VALKYRIE COMODO

Summary

File Name: 67eb0a16282599d3ead2977d264598fa31dd83f0

File Type: PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows

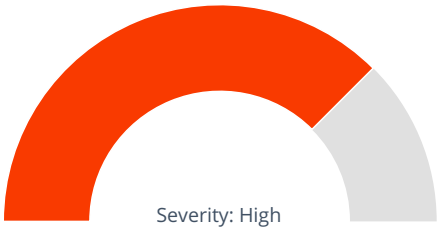
SHA1: 67eb0a16282599d3ead2977d264598fa31dd83f0

MD5: ecebc09fec5652d173f5287faafb9c57

MALWARE

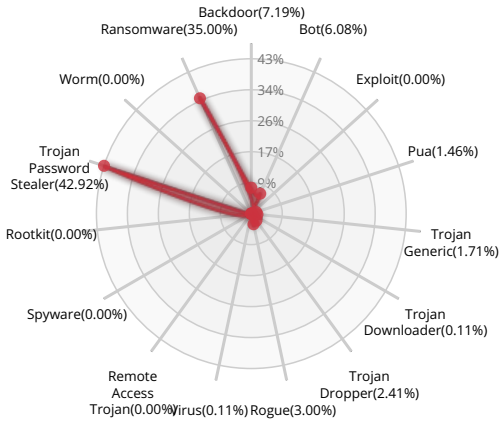
Valkyrie Final Verdict

DETECTION SECTION

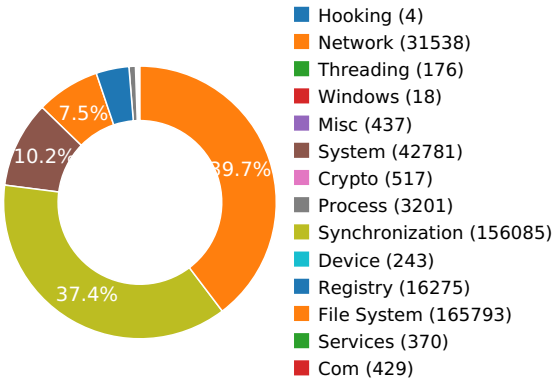


Verdict: Malware

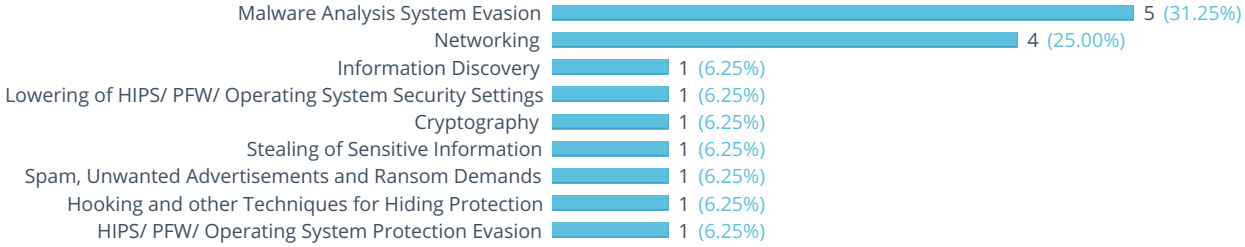
CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW



VALKYRIE COMODO

Activity Details

INFORMATION DISCOVERY

Reads data out of its own binary image	Show sources

NETWORKING

Attempts to connect to a dead IP:Port (2 unique times)	Show sources
HTTP traffic contains suspicious features which may be indicative of malware related traffic	Show sources
Performs some HTTP requests	Show sources
Installs WinPCAP	Show sources

LOWERING OF HIPS/ PFW/ OPERATING SYSTEM SECURITY SETTINGS

Attempts to block SafeBoot use by removing registry keys	Show sources

CRYPTOGRAPHY

At least one IP Address, Domain, or File Name was found in a crypto call	Show sources

STEALING OF SENSITIVE INFORMATION

Steals private information from local Internet browsers	Show sources

SPAM, UNWANTED ADVERTISEMENTS AND RANSOM DEMANDS

Exhibits possible ransomware file modification behavior	Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory	Show sources

MALWARE ANALYSIS SYSTEM EVASION

Possible date expiration check, exits too soon after checking local time	Show sources
A process attempted to delay the analysis task.	Show sources
Checks the CPU name from registry, possibly for anti-virtualization	Show sources
Detects VirtualBox through the presence of a file	Show sources
Attempts to repeatedly call a single API many times in order to delay analysis time	Show sources

HIPS/ PFW/ OPERATING SYSTEM PROTECTION EVASION

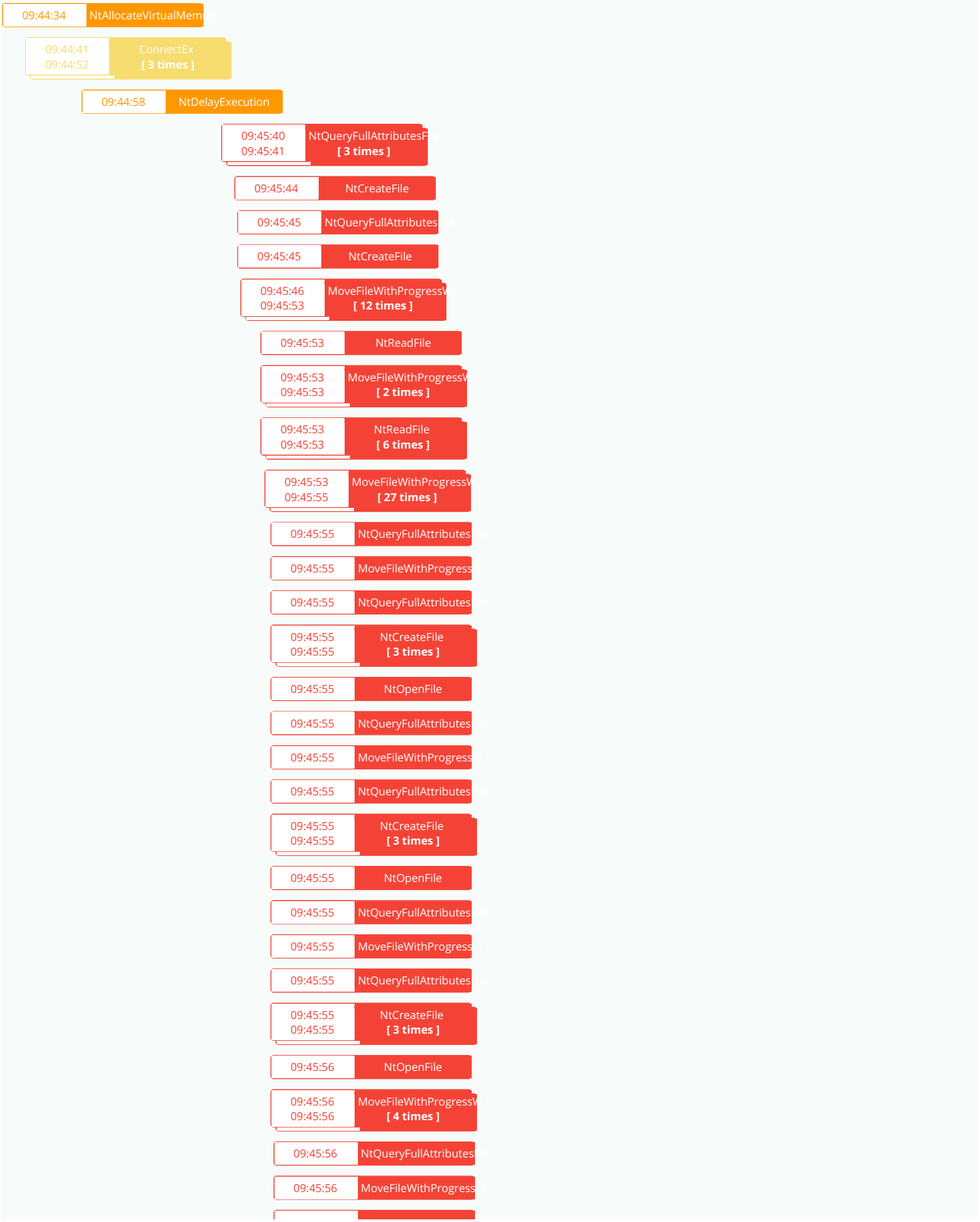
Attempts to identify installed AV products by installation directory	Show sources

Behavior Graph

09:44:34 **09:46:31** **09:48:28**

PID 2208

09:44:34 **Create Process** The malicious file created a child process as 67eb0a16282599d3ead2977d264598fa31dd83f0.exe **(PPID 2440)**



09:45:56 NtQueryFullAttributes

09:45:56 09:45:56 NtCreateFile [3 times]

09:45:56 NtOpenFile

09:45:56 NtQueryFullAttributes

09:45:56 MoveFileWithProgress

09:45:56 NtQueryFullAttributes

09:45:56 09:45:56 NtCreateFile [3 times]

09:45:56 NtOpenFile

09:45:56 NtQueryFullAttributes

09:45:56 MoveFileWithProgress

09:45:56 NtQueryFullAttributes

09:45:56 09:45:56 NtCreateFile [3 times]

09:45:56 NtOpenFile

09:45:56 NtQueryFullAttributes

09:45:56 MoveFileWithProgress

09:45:56 NtQueryFullAttributes

09:45:56 09:45:56 NtCreateFile [3 times]

09:45:56 NtOpenFile

09:45:56 09:45:57 MoveFileWithProgressW [6 times]

09:45:57 CopyFileW

09:45:57 NtQueryFullAttributes

09:45:58 MoveFileWithProgress

09:45:58 NtQueryFullAttributes

09:45:58 09:45:58 NtCreateFile [3 times]

09:45:58 NtOpenFile

09:45:58 NtQueryFullAttributes

09:45:58 MoveFileWithProgress

09:45:58 NtQueryFullAttributes

09:45:58 09:45:58 NtCreateFile [3 times]

