

File Name	c674da5f1c063a0bec896d03492620ac94687e7687a1b91944d93c1d6527c8a7	Threat Level	● 4 - High
Malware Name	Malware.Dynamic	Engine	Sandbox
File Submitted	2018-04-24 08:33:25	Processing Time	200 seconds
File Size	630,784 bytes	Sandbox Replication	124 seconds
Show More	Hash Values	File Details	Environment
MD5 Hash Identifier	20F2CA720CB4DCCA9195113F258CA4EF		
SHA-1 Hash Identifier	2F5E2914AF69F91C5E84E7EA0FC58DAD4B6B741E		
SHA-256 Hash Identifier	C674DA5F1C063A0BEC896D03492620AC94687E7687A1B91944D93C1D6527C8A7		
Screenshots	10		
	Hide hash values		
File Type	PE32 executable (GUI) Intel 80386 (stripped to external PDB)		
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
<ul style="list-style-type: none"> ✓ Hiding, Camouflage, Stealthiness, Detection and Removal Protection 	● 4 - High
Behaved like ransomware , encrypts victims files and demands for ransom to decrypt it	● 4 - High
Behaved like Ransomware and tried to retrieve drives/network,volumeinformation of the victims machine	● 4 - High
Encrypted and uploaded data to suspicious webserver	● 3 - Medium
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
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 (● 1 - Informational

http://msdn.microsoft.com/en-us/library/vstudio/x85tt0dd.aspx) 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

Behaved like Ransomware and tried to retrieve drives/network,volumeinformation of the victims machine 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

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

Networking

3 - Medium

Set INTERNET_OPTION_CONNECT_TIMEOUT: the time-out value to use for Internet connection requests 3 - Medium

Encrypted and uploaded data to suspicious webservice 3 - Medium

Modified INTERNET_OPTION_CONNECT_RETRIES: number of times that Wininet attempts to resolve and connect to a host 2 - Low

Downloaded data from a webservice 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

Security Solution / Mechanism bypass, termination and removal, Anti Debugging, VM Detection

2 - Low

Updated security descriptor for newly created process 2 - Low

Manipulated an existing Windows service by its handle 2 - Low

Created named mutex object 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

Contained long sleep 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

Data spying, Sniffing, Keylogging, Ebanking Fraud

1 - Informational

Contained long sleep 1 - Informational

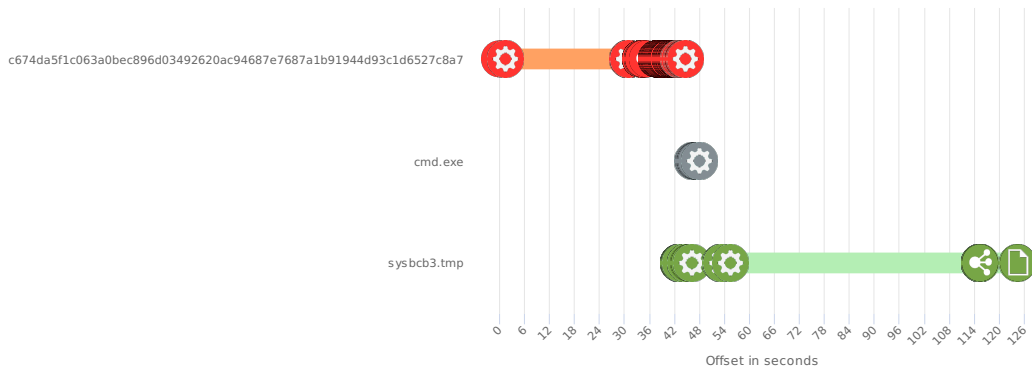
Processes Analyzed

Name	Reason	Severity
c674da5f1c063a0bec896d03492620ac94687e7687a1b91944d93c1d6527c8a7	loaded by MATD Analyzer	4 - High
cmd.exe	executed by c674da5f1c063a0bec896d03492620ac94687e7687a1b91944d93c1d6527c8a7	Unverified
sysbc3.tmp	executed & dropped by c674da5f1c063a0bec896d03492620ac94687e7687a1b91944d93c1d6527c8a7	2 - Low

Timeline Activity

⚙️ Processes
📁 Files
🔍 Registry Operations
🌐 Network Operations
📄 Multiple Operations

Select Any Area to Zoom In



Timeline Activity Details

Time Offset	Event	Details
00:00:00	Signal Objects	Opened an existing named event object
00:01:452	Process Operations, miscellaneous	Set a waiting mode until a specified object is in the signaled state or the time-out interval elapses
00:30:860	Foreign Memory Regions Written	Wrote to the memory of a process: c674da5f1c063a0bec896d03492620ac94687e7687a1b91944d93c1d6527c8a7
00:30:891	Process Operations, miscellaneous	Changed the protection attribute of process address: 0x483000, new attribute: ReadWrite
00:30:891	Process Operations, miscellaneous	Changed the protection attribute of process address: 0x4780b4, new attribute: ReadWrite
00:30:891	Process Operations, miscellaneous	Changed the protection attribute of process address: 0x486000, new attribute: ReadWrite
00:30:891	Process Operations, miscellaneous	Changed the protection attribute of process address: 0x486000, new attribute: ReadOnly
00:30:891	Process Operations, miscellaneous	Changed the protection attribute of process address: 0x483000, new attribute: ReadOnly
00:30:891	Process Operations, miscellaneous	Changed the protection attribute of process address: 0x47f000, new attribute: ReadWrite
00:30:891	Process Operations, miscellaneous	Changed the protection attribute of process address: 0x478000, new attribute: ReadWrite
00:30:891	Process Operations, miscellaneous	Changed the protection attribute of process address: 0x478000, new attribute: ReadOnly
00:30:891	Process Operations, miscellaneous	Changed the protection attribute of process address: 0x401000, new attribute: ReadWrite
00:30:891	Process Operations, miscellaneous	Changed the protection attribute of process address: 0x401000, new attribute: Execute_Read
00:30:891	Process Operations, miscellaneous	Changed the protection attribute of process address: 0x400000, new attribute: ReadOnly
00:30:891	Process Operations, miscellaneous	Changed the protection attribute of process address: 0x400000, new attribute: ReadWrite
00:30:952	Process Operations, miscellaneous	Changed the protection attribute of process address: 0x478280, new attribute: ReadWrite
00:30:952	Process Operations, miscellaneous	Changed the protection attribute of process address: 0x478080, new attribute: ReadOnly