McAfee | Threat Analysis Report

File Name	2e6f9a48d854add9f895a3737fa5fcc9d38d082466765e550cca2dc47a10618e	Threat Level	5 - Very High
Malware Name	Malware.Dynamic	Engine	Sandbox
File Submitted	2018-04-24 08:33:25	Processing Time	43 seconds
File Size	164,352 bytes	Sandbox Replication	19 seconds

Show More | Hash Values | File Details | Environment

MD5 Hash Identifier	59EF984C16A5C1723D9958FBEB1B7450
SHA-1 Hash Identifier	A7BCD0188E3FD0F16226AB44477A04662A5C5450
SHA-256 Hash Identifier	2E6F9A48D854ADD9F895A3737FA5FCC9D38D082466765E550CCA2DC47A10618E

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
Spreading	5 - Very High
Injected code into processes using Dynamic Forking method	5 - Very High
Wrote (injected) data to an area of a foreign process memory	3 - Medium
Exploiting, Shellcode	3 - Medium
Wrote (injected) data to an area of a foreign process memory	3 - Medium
Data spying, Sniffing, Keylogging, Ebanking Fraud	3 - Medium
Allocated a region of memory within the virtual address space of a foreign process	3 - Medium

Hiding, Camouflage, Stealthiness, Detection and Removal Protection — 2 - Low

Deleted itself after installation	2 - Low
Changed the protection attribute of the process	1 - Informational

Persistence, Installation Boot Survival — 1 - Informational

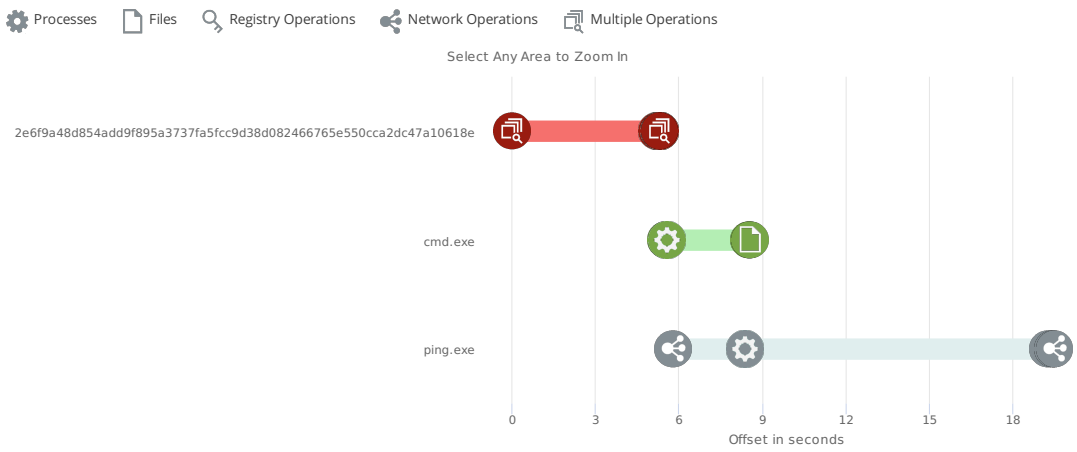
General activities from kernel level, see http://en.wikipedia.org/wiki/Ring_(computer_security)	1 - Informational

Networking — Unverified

Processes Analyzed

Name	Reason	Severity
2e6f9a48d854add9f895a3737fa5fcc9d38d082466765e550cca2dc47a10618e	loaded by MATD Analyzer	5 - Very High
cmd.exe	executed by 2e6f9a48d854add9f895a3737fa5fcc9d38d082466765e550cca2dc47a10618e	2 - Low
ping.exe	executed by 2e6f9a48d854add9f895a3737fa5fcc9d38d082466765e550cca2dc47a10618e & executed by cmd	Unverified

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
00:05:250	Foreign Memory Regions Written	Allocated memory in foreign(or local) processes
00:05:250	Process Operations, miscellaneous	Changed the protection attribute of process address: 0x2e5d70, new attribute: Execute_ReadWrite
00:05:265	File Operations, miscellaneous	Obtained a set of FAT file system attributes for a file or directory
00:05:281	Process Created	c:\vpbcothodm\2e6f9a48d854add9f895a3737fa5fcc9d38d082466765e550cca2dc47a10618e c:\vpbcothodm\2e6f9a48d854add9f895a3737fa5fcc9d38d082466765e550cca2dc47a10618e
00:05:281	Process Operations, miscellaneous	Retrieved the context of the specified thread
00:05:296	Foreign Memory Regions Read	Read data from an area of memory in a specified process
00:05:296	Foreign Memory Regions Written	Copied an address range from the current process into the address range of another process
00:05:296	Process Operations,	Decremented a thread's suspend count