09:45:58 NtOpenFile

09:45:58 NtQueryFullAttributes

09:45:58 MoveFileWithProgress

09:45:58 NtQueryFullAttributes

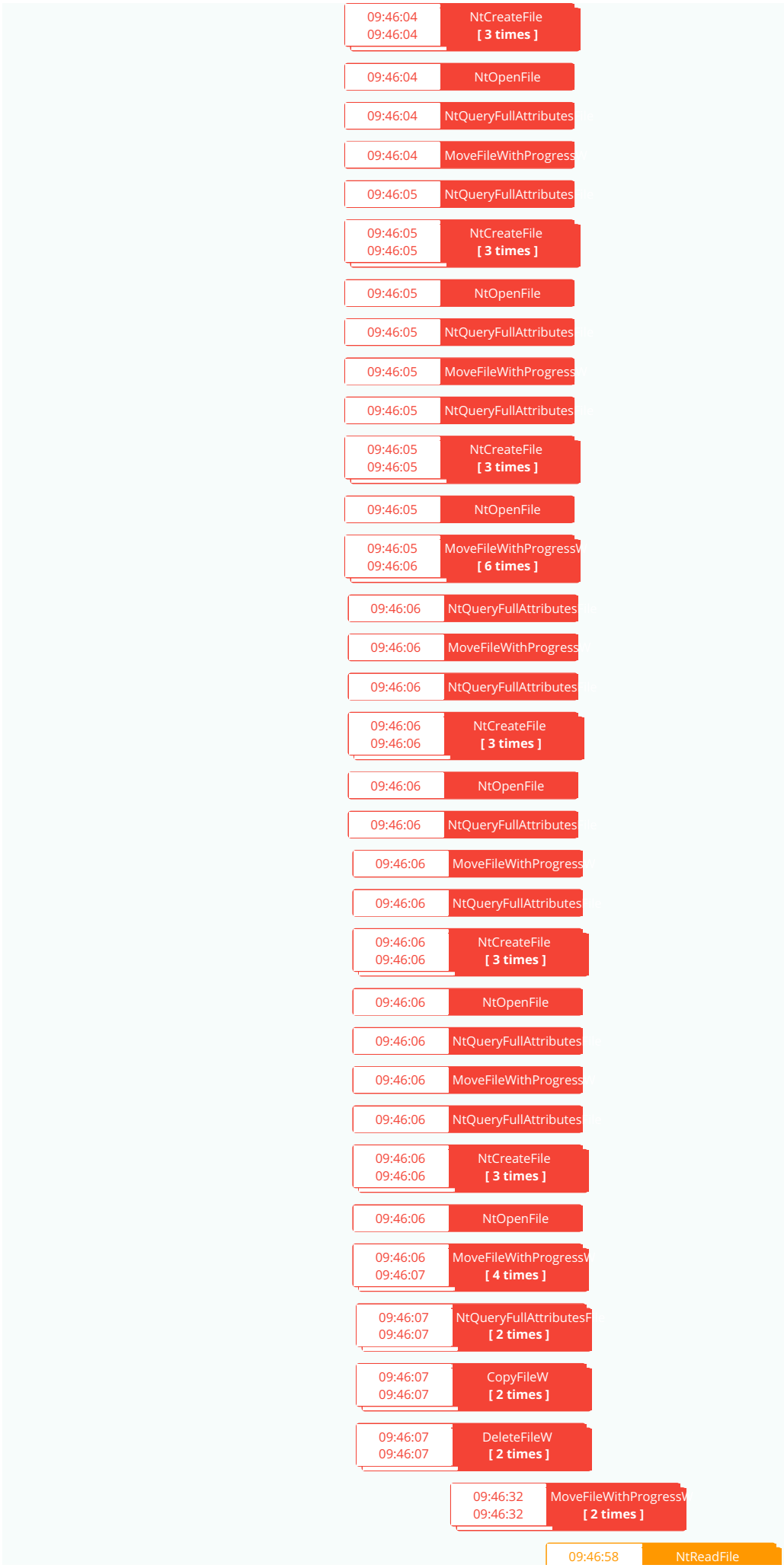
09:45:58 09:45:58 NtCreateFile [3 times]

09:45:58 NtOpenFile

09:45:58 NtQueryFullAttributes

09:45:58	MoveFileWithProgress
09:45:58	NtQueryFullAttributes
09:45:58 09:45:58	NtCreateFile **[3 times]**
09:45:58	NtOpenFile
09:45:58 09:45:59	MoveFileWithProgress **[6 times]**
09:46:00	NtQueryFullAttributes
09:46:00	MoveFileWithProgress
09:46:00	NtQueryFullAttributes
09:46:00 09:46:00	NtCreateFile **[3 times]**
09:46:00	NtOpenFile
09:46:00	NtQueryFullAttributes
09:46:00	MoveFileWithProgress
09:46:00	NtQueryFullAttributes
09:46:00 09:46:00	NtCreateFile **[3 times]**
09:46:00	NtOpenFile
09:46:00	NtQueryFullAttributes
09:46:00	MoveFileWithProgress
09:46:00	NtQueryFullAttributes
09:46:00 09:46:00	NtCreateFile **[3 times]**
09:46:00	NtOpenFile
09:46:00 09:46:01	MoveFileWithProgress **[4 times]**
09:46:01	NtQueryFullAttributes
09:46:01	MoveFileWithProgress
09:46:01	NtQueryFullAttributes
09:46:01 09:46:01	NtCreateFile **[3 times]**
09:46:01	NtOpenFile
09:46:01	NtQueryFullAttributes
09:46:01	MoveFileWithProgress
09:46:01	NtQueryFullAttributes
09:46:01 09:46:01	NtCreateFile **[3 times]**
09:46:01	NtOpenFile
09:46:01	NtQueryFullAttributes
09:46:01	MoveFileWithProgress
09:46:01	NtQueryFullAttributes
09:46:01 09:46:01	NtCreateFile **[3 times]**

Time	Event
09:46:01	NtOpenFile
09:46:01	NtQueryFullAttributes
09:46:02	MoveFileWithProgress
09:46:02	NtQueryFullAttributes
09:46:02 09:46:02	NtCreateFile **[3 times]**
09:46:02	NtOpenFile
09:46:02 09:46:03	MoveFileWithProgressW **[6 times]**
09:46:03	NtQueryFullAttributes
09:46:03	MoveFileWithProgress
09:46:03	NtQueryFullAttributes
09:46:03 09:46:03	NtCreateFile **[3 times]**
09:46:03	NtOpenFile
09:46:03	NtQueryFullAttributes
09:46:03	MoveFileWithProgress
09:46:03	NtQueryFullAttributes
09:46:03 09:46:03	NtCreateFile **[3 times]**
09:46:03	NtOpenFile
09:46:03	NtQueryFullAttributes
09:46:03	MoveFileWithProgress
09:46:03	NtQueryFullAttributes
09:46:03 09:46:03	NtCreateFile **[3 times]**
09:46:03	NtOpenFile
09:46:03	NtQueryFullAttributes
09:46:03	MoveFileWithProgress
09:46:03	NtQueryFullAttributes
09:46:03 09:46:03	NtCreateFile **[3 times]**
09:46:03	NtOpenFile
09:46:03 09:46:04	MoveFileWithProgressW **[6 times]**
09:46:04	NtQueryFullAttributes
09:46:04	MoveFileWithProgress
09:46:04	NtQueryFullAttributes
09:46:04 09:46:04	NtCreateFile **[3 times]**
09:46:04	NtOpenFile
09:46:04	NtQueryFullAttributes
09:46:04	MoveFileWithProgress
09:46:04	NtQueryFullAttributes


09:46:04 09:46:04 NtCreateFile [3 times]
09:46:04 NtOpenFile
09:46:04 NtQueryFullAttributes
09:46:04 MoveFileWithProgress
09:46:05 NtQueryFullAttributes
09:46:05 09:46:05 NtCreateFile [3 times]
09:46:05 NtOpenFile
09:46:05 NtQueryFullAttributes
09:46:05 MoveFileWithProgress
09:46:05 NtQueryFullAttributes
09:46:05 09:46:05 NtCreateFile [3 times]
09:46:05 NtOpenFile
09:46:05 09:46:06 MoveFileWithProgressW [6 times]
09:46:06 NtQueryFullAttributes
09:46:06 MoveFileWithProgress
09:46:06 NtQueryFullAttributes
09:46:06 09:46:06 NtCreateFile [3 times]
09:46:06 NtOpenFile
09:46:06 NtQueryFullAttributes
09:46:06 MoveFileWithProgress
09:46:06 NtQueryFullAttributes
09:46:06 09:46:06 NtCreateFile [3 times]
09:46:06 NtOpenFile
09:46:06 NtQueryFullAttributes
09:46:06 MoveFileWithProgress
09:46:06 NtQueryFullAttributes
09:46:06 09:46:06 NtCreateFile [3 times]
09:46:06 NtOpenFile
09:46:06 09:46:07 MoveFileWithProgressW [4 times]
09:46:07 09:46:07 NtQueryFullAttributesF [2 times]
09:46:07 09:46:07 CopyFileW [2 times]
09:46:07 09:46:07 DeleteFileW [2 times]
09:46:32 09:46:32 MoveFileWithProgressW [2 times]
09:46:58 NtReadFile

09:46:58 [2 times]

09:47:01 NtTerminateProcess

PID 584

09:45:17 **Create Process** The malicious file created a child process as svchost.exe **(PPID 460)**

09:45:24 Create Process

PID 2496

09:45:28 **Create Process** The malicious file created a child process as WmiPrvSE.exe **(PPID 584)**

09:45:28 NtDelayExecution

09:45:34 RegQueryValueExW

09:46:10
09:46:11 NtCreateFile **[6 times]**

PID 2516

09:45:23 **Create Process** The malicious file created a child process as svchost.exe **(PPID 460)**

09:45:25 RegOpenKeyExW

PID 460

09:46:19 **Create Process** The malicious file created a child process as services.exe **(PPID 352)**

09:46:20 Create Process

09:47:57
09:48:28 GetSystemTimeAsFileTi **[3 times]**

PID 2104

09:46:20 **Create Process** The malicious file created a child process as PresentationFontCache.exe **(PPID 460)**

VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

C:\Windows\System32\MSCOREE.DLL.local
C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscoreei.dll
C:\Windows\Microsoft.NET\Framework*
C:\Windows\Microsoft.NET\Framework\v1.0.3705\clr.dll
C:\Windows\Microsoft.NET\Framework\v1.0.3705\mscorwks.dll
C:\Windows\Microsoft.NET\Framework\v1.1.4322\clr.dll
C:\Windows\Microsoft.NET\Framework\v1.1.4322\mscorwks.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\clr.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll
C:\Windows\Microsoft.NET\Framework\v4.0.30319\clr.dll
C:\Users\user\AppData\Local\Temp\67eb0a16282599d3ead2977d264598fa31dd83f0.exe.config
C:\Users\user\AppData\Local\Temp\67eb0a16282599d3ead2977d264598fa31dd83f0.exe
C:\Users\user\AppData\Local\Temp\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Windows\System32\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Windows\system\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Windows\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\ProgramData\Oracle\Java\javapath\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Windows\System32\wbem\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Windows\System32\WindowsPowerShell\v1.0\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Program Files\Microsoft Network Monitor 3\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Program Files (x86)\Universal Extractor\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Program Files (x86)\Universal Extractor\bin\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Program Files (x86)\Windows Kits\8.1\Windows Performance Toolkit\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Python27\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Python27\Scripts\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\tools\sysinternals\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\tools\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\tools\IDA_Pro_v6\python\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Users\user\AppData\Local\Temp\67eb0a16282599d3ead2977d264598fa31dd83f0.exe.Local\
C:\Windows\winsxs\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_d08cc06a442b34fc
C:\Windows\winsxs\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_d08cc06a442b34fc\msvcr80.dll
C:\Windows

