File Name	e3af616583327f189f2d9e0b1c38199e1f35dda391b6a559253be0fb4410a0e9	Threat Level	5 - Very High
Malware Name	Malware.Dynamic	Engine	Sandbox
File Submitted	2018-04-24 08:33:25	Processing Time	44 seconds
File Size	131,072 bytes	Sandbox Replication	19 seconds

Show More Hash Values File Details Environment

MD5 Hash Identifier	425E0923CF2187FFEB3947E89C9E6E57
SHA-1 Hash Identifier	0C1007BA3EF9255C004EA1EF983E02EFE918EE59
SHA-256 Hash Identifier	E3AF616583327F189F2D9E0B1C38199E1F35DDA391B6A559253BE0FB4410A0E9
Screenshots	1

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
Deleted file zone identification information	3 - Medium
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
Contained long sleep	1 - Informational

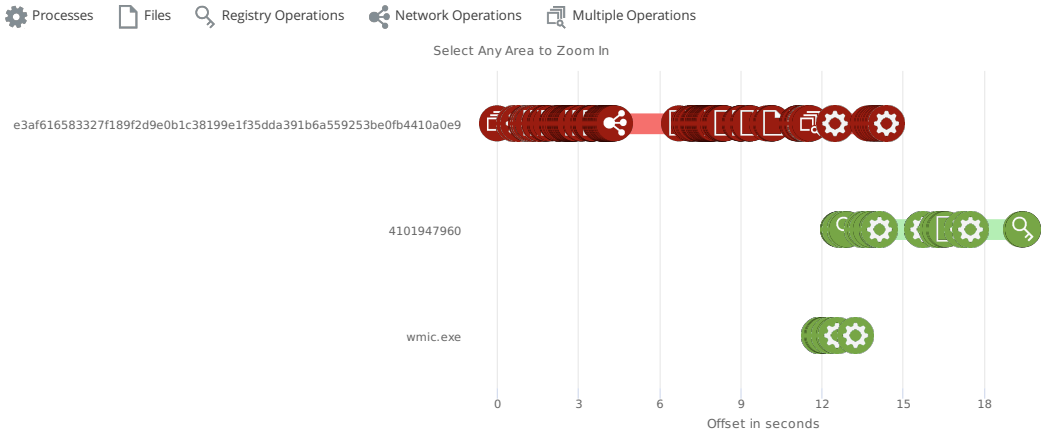
Spreading	5 - Very High
Injected code into processes using Dynamic Forking method	5 - Very High
Injected into a different process memory and changes the access protection of the committed pages	4 - High
Behaved like ransomware , encrypts victims files and demands for ransom to decrypt it	4 - High
Wrote (injected) data to an area of a foreign process memory	3 - Medium
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
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
Hid executable file by changing its attributes	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
Deleted file zone identification information	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
Deleted itself after installation	2 - Low
Uses the Microsoft Cryptographic APIs	1 - Informational
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
Executed active content by Windows shell application	1 - Informational
Created instance of Windows Management Instrumentation (WMI) object	1 - Informational
Data spying, Sniffing, Keylogging, Ebanking Fraud	3 - Medium
Allocated a region of memory within the virtual address space of a foreign process	3 - Medium
Set hook procedure to control system activities	2 - Low
Contained long sleep	1 - Informational
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
Cracks a URL into its component parts	1 - Informational
Persistence, Installation Boot Survival	2 - Low
Manipulated an existing Windows service by its handle	2 - Low

Processes Analyzed

Name	Reason	Severity

e3af616583327f189f2d9e0b1c38199e1f35dda391b6a559253be0fb4410a0e9	loaded by MATD Analyzer	5 - Very High
4101947960	executed & dropped by e3af616583327f189f2d9e0b1c38199e1f35dda391b6a559253be0fb4410a0e9	2 - Low
wmic.exe	executed by e3af616583327f189f2d9e0b1c38199e1f35dda391b6a559253be0fb4410a0e9	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	Others	Obtained the system metric or system configuration setting
00:00:000	Process Operations, miscellaneous	Installed a new hook procedure (type: WH_MSGFILTER)
00:00:000	Process Operations, miscellaneous	Obtained the major and minor version numbers of the system on which the specified process expects to run
00:00:000	Files Created	C:\vpbcothodm\e3af616583327f189f2d9e0b1c38199e1f35dda391b6a559253be0fb4410a0e9 Query Normal
00:00:641	Process Operations, miscellaneous	Searched for a top-level window with string: progman
00:00:797	Process Operations, miscellaneous	Installed a new hook procedure (type: WH_CBT)
00:01:108	Files Copied	C:\Users\Administrator\AppData\Local\CSIDL_X C:\vpbcothodm\nnchng.ex_
00:01:108	Files Modified	C:\vpbcothodm\nnchng.ex_, attribute: Normal
00:01:108	Files Modified	C:\vpbcothodm\nnchng.ex_, attribute: Hidden & System
00:01:108	Files Opened	C:\vpbcothodm\e3af616583327f189f2d9e0b1c38199e1f35dda391b6a559253be0fb4410a0e9 Read Normal
00:01:141	Files Opened	C:\Users\Administrator\AppData\Local\CSIDL_ Read Normal
00:01:141	Files Read	C:\vpbcothodm\e3af616583327f189f2d9e0b1c38199e1f35dda391b6a559253be0fb4410a0e9
00:01:141	Files Opened	C:\vpbcothodm\nnchng.ex_ Read