:\sfgpdspdkq\1b12dcb58fe25a803ebb10b39bace2e87c0752d6a997ecffd6ec666e59e0fd34 c:\sfgpdspdkq\1b12dcb58fe25a803ebb10b39bace2e87c0752d6a997ecffd6ec666e59e0fd34
00:33:265	Foreign Memory Regions Written	Copied an address range from the current process into the address range of another process
00:33:265	Foreign Memory Regions Read	Read data from an area of memory in a specified process
00:33:265	Foreign Memory Regions Written	Allocated memory in foreign(or local) processes
00:33:280	Process Operations, miscellaneous	Set the context for the specified thread
00:33:280	Process Operations, miscellaneous	Decremented a thread's suspend count
00:33:640	Process killed	Ended itself and all of its threads
00:33:797	Files Copied	C:\sfgpdspdkq\1b12dcb58fe25a803ebb10b39bace2e87c0752d6a997ecffd6ec666e59e0fd34 C:\Users\Public\1b12dcb58fe25a803ebb10b39bace2e87c0752d6a997ecffd6ec666e59e0fd34
00:33:797	Registry Modified	HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce\CertificatesCheck C:\Users\Public\1b12dcb58fe25a803ebb10b39bace2e87c0752d6a997ecffd6ec666e59e0fd34 REG_SZ
00:33:797	Registry Created	HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce
00:33:827	Files Created	C:\Users\ADMINI~1\AppData\Local\Temp__t2CC2.tmp.bat Write Normal
00:33:827	Files Modified	C:\Users\ADMINI~1\AppData\Local\Temp__t2CC2.tmp.bat 445 445
00:33:875	Process Created	c:\users\admini~1\appdata\local\temp__t2cc2.tmp.bat
00:34:312	Files	C:\Users\Public\{846ee340-7039-11de-9d20-806e6f6e6963} 258