C:\Windows\winsxs
C:\Windows\Microsoft.NET\Framework\v4.0.30319
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config
C:\Windows\Microsoft.NET\Framework\v2.0.50727\fusion.localgac
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\security.config
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\security.config.cch
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\enterprisesec.config
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\enterprisesec.config.cch
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config.cch
C:\Windows\assembly\NativeImages_v2.0.50727_32\index126.dat
C:\Windows\assembly\NativeImages_v2.0.50727_32\mscorlib\62a0b3e4b40ec0e8c5cfaa0c8848e64a\mscorlib.ni.dll
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.INI
C:\Users
C:\Users\user
C:\Users\user\AppData
C:\Users\user\AppData\Local
C:\Users\user\AppData\Local\Temp
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorsec.dll
C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af
C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll
C:\Windows\System32\p2pcollab.dll
C:\Windows\System32\qagentrt.dll
C:\Windows\System32\dnsapi.dll
C:\Windows\System32\en-US\dnsapi.dll.mui
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates*
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\1233B8D21D2ECB0483D16253D1FF3964BD09EF0C
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\16B1DD478BCE71A0FB1822E8F4F30AB467BBEFD4
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\2064A97B987412930E2994D60AE7EB72D89BC4F7
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\37998502C2CC1852F8774DAF543DD76D10D6FD93
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\418C30DD41197CBAABF21675F8559794F5551115
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\44E5AE16D06F9FBB92D6D9444B5C65C0F331D0EC
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\4FDDCB932603534677ECAE8C7D0FD914FD443E83
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\5D247FE955609769879FB1DD016537EEF650B8EC
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\6A8C669D7D1D5759CE7C1E0C5BE286257C31F366

C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\744CDF45BF43EF285758286CAC89AF786F938342
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\761F091EA5F80A98B0D89734231D300CF9C027E8
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\7A5F1A5DE6AA551C795CC508128C6D894FA2C502
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\8291DA84F9266F6D0ED367AF8BE3FA722529EB91
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\871E3CD70B6F8EE3C1E7BE4C7BEF4FFCCE673E32
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\8A82FE0617F4170E0BF052CF6BABFC628DA51919
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\8B943CF0CAEF7F6F04E98C9405960323B23C516D
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\9317D002FC43BDA932B8397B6E729B83D48EEB8D
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\95EEF9A37407C5B87BCF95D69B01DCFDAFD07635

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\InstallRoot
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\CLRLoadLogDir
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\UseLegacyV2RuntimeActivationPolicyDefaultValue
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\OnlyUseLatestCLR
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Fusion\NoClientChecks
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\GCStressStart
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\GCStressStartAtJit
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\DisableConfigCache
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\CacheLocation
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\DownloadCacheQuotaInKB
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\EnableLog
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\LoggingLevel
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\ForceLog
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\LogFailures
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\VersioningLog
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\LogResourceBinds
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\UseLegacyIdentityFormat
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\DisableMSIPeek
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NoClientChecks
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DevOverrideEnable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\LatestIndex
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\index126\NIUsageMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\index126\ILUsageMask

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\ConfigMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\ConfigString
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\MVID
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\EvalationData
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\Status
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\ILDependencies
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\NIDependencies
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\MissingDependencies
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\7950e2c5\183e33de\83\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\7950e2c5\183e33de\83\Status
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\7950e2c5\183e33de\83\Modules
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\7950e2c5\183e33de\83\SIG
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\7950e2c5\183e33de\83\LastModTime
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\GACChangeNotification\Default\mscorlib,2.0.0.0,,b77a5c561934e089,x86
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\crypt32\DebugHeapFlags
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\Certificate\{31D1ADC1-D329-11D1-8ED8-0080C76516C6}\$DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\Certificate\{31D1ADC1-D329-11D1-8ED8-0080C76516C6}\$Function
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\FinalPolicy\{31D1ADC1-D329-11D1-8ED8-0080C76516C6}\$DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\FinalPolicy\{31D1ADC1-D329-11D1-8ED8-0080C76516C6}\$Function
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\Initialization\{31D1ADC1-D329-11D1-8ED8-0080C76516C6}\$DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\Initialization\{31D1ADC1-D329-11D1-8ED8-0080C76516C6}\$Function
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\Message\{31D1ADC1-D329-11D1-8ED8-0080C76516C6}\$DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\Message\{31D1ADC1-D329-11D1-8ED8-0080C76516C6}\$Function
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\Signature\{31D1ADC1-D329-11D1-8ED8-0080C76516C6}\$DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\Signature\{31D1ADC1-D329-11D1-8ED8-0080C76516C6}\$Function
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\CertCheck\{31D1ADC1-D329-11D1-8ED8-0080C76516C6}\$DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\CertCheck\{31D1ADC1-D329-11D1-8ED8-0080C76516C6}\$Function
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing\State
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Security\Safety Warning Level
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\crypt32\DiagLevel
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\crypt32\DiagMatchAnyMask

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 0\CryptDllFindOIDInfo\1.3.6.1.4.1.311.44.3.4!7\Name
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\MUI\StringCacheSettings\StringCacheGeneration
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\p2pcollab.dll,-8042
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 0\CryptDllFindOIDInfo\1.3.6.1.4.1.311.47.1.1!7\Name
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 0\CryptDllFindOIDInfo\1.3.6.1.4.1.311.64.1.1!7\Name
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\dnsapi.dll,-103
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\SystemCertificates\AuthRoot\DisableRootAutoUpdate
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\AutoUpdate\DisallowedCertSyncDeltaTime
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\DisableMandatoryBasicConstraints
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\DisableCANameConstraints
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\DisableUnsupportedCriticalExtensions
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\MaxAIAUrlCountInCert
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\MaxAIAUrlRetrievalCountPerChain
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\MaxUrlRetrievalByteCount
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\MaxAIAUrlRetrievalByteCount
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\MaxAIAUrlRetrievalCertCount
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\CryptnetPreFetchTriggerPeriodSeconds
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\EnableWeakSignatureFlags
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\MinRsaPubKeyBitLength

MODIFIED FILES

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506
C:\Users\user\AppData\Local\Temp\CabDEDC.tmp
C:\Users\user\AppData\Local\Temp\TarDEDD.tmp
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\8890A77645B73478F5B1DED18ACBF795_B95A585585762F8B2D72E152F328449A
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\8890A77645B73478F5B1DED18ACBF795_B95A585585762F8B2D72E152F328449A
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\DE0101390D8E4B74E3DD39ACA5B00000_BCA65E535E79DBF987FC1C7A3D60D995
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\DE0101390D8E4B74E3DD39ACA5B00000_BCA65E535E79DBF987FC1C7A3D60D995
C:\Users\user\AppData\Local\Temp\logs\main.log

C:\Users\user\AppData\Local\Temp\data\prefs.jdat
C:\Users\user\AppData\Local\Temp\data\sdet.jdat
C:\Users\user\AppData\Roaming\TotalAV\3.0.0\avira32redist.zip
C:\Users\user\AppData\Local\Temp\installoptions.jdat
C:\Users\user\AppData\Local\Temp\SAVAPI\0bg2nfrj.nlb
C:\Users\user\AppData\Local\Temp\SAVAPI\aebb.dll
C:\Users\user\AppData\Local\Temp\SAVAPI\q2hu5l5j.2fm
C:\Users\user\AppData\Local\Temp\SAVAPI\aecore.dll
C:\Users\user\AppData\Local\Temp\SAVAPI\b3uez3lj.pg0
C:\Users\user\AppData\Local\Temp\SAVAPI\aecrypto.dll
C:\Users\user\AppData\Local\Temp\SAVAPI\niq3mj4r.ota
C:\Users\user\AppData\Local\Temp\SAVAPI\aedroid.dll
C:\Users\user\AppData\Local\Temp\SAVAPI\tv0a2ltz.s2v
C:\Users\user\AppData\Local\Temp\SAVAPI\aeemu.dll
C:\Users\user\AppData\Local\Temp\SAVAPI\pl4c3rxy.ro1
C:\Users\user\AppData\Local\Temp\SAVAPI\aeexp.dll
C:\Users\user\AppData\Local\Temp\SAVAPI\0uayvcvt.a24
C:\Users\user\AppData\Local\Temp\SAVAPI\aegen.dll
C:\Users\user\AppData\Local\Temp\SAVAPI\mhnom3gg.bei
C:\Users\user\AppData\Local\Temp\SAVAPI\aehelp.dll
C:\Users\user\AppData\Local\Temp\SAVAPI\unbw5yxs.c4q
C:\Users\user\AppData\Local\Temp\SAVAPI\aeheur.dll
C:\Users\user\AppData\Local\Temp\SAVAPI\kgo3v0ql.fbh
C:\Users\user\AppData\Local\Temp\SAVAPI\aelibinf.dll
C:\Users\user\AppData\Local\Temp\SAVAPI\bempms2y.joz
C:\Users\user\AppData\Local\Temp\SAVAPI\aelidb.dat
C:\Users\user\AppData\Local\Temp\SAVAPI\vpdxkudi.z2q
C:\Users\user\AppData\Local\Temp\SAVAPI\aemobile.dll
C:\Users\user\AppData\Local\Temp\SAVAPI\r2orkg03.nvl
C:\Users\user\AppData\Local\Temp\SAVAPI\aemvdb.dat
C:\Users\user\AppData\Local\Temp\SAVAPI\aiskpuas.dm3
C:\Users\user\AppData\Local\Temp\SAVAPI\aeoffice.dll
C:\Users\user\AppData\Local\Temp\SAVAPI\dgb1loea.g20
C:\Users\user\AppData\Local\Temp\SAVAPI\aepack.dll
C:\Users\user\AppData\Local\Temp\SAVAPI\sea24ktc.wve

C:\Users\user\AppData\Local\Temp\SAVAPI\aerdl.dll
C:\Users\user\AppData\Local\Temp\SAVAPI\hioe1s40.2w5
C:\Users\user\AppData\Local\Temp\SAVAPI\aesbx.dll
C:\Users\user\AppData\Local\Temp\SAVAPI\crwfmbeb.jic
C:\Users\user\AppData\Local\Temp\SAVAPI\aescn.dll
C:\Users\user\AppData\Local\Temp\SAVAPI\eg4kwk42.a3n
C:\Users\user\AppData\Local\Temp\SAVAPI\aescript.dll
C:\Users\user\AppData\Local\Temp\SAVAPI\h52ahx1z.dbw
C:\Users\user\AppData\Local\Temp\SAVAPI\aeset.dat
C:\Users\user\AppData\Local\Temp\SAVAPI\5zvu5ybb.1qs
C:\Users\user\AppData\Local\Temp\SAVAPI\aevdf.dat
C:\Users\user\AppData\Local\Temp\SAVAPI\5k5ftaqd.0ys
C:\Users\user\AppData\Local\Temp\SAVAPI\aevdf.dll
C:\Users\user\AppData\Local\Temp\SAVAPI\cer3rh0h.zqn
C:\Users\user\AppData\Local\Temp\SAVAPI\apcfile.dll
C:\Users\user\AppData\Local\Temp\SAVAPI\wjo50igi.mse
C:\Users\user\AppData\Local\Temp\SAVAPI\apchash.dll
C:\Users\user\AppData\Local\Temp\SAVAPI\2ldq44pa.orm
C:\Users\user\AppData\Local\Temp\SAVAPI\avupdate-savapilib-engine.conf
C:\Users\user\AppData\Local\Temp\SAVAPI\tz2luugb.vxt
C:\Users\user\AppData\Local\Temp\SAVAPI\avupdate.exe
C:\Users\user\AppData\Local\Temp\SAVAPI\px3d5aa2.t13
C:\Users\user\AppData\Local\Temp\SAVAPI\avupdate_msg.avr
C:\Users\user\AppData\Local\Temp\SAVAPI\xwvxdify.1jl
C:\Users\user\AppData\Local\Temp\SAVAPI\cacert.crt
C:\Users\user\AppData\Local\Temp\SAVAPI\o4lcddce.bgh
C:\Users\user\AppData\Local\Temp\SAVAPI\msvcp120.dll
C:\Users\user\AppData\Local\Temp\SAVAPI\3pklbpwr.sc4
C:\Users\user\AppData\Local\Temp\SAVAPI\msvcr120.dll
C:\Users\user\AppData\Local\Temp\SAVAPI\dj4xtjiw.ozn

