

File Name	<a href="#">0c2830e7c6a5211ca77a7c312a823ad64e5c64903d652d532f4968ab164fb52d</a>	Threat Level	<span style="color: red;">● 5 - Very High</span>
Malware Name	Malware.Dynamic	Engine	Sandbox
File Submitted	2018-04-24 08:33:26	Processing Time	209 seconds
File Size	126,976 bytes	Sandbox Replication	180 seconds
Show More	<a href="#">Hash Values</a>	<a href="#">File Details</a>	<a href="#">Environment</a>
MD5 Hash Identifier	01082E7169DC0B8D59FB514FBC44EB5C		
SHA-1 Hash Identifier	39E358AB8EE3C4FBDD03F5AB34414F6F89F25EEB		
SHA-256 Hash Identifier	0C2830E7C6A5211CA77A7C312A823AD64E5C64903D652D532F4968AB164FB52D		
	<a href="#">Hide hash values</a>		
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		
	<a href="#">Hide file details</a>		
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			
	<a href="#">Hide environment</a>		

**Behavior Classification**

Behavior	Severity
<ul style="list-style-type: none"> <li>Persistence, Installation Boot Survival</li> </ul>	<span style="color: red;">● 4 - High</span>
<div style="border: 1px solid #ccc; padding: 5px;"> <ul style="list-style-type: none"> <li>Malicious behavior: set application name into auto-run registry entry and executed it by system shell</li> <li>Behaved like Ransomware family</li> </ul> </div>	<ul style="list-style-type: none"> <li><span style="color: red;">● 4 - High</span></li> <li><span style="color: red;">● 4 - High</span></li> </ul>

Altered auto-run registry entry that executed at next Windows boot ● 3 - Medium

▼ 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
Modified time attribute of the specified file after its creation	● 2 - Low
Uses the Microsoft Cryptographic APIs	● 1 - Informational

▼ Spreading

● 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 process through execution of Windows cmd application	● 2 - Low
Executed active content by Windows shell application	● 1 - Informational

▼ 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

▼ Networking

● Unverified

▼ Data spying, Sniffing, Keylogging, Ebanking Fraud

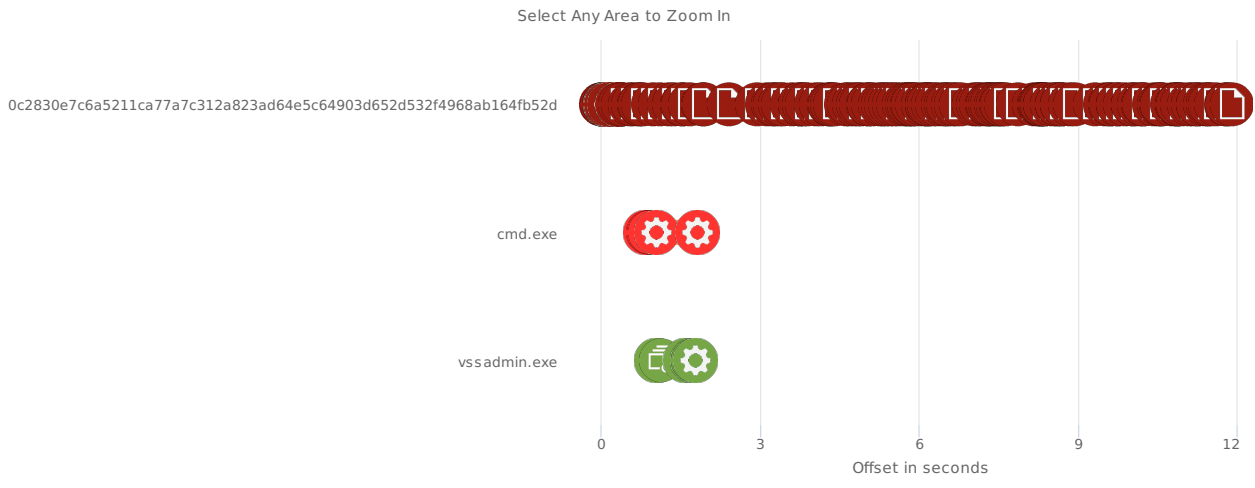
● Unverified

**Processes Analyzed**

Name	Reason	Severity
0c2830e7c6a5211ca77a7c312a823ad64e5c64903d652d532f4968ab164fb52d	loaded by MATD Analyzer	● 5 - Very High
cmd.exe	executed by 0c2830e7c6a5211ca77a7c312a823ad64e5c64903d652d532f4968ab164fb52d	● 4 - High
vssadmin.exe	executed by cmd	● 2 - Low

**Timeline Activity**

- Processes
- Files
- Registry Operations
- Network Operations
- Multiple Operations



Timeline Activity Details

Time Offset	Event	Details
00:00:00	Others	Retrieved the current local date and time
00:00:00	Signal Objects	onylonlock
00:00:00	File Operations, miscellaneous	Determined whether a disk drive C:\ is a removable, fixed, CD-ROM, RAM disk, or network drive
00:00:00	File Operations, miscellaneous	Obtained a bitmask representing the currently available disk drives
00:00:00	File Operations, miscellaneous	Retrieved the full path for the module
00:00:00	Process Operations, miscellaneous	Enabled an application to supersede the top-level exception handler
00:00:00	Process Operations, miscellaneous	Changed the protection attribute of process address: 0xba0000, new attribute: ReadWrite
00:00:00	Process Operations, miscellaneous	Changed the protection attribute of process address: 0xba0000, new attribute: ReadOnly
00:00:047	Others	Expanded environment-variable strings and replace them with the values defined for the current use
00:00:062	Files Created	C:\Users\Administrator\AppData\Roaming\!#_DECRYPT_#!.inf Write Normal
00:00:062	Registry Modified	HKCU\Software\Microsoft\Windows\CurrentVersion\Run\info C:\Users\Administrator\AppData\Roaming\!#_DECRYPT_#!.inf REG_SZ
00:00:062	Registry Opened	HKCU\Software\Microsoft\Windows\CurrentVersion\Run
00:00:062	Files Modified	C:\Users\Administrator\AppData\Roaming\!#_DECRYPT_#!.inf 174 174
00:00:062	Files Modified	C:\Users\Administrator\AppData\Roaming\!#_DECRYPT_#!.inf 1001 1001
00:00:078	Process Operations, miscellaneous	Initialized COM library for the current thread and set it in the concurrency mode
00:00:094	Process Created	{871C5380-42A0-1069-A2EA-08002B30309D}
00:00:109	Process Created	{1F486A52-3CB1-48FD-8F50-B8DC300D9F9D}
00:00:156	Process Created	{7B8A2D94-0AC9-11D1-896C-00C04FB6BFC4}