RESOLVED APIS

advapi32.dll.RegOpenKeyExW
advapi32.dll.RegQueryInfoKeyW
advapi32.dll.RegEnumKeyExW

advapi32.dll.RegEnumValueW
advapi32.dll.RegCloseKey
advapi32.dll.RegQueryValueExW
kernel32.dll.FlsAlloc
kernel32.dll.FlsFree
kernel32.dll.FlsGetValue
kernel32.dll.FlsSetValue
kernel32.dll.InitializeCriticalSectionEx
kernel32.dll.CreateEventExW
kernel32.dll.CreateSemaphoreExW
kernel32.dll.SetThreadStackGuarantee
kernel32.dll.CreateThreadpoolTimer
kernel32.dll.SetThreadpoolTimer
kernel32.dll.WaitForThreadpoolTimerCallbacks
kernel32.dll.CloseThreadpoolTimer
kernel32.dll.CreateThreadpoolWait
kernel32.dll.SetThreadpoolWait
kernel32.dll.CloseThreadpoolWait
kernel32.dll.FlushProcessWriteBuffers
kernel32.dll.FreeLibraryWhenCallbackReturns
kernel32.dll.GetCurrentProcessorNumber
kernel32.dll.GetLogicalProcessorInformation
kernel32.dll.CreateSymbolicLinkW
kernel32.dll.EnumSystemLocalesEx
kernel32.dll.CompareStringEx
kernel32.dll.GetDateFormatEx
kernel32.dll.GetLocaleInfoEx
kernel32.dll.GetTimeFormatEx
kernel32.dll.GetUserDefaultLocaleName
kernel32.dll.IsValidLocaleName
kernel32.dll.LCMapStringEx
kernel32.dll.GetTickCount64
advapi32.dll.EventRegister
mscoree.dll.#142
mscoreei.dll.RegisterShimImplCallback

mscoreei.dll.OnShimDllMainCalled
mscoreei.dll._CorExeMain
shlwapi.dll.UrlIsW
version.dll.GetFileVersionInfoSizeW
version.dll.GetFileVersionInfoW
version.dll.VerQueryValueW
kernel32.dll.InitializeCriticalSectionAndSpinCount
kernel32.dll.IsProcessorFeaturePresent
msvcrt.dll._set_error_mode
msvcrt.dll.?set_terminate@@YAP6AXXZP6AXXZ@Z
kernel32.dll.FindActCtxSectionStringW
kernel32.dll.GetSystemWindowsDirectoryW
mscoree.dll.GetProcessExecutableHeap
mscoreei.dll.GetProcessExecutableHeap
mscorwks.dll._CorExeMain
mscorwks.dll.GetCLRFunction
advapi32.dll.RegisterTraceGuidsW
advapi32.dll.UnregisterTraceGuids
advapi32.dll.GetTraceLoggerHandle
advapi32.dll.GetTraceEnableLevel
advapi32.dll.GetTraceEnableFlags
advapi32.dll.TraceEvent
mscoree.dll.IEE
mscoreei.dll.IEE
mscorwks.dll.IEE
mscoree.dll.GetStartupFlags
mscoreei.dll.GetStartupFlags
mscoree.dll.GetHostConfigurationFile
mscoreei.dll.GetHostConfigurationFile
mscoreei.dll.GetCORVersion
mscoree.dll.GetCORSystemDirectory
mscoreei.dll.GetCORSystemDirectory_RetAddr
mscoreei.dll.CreateConfigStream
ntdll.dll.RtlUnwind

kernel32.dll.IsWow64Process
advapi32.dll.AllocateAndInitializeSid
advapi32.dll.OpenProcessToken
advapi32.dll.GetTokenInformation

DELETED FILES

C:\Users\user\AppData\Local\Temp\CabDEDC.tmp
C:\Users\user\AppData\Local\Temp\TarDEDD.tmp
C:\Users\user\AppData\Local\Temp\SAVAPI\0bg2nfrj.nlb
C:\Users\user\AppData\Local\Temp\SAVAPI\q2hu5l5j.2fm
C:\Users\user\AppData\Local\Temp\SAVAPI\b3uez3lj.pg0
C:\Users\user\AppData\Local\Temp\SAVAPI\niq3mj4r.ota
C:\Users\user\AppData\Local\Temp\SAVAPI\tv0a2ltz.s2v
C:\Users\user\AppData\Local\Temp\SAVAPI\pl4c3rxy.ro1
C:\Users\user\AppData\Local\Temp\SAVAPI\0uayvcvt.a24
C:\Users\user\AppData\Local\Temp\SAVAPI\mhnom3gg.bei
C:\Users\user\AppData\Local\Temp\SAVAPI\unbw5yxs.c4q
C:\Users\user\AppData\Local\Temp\SAVAPI\kgo3v0ql.fbh
C:\Users\user\AppData\Local\Temp\SAVAPI\bempms2y.joz
C:\Users\user\AppData\Local\Temp\SAVAPI\vpdxkudi.z2q
C:\Users\user\AppData\Local\Temp\SAVAPI\r2orkg03.nvl
C:\Users\user\AppData\Local\Temp\SAVAPI\aiskpuas.dm3
C:\Users\user\AppData\Local\Temp\SAVAPI\dgb1loea.g20
C:\Users\user\AppData\Local\Temp\SAVAPI\sea24ktc.wve
C:\Users\user\AppData\Local\Temp\SAVAPI\hioe1s40.2w5
C:\Users\user\AppData\Local\Temp\SAVAPI\crwfmbeb.jic
C:\Users\user\AppData\Local\Temp\SAVAPI\eg4kwk42.a3n
C:\Users\user\AppData\Local\Temp\SAVAPI\h52ahx1z.dbw
C:\Users\user\AppData\Local\Temp\SAVAPI\5zvu5ybb.1qs
C:\Users\user\AppData\Local\Temp\SAVAPI\5k5ftaqd.0ys
C:\Users\user\AppData\Local\Temp\SAVAPI\cer3rh0h.zqn
C:\Users\user\AppData\Local\Temp\SAVAPI\wjo50igi.mse
C:\Users\user\AppData\Local\Temp\SAVAPI\2ldq44pa.orm
C:\Users\user\AppData\Local\Temp\SAVAPI\tz2luugb.vxt
C:\Users\user\AppData\Local\Temp\SAVAPI\px3d5aa2.t13

C:\Users\user\AppData\Local\Temp\SAVAPI\xwvxdify.1jl
C:\Users\user\AppData\Local\Temp\SAVAPI\o4lcddce.bgh
C:\Users\user\AppData\Local\Temp\SAVAPI\3pklbpwr.sc4
C:\Users\user\AppData\Local\Temp\SAVAPI\dj4xtjiw.ozn
C:\Users\user\AppData\Local\Temp\SAVAPI\epk3nucs.tum
C:\Users\user\AppData\Local\Temp\SAVAPI\mnbd4hbl.1vx
C:\Users\user\AppData\Local\Temp\SAVAPI\5bvxhhtd.11t
C:\Users\user\AppData\Local\Temp\SAVAPI\on_access\x31werag.m12
C:\Users\user\AppData\Local\Temp\SAVAPI\on_access\immhbeij.vad
C:\Users\user\AppData\Local\Temp\SAVAPI\on_access\krarcl4z.umt
C:\Users\user\AppData\Local\Temp\SAVAPI\on_access\utils\qm4rbvfr.msk
C:\Users\user\AppData\Local\Temp\SAVAPI\on_access\utils\e4y4bpu1.rcf
C:\Users\user\AppData\Local\Temp\SAVAPI\on_access\utils\ig4ususz.nz3
C:\Users\user\AppData\Local\Temp\SAVAPI\on_access\utils\o2zhqpss.1qn
C:\Users\user\AppData\Local\Temp\SAVAPI\on_access\win32\vista\w2ss4uox.evn
C:\Users\user\AppData\Local\Temp\SAVAPI\on_access\win32\vista\len4vm1u.bjd
C:\Users\user\AppData\Local\Temp\SAVAPI\on_access\win32\vista\uhq5meip.gsl
C:\Users\user\AppData\Local\Temp\SAVAPI\on_access\win32\vista\33m3xgt1.oyw
C:\Users\user\AppData\Local\Temp\SAVAPI\on_access\win32\vista\44m5b0d4.p0h
C:\Users\user\AppData\Local\Temp\SAVAPI\on_access\win32\vista\h2g3jyve.mrj
C:\Users\user\AppData\Local\Temp\SAVAPI\on_access\win32\vista\vv2sses1.rok
C:\Users\user\AppData\Local\Temp\SAVAPI\on_access\win32\win7\dwhuy3rz.2lu
C:\Users\user\AppData\Local\Temp\SAVAPI\on_access\win32\win7\p3aj5mey.utp
C:\Users\user\AppData\Local\Temp\SAVAPI\on_access\win32\win7\ooodbgf3.qzi
C:\Users\user\AppData\Local\Temp\SAVAPI\on_access\win32\win7\tpsw0opf.mej
C:\Users\user\AppData\Local\Temp\SAVAPI\on_access\win32\win7\h2r1qwoh.mdo
C:\Users\user\AppData\Local\Temp\SAVAPI\on_access\win32\win7\ycv4vgnb.4bk
C:\Users\user\AppData\Local\Temp\SAVAPI\on_access\win32\win7\ca1aq1wf.yld
C:\Users\user\AppData\Local\Temp\SAVAPI\on_access\win32\win7\x0w2bpom.0si
C:\Users\user\AppData\Local\Temp\SAVAPI\on_access\win32\win7\kxzhfcmv.fxc
C:\Users\user\AppData\Local\Temp\SAVAPI\on_access\win32\win7\jwcjkafz.tfl
C:\Users\user\AppData\Local\Temp\SAVAPI\on_access\win32\win8\x12pmzrw.fff
C:\Users\user\AppData\Local\Temp\SAVAPI\on_access\win32\win8\0qewyf0p.cc4
C:\Users\user\AppData\Local\Temp\SAVAPI\on_access\win32\win8\rg1emohx.xvr
C:\Users\user\AppData\Local\Temp\SAVAPI\on_access\win32\win8\01l5q3p5.kkc

C:\Users\user\AppData\Local\Temp\SAVAPI\on_access\win32\win8\wzf3rdjj.vhx
C:\Users\user\AppData\Local\Temp\SAVAPI\on_access\win32\win8\u4ulujiy.vrq
C:\Users\user\AppData\Local\Temp\SAVAPI\on_access\win32\win8\1zi5aneo.qq4
C:\Users\user\AppData\Local\Temp\SAVAPI\on_access\win32\win8\lj2z4ec5.age
C:\Users\user\AppData\Local\Temp\SAVAPI\on_access\win32\win8\oqhakkyj.45v
C:\Users\user\AppData\Local\Temp\SAVAPI\on_access\win32\win8\upxncxdw.mk1
C:\Users\user\AppData\Local\Temp\SAVAPI\on_access\win32\xp\q2gfzfi2.nus
C:\Users\user\AppData\Local\Temp\SAVAPI\on_access\win32\xp\rixpythy.kka
C:\Users\user\AppData\Local\Temp\SAVAPI\on_access\win32\xp\35fk0v3p.xi5
C:\Users\user\AppData\Local\Temp\SAVAPI\on_access\win32\xp\tqoqme05.xto
C:\Users\user\AppData\Local\Temp\SAVAPI\on_access\win32\xp\5xoap522.h1r
C:\Users\user\AppData\Local\Temp\SAVAPI\on_access\win32\xp\t3neeffs.evj

REGISTRY KEYS

HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\Policy\
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\Policy\v4.0
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\InstallRoot
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\CLRLoadLogDir
HKEY_CURRENT_USER\Software\Microsoft\.NETFramework
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\UseLegacyV2RuntimeActivationPolicyDefaultValue
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\OnlyUseLatestCLR
Policy\Standards
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\Policy\Standards
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\Policy\Standards\v2.0.50727
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Fusion\NoClientChecks
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide\AssemblyStorageRoots
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\GCStressStart
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\GCStressStartAtJit
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\DisableConfigCache
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\Policy\AppPatch
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\Policy\AppPatch\v4.0.30319.00000

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\Policy\AppPatch\v4.0.30319.00000\mscorwks.dll
HKEY_LOCAL_MACHINE\Software\Microsoft\Fusion
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\67eb0a16282599d3ead2977d264598fa31dd83f0.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\CacheLocation
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\DownloadCacheQuotaInKB
HKEY_CURRENT_USER\Software\Microsoft\Fusion
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\EnableLog
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\LoggingLevel
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\ForceLog
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\LogFailures
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\VersioningLog
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\LogResourceBinds
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\UseLegacyIdentityFormat
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\DisableMSIPeek
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NoClientChecks
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DevOverrideEnable
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\Security\Policy\Extensions\NamedPermissionSets
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\Security\Policy\Extensions\NamedPermissionSets\Internet
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\Security\Policy\Extensions\NamedPermissionSets\LocalIntranet
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2298303332-66077612-2598613238-1000
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\v2.0.50727\Security\Policy
HKEY_LOCAL_MACHINE\Software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\LatestIndex
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\index126
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\index126\NIUsageMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\index126\ILUsageMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\ConfigMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\ConfigString
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\MVID
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\EvalationData
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\Status

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\ILDependencies
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\NIDependencies
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\MissingDependencies
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\7950e2c5\183e33de\83
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\7950e2c5\183e33de\83\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\7950e2c5\183e33de\83\Status
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\7950e2c5\183e33de\83\Modules
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\7950e2c5\183e33de\83\SIG
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\7950e2c5\183e33de\83\LastModTime
HKEY_LOCAL_MACHINE\Software\Microsoft\Fusion\GACChangeNotification\Default
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\GACChangeNotification\Default\mscorlib,2.0.0.0,,b77a5c561934e089,x86
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\crypt32
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\crypt32\DebugHeapFlags
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\msasn1
HKEY_CURRENT_USER
HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\Providers\Trust\Certificate\{31D1ADC1-D329-11D1-8ED8-0080C76516C6}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\Certificate\{31D1ADC1-D329-11D1-8ED8-0080C76516C6}\$DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\Certificate\{31D1ADC1-D329-11D1-8ED8-0080C76516C6}\$Function
HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\Providers\Trust\FinalPolicy\{31D1ADC1-D329-11D1-8ED8-0080C76516C6}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\FinalPolicy\{31D1ADC1-D329-11D1-8ED8-0080C76516C6}\$DLL

EXECUTED COMMANDS

C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
C:\Windows\Microsoft.Net\Framework64\v3.0\WPF\PresentationFontCache.exe

READ FILES

C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscoreei.dll
C:\Users\user\AppData\Local\Temp\67eb0a16282599d3ead2977d264598fa31dd83f0.exe.config
C:\Users\user\AppData\Local\Temp\67eb0a16282599d3ead2977d264598fa31dd83f0.exe
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll
C:\Windows\winsxs\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_d08cc06a442b34fc\msvcr80.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\security.config
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\security.config.cch
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\enterprisesec.config

C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\enterprisesec.config.cch
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config.cch
C:\Windows\assembly\NativeImages_v2.0.50727_32\index126.dat
C:\Windows\assembly\NativeImages_v2.0.50727_32\mscorlib\62a0b3e4b40ec0e8c5cfaa0c8848e64a\mscorlib.ni.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorsec.dll
C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll
C:\Windows\System32\p2pcollab.dll
C:\Windows\System32\dnsapi.dll
C:\Windows\System32\en-US\dnsapi.dll.mui
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\1233B8D21D2ECB0483D16253D1FF3964BD09EF0C
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\16B1DD478BCE71A0FB1822E8F4F30AB467BBEFD4
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\2064A97B987412930E2994D60AE7EB72D89BC4F7
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\37998502C2CC1852F8774DAF543DD76D10D6FD93
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\418C30DD41197CBAABF21675F8559794F5551115
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\44E5AE16D06F9FBB92D6D9444B5C65C0F331D0EC
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\4FDDCB932603534677ECAE8C7D0FD914FD443E83
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\5D247FE955609769879FB1DD016537EEF650B8EC
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\6A8C669D7D1D5759CE7C1E0C5BE286257C31F366
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\744CDF45BF43EF285758286CAC89AF786F938342
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\761F091EA5F80A98B0D89734231D300CF9C027E8
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\7A5F1A5DE6AA551C795CC508128C6D894FA2C502
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\8291DA84F9266F6D0ED367AF8BE3FA722529EB91
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\871E3CD70B6F8EE3C1E7BE4C7BEF4FFCCE673E32
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\8A82FE0617F4170E0BF052CF6BABFC628DA51919
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\8B943CF0CAEF7F6F04E98C9405960323B23C516D
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\9317D002FC43BDA932B8397B6E729B83D48EEB8D
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\95EEF9A37407C5B87BCF95D69B01DCFDAFD07635
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\A092A81885DDD5AAD1EC1A803D7183779D81B6F9
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\BAED8A8C5A147CFA78E686BB4A8E5829C2F934F5
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\C8A51E044BF5AF39158BB24E414E8FDCD2891C3A
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\FB45378AB288E369B22C860D123A809F530D5CC1
C:\Windows\System32\en-US\WINHTTP.dll.mui
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

C:\Users\user\AppData\Local\Temp\CabDEDC.tmp

C:\Users\user\AppData\Local\Temp\TarDEDD.tmp

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\8890A77645B73478F5B1DED18ACBF795_B95A585585762F8B2D72E152F328449A

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\8890A77645B73478F5B1DED18ACBF795_B95A585585762F8B2D72E152F328449A

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\DE0101390D8E4B74E3DD39ACA5B00000_BCA65E535E79DBF987FC1C7A3D60D995

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\DE0101390D8E4B74E3DD39ACA5B00000_BCA65E535E79DBF987FC1C7A3D60D995

C:\Windows\System32\l_intl.nls

C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorjit.dll

C:\Windows\assembly\pubpol20.dat

C:\Windows\assembly\NativeImages_v2.0.50727_32\System\9e0a3b9b9f457233a335d7fba8f95419\System.ni.dll

C:\Windows\assembly\NativeImages_v2.0.50727_32\WindowsBase\cf293040f3a93afa1ea782487acae816\WindowsBase.ni.dll

C:\Windows\assembly\NativeImages_v2.0.50727_32\PresentationCore\2ad23de8284d4594aa658dfb5e667d97\PresentationCore.ni.dll

C:\Windows\assembly\NativeImages_v2.0.50727_32\PresentationFramewo#\bfaf8f86e69928fb2f67987c0203f603\PresentationFramework.ni.dll

C:\Windows\assembly\GAC_32\PresentationCore\3.0.0.0__31bf3856ad364e35\PresentationCore.dll

C:\Windows\Microsoft.NET\Framework\v3.0\WPF\wpfgfx_v0300.dll

C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\sorttbls.nlp

C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\sortkey.nlp

C:\Windows\System32\tzres.dll

C:\Windows\assembly\GAC_32\PresentationCore\3.0.0.0__31bf3856ad364e35\wpfgfx_v0300.dll

C:\Windows\Microsoft.NET\Framework\v2.0.50727\Culture.dll

C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorrc.dll

C:\Windows\assembly\NativeImages_v2.0.50727_32\PresentationFramewo#\299d0b38053fd7cbd84bac2178c3703b\PresentationFramework.Aero.ni.dll

C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Xml\461d3b6b3f43e6fbe6c897d5936e17e4\System.Xml.ni.dll

C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Data\1e85062785e286cd9eae9c26d2c61f73\System.Data.ni.dll

C:\Windows\assembly\GAC_32\System.Data\2.0.0.0__b77a5c561934e089\System.Data.dll

C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Management\6f3b99ed0b791ff4d8aa52f2f0cd0bcf\System.Management.ni.dll

C:\Windows\Microsoft.NET\Framework\v2.0.50727\wminet_utils.dll

C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Configuration\bc09ad2d49d8535371845cd7532f9271\System.Configuration.ni.dll

C:\Users\user\AppData\Roaming\TotalAV\3.0.0\avira32redist.zip

C:\Users\user\AppData\Local\Temp\SAVAPI\0bg2nfrj.nlb

MUTEXES

Global\CLR_CASOFF_MUTEX

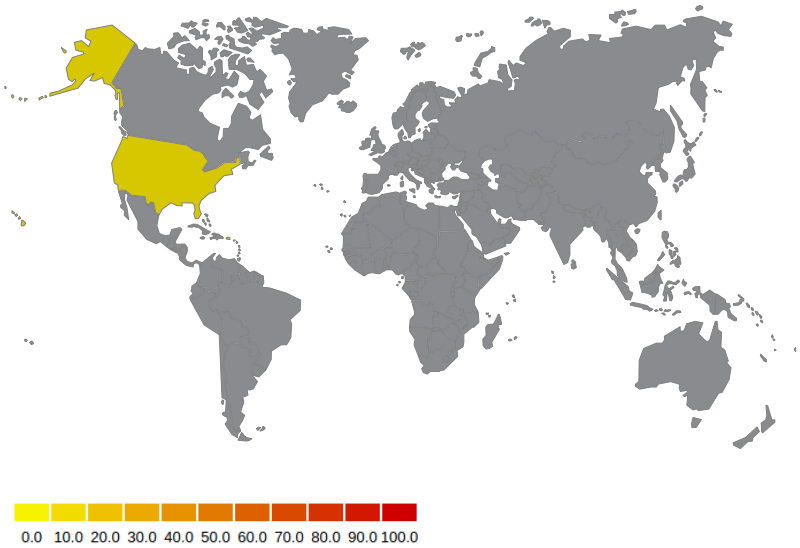
Local__DDrawExclMode__
Local__DDrawCheckExclMode__
Global\com.TotalAV.apprunning
Global\.net clr networking
DBWinMutex
CicLoadWinStaWinSta0
Local\MSCTF.CtfMonitorInstMutexDefault1

MODIFIED REGISTRY KEYS

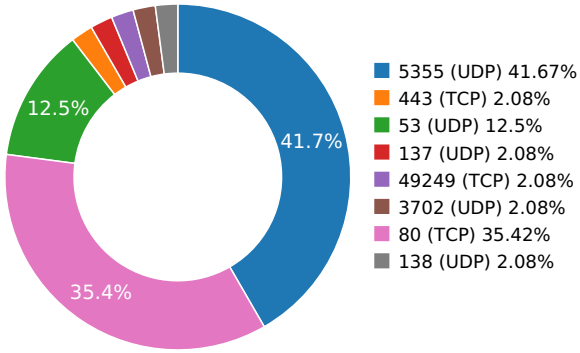
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\LanguageList
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\p2pcollab.dll,-8042
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\dnsapi.dll,-103
HKEY_LOCAL_MACHINE\Software\Microsoft\Tracing\67eb0a16282599d3ead2977d264598fa31dd83f0_RASAPI32
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\67eb0a16282599d3ead2977d264598fa31dd83f0_RASAPI32\EnableFileTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\67eb0a16282599d3ead2977d264598fa31dd83f0_RASAPI32\EnableConsoleTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\67eb0a16282599d3ead2977d264598fa31dd83f0_RASAPI32\FileTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\67eb0a16282599d3ead2977d264598fa31dd83f0_RASAPI32\ConsoleTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\67eb0a16282599d3ead2977d264598fa31dd83f0_RASAPI32\MaxFileSize
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\67eb0a16282599d3ead2977d264598fa31dd83f0_RASAPI32\FileDirectory
HKEY_CURRENT_USER\SOFTWARE\Classes\CLSID\{d79b57ed-727c-4ab8-ba67-e7c6fd30fac1}\LocalServer32
HKEY_CURRENT_USER\Software\Classes\Wow6432Node\CLSID\{d79b57ed-727c-4ab8-ba67-e7c6fd30fac1}\LocalServer32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\LastServiceStart
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Transports\Decoupled\Server
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Server\CreationTime
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Server\MarshaledProxy
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Server\ProcessIdentifier
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\ConfigValueEssNeedsLoading
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\List of event-active namespaces
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\ESS\//./root/CIMV2\SCM Event Provider

Network Behavior

CONTACTED IPS



NETWORK PORT DISTRIBUTION



Name	IP	Country	ASN	ASN Name	Trigger Process Type
	8.8.4.4	United States	15169	Level 3 Parent, LLC	Malware Process
	104.18.20.226	United States	13335	Cloudflare, Inc.	Malware Process
	23.215.131.176	United States	20940	Akamai Technologies, Inc.	OS Process
	23.215.131.200	United States	20940	Akamai Technologies, Inc.	OS Process
	23.23.157.142	United States	14618	Amazon.com, Inc.	Malware Process
crl.globalsign.net	104.18.21.226	United States	13335	Cloudflare, Inc.	Malware Process
crl.microsoft.com	63.238.216.200	United States	209	Qwest Communications Com...	OS Process
ocsp.digicert.com	72.21.91.29	United States	15133	MCI Communications Service...	Malware Process
storage.googleapis.com	172.217.12.176	United States	15169	Google LLC	Malware Process
ctldl.windowsupdate.com	184.24.97.176	United States	20940	Akamai Technologies, Inc.	OS Process
api.raygun.io	54.243.218.230	United States	14618	Amazon Technologies Inc.	Malware Process

HTTP PACKETS

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
ctldl.windowsupdate.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	14.8448390961
Path: /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?5214f422c8e1da2d **URI:** http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?5214f422c8e1da2d						
ctldl.windowsupdate.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	20.185049057
Path: /msdownload/update/v3/static/trustedr/en/authrootstl.cab?1932ba0be8ccc86d **URI:** http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab?1932ba0be8ccc86d						
ocsp.digicert.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	25.6093070507
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTfqhLjKLEJQZPin0KCzkdAQpVYowQUsT7DaQP4v0cB1JgmGggC72NkK8MCEA3Q4zdKyVvb%2BmtDSypI7AY%3D **URI:** http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTfqhLjKLEJQZPin0KCzkdAQpVYowQUsT7DaQP4v0cB1JgmGggC72NkK8MCEA3Q4zdKyVvb%2BmtDSypI7AY%3D						
ocsp.digicert.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	30.8133530617
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBSHRqVSKsocqbcuJkRZwJjSAmttHAQUrWkGcPyAGxazqRiUa5QChl73J4wCEA8DpEdAc3HbUzijkx9jirc%3D **URI:** http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSHRqVSKsocqbcuJkRZwJjSAmttHAQUrWkGcPyAGxazqRiUa5QChl73J4wCEA8DpEdAc3HbUzijkx9jirc%3D						
crl.microsoft.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	69.8760750294
Path: /pki/crl/products/tspca.crl **URI:** http://crl.microsoft.com/pki/crl/products/tspca.crl						
crl.microsoft.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	75.591643095
Path: /pki/crl/products/CodeSignPCA2.crl **URI:** http://crl.microsoft.com/pki/crl/products/CodeSignPCA2.crl						
storage.googleapis.com	80	GET	1.1		1	77.4215579033
Path: /ss-installers/windows/avirasdk/3.0.0/avira32redist.zip **URI:** http://storage.googleapis.com/ss-installers/windows/avirasdk/3.0.0/avira32redist.zip						
crl.microsoft.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	81.6734809875
Path: /pki/crl/products/WinPCA.crl **URI:** http://crl.microsoft.com/pki/crl/products/WinPCA.crl						
crl.globalsign.net	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	88.5741620064
Path: /primobject.crl **URI:** http://crl.globalsign.net/primobject.crl						
storage.googleapis.com	80	HEAD	1.1		1	100.901161909
Path: /savapi/vdf.zip **URI:** http://storage.googleapis.com/savapi/vdf.zip						
storage.googleapis.com	80	GET	1.1		1	100.940212965
Path: /savapi/vdf.zip **URI:** http://storage.googleapis.com/savapi/vdf.zip						

DNS QUERIES

Request	Type
ctldl.windowsupdate.com	A
Answers - ctldl.windowsupdate.nsatc.net (CNAME) - 23.215.131.176 (A) - a1621.g.akamai.net (CNAME) - ctldl.windowsupdate.com.edgesuite.net (CNAME) - 23.215.131.169 (A)	
ocsp.digicert.com	A
Answers - cs9.wac.phicdn.net (CNAME) - 72.21.91.29 (A)	
crl.microsoft.com	A
Answers - crl.www.ms.akadns.net (CNAME) - 23.215.131.200 (A) - 23.215.131.195 (A) - a1363.dscg.akamai.net (CNAME)	
storage.googleapis.com	A
Answers - storage.l.googleusercontent.com (CNAME) - 172.217.12.176 (A)	
crl.globalsign.net	A
Answers - 104.18.21.226 (A) - global.prd.cdn.globalsign.com (CNAME) - cdn.globalsigncdn.com.cdn.cloudflare.net (CNAME) - 104.18.20.226 (A)	
api.raygun.io	A
Answers - raygun-api-763117148.us-east-1.elb.amazonaws.com (CNAME) - 174.129.18.184 (A) - 54.243.47.173 (A) - 23.23.157.142 (A) - 54.243.218.230 (A)	

TCP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
14.8448390961	Sandbox	23.215.131.176	80
20.185049057	Sandbox	23.215.131.176	80
25.6093070507	Sandbox	72.21.91.29	80
69.8760750294	Sandbox	23.215.131.200	80
77.4215579033	Sandbox	172.217.12.176	80
88.5741620064	Sandbox	104.18.20.226	80
101.382941008	Sandbox	192.168.56.9	49249
152.438287973	Sandbox	23.23.157.142	443

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.1119120121	Sandbox	192.168.56.255	137
3.20403194427	Sandbox	224.0.0.252	5355
3.20430803299	Sandbox	224.0.0.252	5355
3.62535691261	Sandbox	239.255.255.250	3702
5.76714992523	Sandbox	224.0.0.252	5355
9.15719604492	Sandbox	192.168.56.255	138
9.63107609749	Sandbox	224.0.0.252	5355
12.2271358967	Sandbox	224.0.0.252	5355
14.7877669334	Sandbox	8.8.4.4	53
15.0484728813	Sandbox	224.0.0.252	5355
17.6236178875	Sandbox	224.0.0.252	5355
20.4292578697	Sandbox	224.0.0.252	5355
22.9976608753	Sandbox	224.0.0.252	5355
25.5487699509	Sandbox	8.8.4.4	53
25.6967160702	Sandbox	224.0.0.252	5355
28.264029026	Sandbox	224.0.0.252	5355
64.0723938942	Sandbox	224.0.0.252	5355
67.1836988926	Sandbox	224.0.0.252	5355
69.8032031059	Sandbox	8.8.4.4	53
70.215446949	Sandbox	224.0.0.252	5355
73.0166919231	Sandbox	224.0.0.252	5355
74.3376069069	Sandbox	224.0.0.252	5355
75.9590499401	Sandbox	224.0.0.252	5355
77.3611409664	Sandbox	8.8.4.4	53
79.0475780964	Sandbox	224.0.0.252	5355
82.4072289467	Sandbox	224.0.0.252	5355
85.5330879688	Sandbox	224.0.0.252	5355
88.2544338703	Sandbox	8.8.4.4	53
152.275830984	Sandbox	8.8.4.4	53

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\SAVAPI\Aegen.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** ec545a77015ee17f2015eb5befea2a83 **SHA-1 :** 42a892bb31a2035a599b54cea8731ad923c818d5 **SHA-256 :** 44f3a24fa8423f65c61338772c8a9ffb655be8e84 **SHA-512 :** a8ca86748bbf30260a9b2abce6be20c36e1f6ee7 **Size :** 707.016 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\8890A77645B73478F5B1DED18ACBF795_B95A585585762F8B2D72E152F328449A	**Type :** data **MD5 :** 365d10d8837447dcb15c117fe3b8368a **SHA-1 :** 3815d4499231b0892ffade9d36bde552c2929775 **SHA-256 :** a0b6611ee75d3b26516a22a27d22c3c3ddb3fd5l **SHA-512 :** 5cd5f2fa469b9a0accf9b405d25090514b7fa2d22 **Size :** 0.43 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	**Type :** data **MD5 :** 255a5fb8b19ecee9847b77fe4975e21c **SHA-1 :** 75f6f00bf1b470b711dd0796c22d318323f099a3 **SHA-256 :** 778611b79e23a1eaf7b899a1a31687310bc10bf2 **SHA-512 :** f712e446c14a6e06bcbd911ca8fd4b2c0a7578fc7 **Size :** 0.328 Kilobytes.
C:\Users\User\AppData\Local\Temp\SAVAPI\On_access\Utils\On-Access-Drivers-Final.Cmd	**Type :** ASCII text, with CRLF line terminators **MD5 :** 99f88fb25d97a1712de7d107cdd9eb32 **SHA-1 :** e4d3ec77c037b3667837e9b3ebf1d56729fbd270 **SHA-256 :** 2b917642a0c8d4777b51c1b6b6c55e550b01af7a **SHA-512 :** b5e827baf7a9ff1da1ff372f82edd1275031bdae8 **Size :** 2.385 Kilobytes.
C:\Users\User\AppData\Local\Temp\SAVAPI\On_access\Win32\Vista\Avgntflt.Sys **C:\Users\User\AppData\Local\Temp\SAVAPI\On_access\Win32\Win7\Avgntflt.Sys**	**Type :** PE32 executable (native) Intel 80386, for MS Windows **MD5 :** a84684bebc36790cae1d5c771666e480 **SHA-1 :** f0b6aaee56b8f5c0370b4573f45ac30e3a9baacc **SHA-256 :** 831fdfae43f95f8c4485d1f7c8ad84653555c93622 **SHA-512 :** 486684d58559e9e94549c75b94af9e250037db74 **Size :** 130.912 Kilobytes.
C:\Users\User\AppData\Local\Temp\SAVAPI\Aedroid.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 8bd9ad92261aa190a6af51f7d29ab391 **SHA-1 :** 37fd397d4e33d6750a4ff080fe68d19611deb226 **SHA-256 :** e3ee2e5e91e89b931167e99818c779dc0c5dc488 **SHA-512 :** ece28d6a294fd84b08dda1cb0ab6ef0325fad917 **Size :** 2801.64 Kilobytes.
C:\Users\User\AppData\Local\Temp\SAVAPI\Savapiclient.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** ab90d31f5ff147483a0bc0cf2f95c2f1 **SHA-1 :** 48fff5c338f4d7194c68691eafeef77aa917a05b **SHA-256 :** 6862a4e1bc0233378710b4fa03ee53fd3d2a899b **SHA-512 :** 698857df9b472673556eb905ef89021e5cc56b1c **Size :** 126.032 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\SAVAPI\Apchash.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** cce3f50e5eb4797684e8d228c44d23bf **SHA-1 :** bdb9fe6e7ff36bcde1a2ceeab38b6cd5fae5f173 **SHA-256 :** 6fa32b8b36b807e4aec6a19e04f7e898116b5993 **SHA-512 :** 35c08115ab0f24ada9120c3d1d472bc9b156c708 **Size :** 133.264 Kilobytes.
C:\Users\User\AppData\Local\Temp\Logs\Main.Log	**Type :** ASCII text, with very long lines, with CRLF line terminators **MD5 :** 56ba356b1900f6fa2ae6deb9f36908a2 **SHA-1 :** 6962f605c020a3a68bfd156217be44edbe115323 **SHA-256 :** 13158628316edaaa01b21d20953c33f33b82813 **SHA-512 :** 3f6aece68cd8c2743796f4b9626a3ba6fe83874e1 **Size :** 16.885 Kilobytes.
C:\Users\User\AppData\Local\Temp\SAVAPI\Cacert.Crt	**Type :** PEM certificate **MD5 :** 51ccb61f5718d83b07a33c1b696fdcd1 **SHA-1 :** 94f361ddadf5acbe287daa7aa0377b01f6163a48 **SHA-256 :** 6d382f5bafe9d933ee1756438ea8e565978ee7d5 **SHA-512 :** 7a3476885252045b2743a4664e8043530b0ff4b5 **Size :** 6.065 Kilobytes.
C:\Users\User\AppData\Local\Temp\SAVAPI\On_access\Utils\Sd_inst.Exe	**Type :** PE32 executable (console) Intel 80386, for MS Windows **MD5 :** 3a42f27bd1d209ff45b38aa7d6fbd3b0 **SHA-1 :** d1c28b306efeb164481e10f866009acf4be649f7 **SHA-256 :** 621f2bda22c2fd358c56fc7b61a52687a5085d96 **SHA-512 :** 8de7ae65a08d2d923b44eec90aca47829493ed3 **Size :** 90.368 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157	**Type :** Microsoft Cabinet archive data, 6509 bytes, 1 file **MD5 :** 33b39e2a516ef730a8fa922894f0fbd5 **SHA-1 :** 03d455583dda59215d945af76af6293b202f586f **SHA-256 :** 9446e8f2056fea3ac1365a809ada04602606242c **SHA-512 :** 75763aa13b43eb96294b0f84e13106611198872 **Size :** 6.509 Kilobytes.
C:\Users\User\AppData\Local\Temp\SAVAPI\Aehelp.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 189679348cecebd814ccf11f0be048ff **SHA-1 :** 43851ca4401d3cb176575c30dc0f767893ba28fd **SHA-256 :** 3e993b11d1e6b9d471c1248b466eb02e106e5da **SHA-512 :** 4d6bb5e929383836a9fc158b2be8fa5bf5b08f71 **Size :** 299.728 Kilobytes.
C:\Users\User\AppData\Local\Temp\SAVAPI\Msvcr120.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 034ccadc1c073e4216e9466b720f9849 **SHA-1 :** f19e9d8317161edc7d3e963cc0fc46bd5e4a55a1 **SHA-256 :** 86e39b5995af0e042fcdaa85fe2aefd7c9ddc7ad6 **SHA-512 :** 5f11ef92d936669ee834a5cef5c7d0e7703bf05d0 **Size :** 970.912 Kilobytes.
C:\Users\User\AppData\Local\Temp\SAVAPI\Aecrypto.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** dff010b4b3da7bc89660debc1d5f7afa **SHA-1 :** 8181f22a85c96260ba516b8210bfb6e1d92f405c **SHA-256 :** 151cefe5119fd59636986befec370aed14bbac2ce **SHA-512 :** 4482473f06c8e2e667b95c5991950e8d5edb8ef2 **Size :** 141.8 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\Data\Sdet.Jdat	**Type :** ASCII text, with very long lines, with no line terminators **MD5 :** 666b67bbd0b282adac02b445973eeaa9 **SHA-1 :** 0da22085ac4f3871a726004e9607b8e92b0a9bd1 **SHA-256 :** 13292458b40416ff7da735aa5b48878c5ae34e28 **SHA-512 :** d57edaf1d5e420c75a11f9c247ae4892c691f01e2 **Size :** 0.4 Kilobytes.
C:\Users\User\AppData\Local\Temp\SAVAPI\Aeexp.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** f86f0e04965f2d4b24f9bfaf7d0caf29 **SHA-1 :** 67f4768e337183ac8cc758a0d3e52b3e212ab0bf **SHA-256 :** e4878da4a1e284b7b3146a0375cc5b7b63110a7 **SHA-512 :** b63c91febe64476c465c9cbea59ed400af6e0675 **Size :** 399.464 Kilobytes.
C:\Users\User\AppData\Local\Temp\SAVAPI\Aevdf.Datmjrzychs.V4o.PendingOverwrite	**Type :** ASCII text, with very long lines **MD5 :** 8689417dde8e65ef8acb51bb2e0d20a3 **SHA-1 :** ec9b5f17e3193825b72254b935802cafad23ca2a **SHA-256 :** 6865193443363fbf4005880222910015b639a7b5 **SHA-512 :** cec55fa8166b5ecf86c140b28c32f8904981e1bbe **Size :** 5.484 Kilobytes.
C:\Users\User\AppData\Local\Temp\SAVAPI\On_access\Utils\On-Access-Drivers-Post.Cmd	**Type :** ASCII text, with CRLF line terminators **MD5 :** 20df71f8a8628840063b627705eebdbe **SHA-1 :** ae13d32e8b6e0559d44b10a1a109b0fbbf6a2c80 **SHA-256 :** 293b013dccd92272457636a1b81388a90c064eb **SHA-512 :** eaab41b693e718ab758d0236c9bc0e61f752a1e1 **Size :** 3.835 Kilobytes.
C:\Users\User\AppData\Local\Temp\SAVAPI\Aepack.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** c5a13c082775631c1afe9b9c1d79dccd **SHA-1 :** 2523e0a0dd569a252da3ecf9fb08b6db353b8e88 **SHA-256 :** f7f37dbff085331ee6dd1ebf271b1af0d034f584d **SHA-512 :** bd5f694cd9cf0807ac91fd8b5baa6840669bfb578 **Size :** 835.856 Kilobytes.
C:\Users\User\AppData\Local\Temp\SAVAPI\Productname.Dat	**Type :** ASCII text, with no line terminators **MD5 :** 0e1802d2bd4a0046729c6c6e45fa9862 **SHA-1 :** eea616975fb17754300d25c025f3d2a962295382 **SHA-256 :** 55bea11ba99bbf0272c70ce7a8c1845ba934f0ab **SHA-512 :** ff58fc6837cb51ba4f0ce65fb96630c4abad093737 **Size :** 0.017 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\DE0101390D8E4B74E3DD39ACA5B00000_BCA65E535E79DBF987FC1C7A3D60D995	**Type :** data **MD5 :** c272f34aa84c2e0e4bfed7b90cd12d9c **SHA-1 :** 537d2d2c44ba26661c000b0de43c1eb1252f7fb8 **SHA-256 :** 183d2c8df84b24a0521ffbf7f9ec4d1cb50b0af48 **SHA-512 :** fbd5ba4979c0fc606676af9660f43ab93b65cd9d2 **Size :** 0.471 Kilobytes.
C:\Users\User\AppData\Local\Temp\SAVAPI\Vdfupd.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** f35c6f578d1cb2c4796aa7282c5ae47e **SHA-1 :** a228d0d28a66c5a3cbdeb515aa8ee691ee326503 **SHA-256 :** a323f83d87d8aee61ba11fc5de6d5b0ee7ef4338 **SHA-512 :** 9b0e5d919e18d9a64afe9196f1c04124e88a52ce **Size :** 102.48 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\TarDEDD.Tmp	**Type :** data **MD5 :** fe1c6ccc98d43c2bbed20e1780b66386 **SHA-1 :** b6ff695038e6ecd5d1011a40718359c74ca3a641 **SHA-256 :** 6f8d70366d59d5c50d62d0e9b1a01321647f48bf **SHA-512 :** 3dc51e96645fad49926e32bb71d2221a289dc8a **Size :** 129.865 Kilobytes.
C:\Users\User\AppData\Local\Temp\SAVAPI\Aescript.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** f54b9813a49a74265338f7dcdfcf1272 **SHA-1 :** 06ae685968b5085ec26af756aacaca5a2ed1a23d **SHA-256 :** 1d7ca8e699d6cb4bad22e39426d1d3064aff31ce **SHA-512 :** e810e307be71c3c318a1cd6e5d75d4488b4c914 **Size :** 989.624 Kilobytes.
C:\Users\User\AppData\Local\Temp\SAVAPI\Aelibinf.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 0fc5c8a5ff713a93b9131839c0ea3a65 **SHA-1 :** 6d4fcb47ba58fc5bc64a662e4e9f31f1f5576031 **SHA-256 :** 43b38d8e9d0233a280cf794eb1f82e67d1209532 **SHA-512 :** 9454c709330f8243af788344a43016b42d7bac76 **Size :** 79.464 Kilobytes.
C:\Users\User\AppData\Local\Temp\SAVAPI\Aebb.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** ca7497dfec41ae39c2aba49df489716c **SHA-1 :** 045b53ae730dedb2af65095d611237646ecd6719 **SHA-256 :** be84ca71660188e04c3a777e19019412e280af4b **SHA-512 :** 95501aa07a12cf407e7243fb54240f8f53b7d2465 **Size :** 71.144 Kilobytes.
C:\Users\User\AppData\Local\Temp\SAVAPI\Aeoffice.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 19e0f29836a72f6a89f02ba39afe1066 **SHA-1 :** 36da86f0ae7ee4214318ee2e61cc00c1a5b6b076 **SHA-256 :** 0783b56c5cf1ad6b5391966e93954cc076d3808b **SHA-512 :** 4ce7ca23a4bde2451a32a53d9953ba06264b58e **Size :** 677.928 Kilobytes.
C:\Users\User\AppData\Local\Temp\SAVAPI\Aescn.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 4c97c892c0c4d7543a8881717c48c189 **SHA-1 :** 7f3030e9325ae180ab7840a2a7882023bdc9a11c **SHA-256 :** b78803653e5761983562bae965d8ce7a8dd2885 **SHA-512 :** d619bc82f5146383e0e1912b2f3d3e26b5f5cd86 **Size :** 158.416 Kilobytes.
C:\Users\User\AppData\Local\Temp\SAVAPI\Aeheur.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 625f5c5e9e71bc7b27c716f9269ec206 **SHA-1 :** 219f970c48deec21e1c92168dca9fe30bf5a10ad **SHA-256 :** 10424489b9c24cfb5d110673ee66dba9fe66549b **SHA-512 :** a007ac9294b819b9c7db5702ce06b40912de368 **Size :** 11703.832 Kilobytes.
C:\Users\User\AppData\Local\Temp\SAVAPI\On_access\Win32\Vista\Avipbb.Inf	**Type :** ASCII text, with CRLF line terminators **MD5 :** baa52399f090754b28fd5ab390cce1ae **SHA-1 :** f8886063e4e052e6e16d0e2de68bfa3677364e3c **SHA-256 :** 5cb8233117695a563c9a484197da50631044903 **SHA-512 :** c5279bfcb109536ce2f5ebfc2e8405cdad7832a06 **Size :** 1.962 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\SAVAPI\Aelidb.Dat	**Type :** data **MD5 :** b613ccdc414d5b2fd69e7269b7173dd1 **SHA-1 :** 8b60c9aadac2a12c66d8ef97c803f150665276f7 **SHA-256 :** 1ac108d4da3cf23607dc4714f68f6d5ec35ee733(**SHA-512 :** 682e098b63f18d07f57f0460f60ddd1e85228634 **Size :** 88.15 Kilobytes.
C:\Users\User\AppData\Local\Temp\SAVAPI\On_access\Win32\Win7\Avipbb.Cat	**Type :** empty **MD5 :** d41d8cd98f00b204e9800998ecf8427e **SHA-1 :** da39a3ee5e6b4b0d3255bfef95601890afd80709 **SHA-256 :** e3b0c44298fc1c149afbf4c8996fb92427ae41e46 **SHA-512 :** cf83e1357eefb8bdf1542850d66d8007d620e405 **Size :** 0.0 Kilobytes.
C:\Users\User\AppData\Local\Temp\SAVAPI\Aeset.Dat	**Type :** ASCII text, with very long lines **MD5 :** 2c36f2266318f34d27966ad9e010a272 **SHA-1 :** 9afc4b697b88aa450d15470fac1f0169a545dfa5 **SHA-256 :** 2a85d4f7674b43b2017c412e49259a3281258a64 **SHA-512 :** 6a1c1322be75741a58f3b480a7474d329095fc34 **Size :** 3.042 Kilobytes.
C:\Users\User\AppData\Local\Temp\SAVAPI\Aemobile.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 022689df63f0e1d54011638b761c4def **SHA-1 :** b229036d47a383c72f65bb1896cd8312a0108ec9 **SHA-256 :** 6a9c3004cc6a106e0501be07d383df9c564712fa7 **SHA-512 :** 3178c2430ad497e353382ce9e01eef09ce7d7659 **Size :** 362.072 Kilobytes.
C:\Users\User\AppData\Local\Temp\SAVAPI\On_access\On-Access-Drivers-Install.Cmd	**Type :** ASCII text, with CRLF line terminators **MD5 :** 188fa7298e772f9dcf3912bdf1ffc2a2 **SHA-1 :** 29367a9ed2c0ddb62f25228204b12cdc72da0ea9 **SHA-256 :** a1fb989e87906a4e5f06ed61d2aaf2203c2a95c6(**SHA-512 :** 70fcda1ce21a7b8d68b5221f2b0e4cb2c8000eff3 **Size :** 5.831 Kilobytes.
C:\Users\User\AppData\Local\Temp\SAVAPI\Aerdl.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** f94e67a96db01268382f84017a1c956a **SHA-1 :** 1fcf434fa03e6568dde35052612b62d9078ee043 **SHA-256 :** 0979821d13aec02aa5e32fcc814a3bec11d114bf8 **SHA-512 :** b4796fb6646f997e03a2f97a8682990f7aca745b2 **Size :** 1263.912 Kilobytes.
C:\Users\User\AppData\Local\Temp\SAVAPI\Aesbx.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** dc4a1bd86008a08e55a8c161d06939a2 **SHA-1 :** 4626130048d0f754d86dc2bf189f9702fbd77d0f **SHA-256 :** 1c55867f96a12e759871a4ddab4d3c4b82c4caf0 **SHA-512 :** 1e25ff70b5eb7d2f19af8d5f6e5043ca084d7b51b **Size :** 1667.056 Kilobytes.
C:\Users\User\AppData\Local\Temp\SAVAPI\Apcfile.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386, for MS Windows **MD5 :** 2b82f7bae600676a10143dc6b3caddb1 **SHA-1 :** 046148a8852416f2f53ef79dfb5cfa78233c08e1 **SHA-256 :** da67392efbf41609e374fb36b54a74cce0a4198ff **SHA-512 :** fd205c79a9bab63dad695f36ba3fa4309d10d9bf **Size :** 1698.744 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Roaming\TotalAV\3.0.0\Avira32redist.Zip	**Type :** Zip archive data, at least v2.0 to extract **MD5 :** b993054aa6a9ac6ffd5547a8dd6791d0 **SHA-1 :** 982a923a4e3a126d957215c74dcc4e8264041c02 **SHA-256 :** 75994abdbeb14ec38257735e86596b540ca1e3b **SHA-512 :** 9775dae3e1764a64440f1b6d7ed13f0ae416bfa6 **Size :** 16538.155 Kilobytes.
C:\Users\User\AppData\Local\Temp\SAVAPI\On_access\On-Access-Drivers-Uninstall.Cmd	**Type :** ASCII text, with CRLF line terminators **MD5 :** 84d649fe05e145a29f6a326667c40a51 **SHA-1 :** 4154ba19cfa0180ee67916259bcb09a4040a932f **SHA-256 :** 06349b1cfb7db167018ad76bc0fd887cdfcf791ed **SHA-512 :** b45d3427752258078b16583dc4e14183e62d7f7 **Size :** 7.356 Kilobytes.
C:\Users\User\AppData\Local\Temp\SAVAPI\Avupdate_msg.Avr	**Type :** data **MD5 :** 206259be74a0d86d2f2e351ddaae873b **SHA-1 :** 62b94eb7f71df4e6c20b3bba3001616f54642c18 **SHA-256 :** a0ae2033908dac1d9fb2b3b42ecb5ddd89a76f03 **SHA-512 :** ddf6bbb6030a5071629e4974a4eff9658cecbf4d2 **Size :** 6.392 Kilobytes.
C:\Users\User\AppData\Local\Temp\SAVAPI\Avupdate.Exe	**Type :** PE32 executable (console) Intel 80386, for MS Windows **MD5 :** b4e681c7a94989c585e20e94a6d190e2 **SHA-1 :** 0135a34c15b292c1ddd76680de61d80903b1ecc0 **SHA-256 :** b5c5a11a2c79dd9ec21389c74c7c3fbb60c12db8 **SHA-512 :** 0ba3e17085690eed7cc2dc14b838befb7fab73a4 **Size :** 1967.224 Kilobytes.
C:\Users\User\AppData\Local\Temp\SAVAPI\Savapi.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 57ca420885edc30750e29f0f545e5c94 **SHA-1 :** bcc4002e5a48c9189360dd51a0d757138437df25 **SHA-256 :** 5e6d0116152707f0e648f5e0a780510b80af04ce **SHA-512 :** d3f42c181cdef20dc24e99048a1ac29ff3883bda0 **Size :** 1804.68 Kilobytes.
C:\Users\User\AppData\Local\Temp\SAVAPI\On_access\README	**Type :** ASCII text, with CRLF line terminators **MD5 :** 6a30abbfd119dc7b330a0d5aaff4c8f8 **SHA-1 :** d2d5d0be8fa67cfc4886def0009aafcfa67f82c7 **SHA-256 :** a7d68c07f77d97b06368d97ec4a52593931505a3 **SHA-512 :** 92ac1a849bd028a309680cb597dd93579c834b7 **Size :** 0.386 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157	**Type :** data **MD5 :** 894b6ded18e8718e3f5c75575ba7afcc **SHA-1 :** b344e9831b6d54d1e2aa45d6006fc2914ca00276 **SHA-256 :** 7ab4a46665ba87c09250bef8addee377b05c0aba **SHA-512 :** 03570b19e71c395281d3152ace85d197a91c883c **Size :** 0.342 Kilobytes.
C:\Users\User\AppData\Local\Temp\SAVAPI\Aeemu.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** c147954ad962c8845b3d545a01300e6e **SHA-1 :** 1d08ffa9d17b2b4131be1cc0c9534534ae248779 **SHA-256 :** b716dfbf6b92d4e38ac4a1a46a962e411ee89535 **SHA-512 :** 3224f39cbc14d6cad300ffca59b31669fce46d3f7f **Size :** 420.248 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\SAVAPI\Aecore.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 75d070b39149c915fab7e7eb5f492332 **SHA-1 :** c65499a625709c24ac890363a0d51820f433945a **SHA-256 :** 9acc2fe8a78545431c2f7f6e8438b7f4077c40dd5 **SHA-512 :** 1f88fd3212b9e89e19b992f291d068be7c09e9f9 **Size :** 266.48 Kilobytes.
C:\Users\User\AppData\Local\Temp\SAVAPI\On_access\Win32\Vista\Avipbb.Sys	**Type :** PE32 executable (native) Intel 80386, for MS Windows **MD5 :** cc2fa54e156c009163bf8e797e2f882f **SHA-1 :** 04c77b2d5a79490139c1321d74d9473fcdbb72d5 **SHA-256 :** 95aa6277ac95b077541a2287a662d539ec3da44 **SHA-512 :** cd5ba971701308c3d0d4fd21078e7c3d895a9b4 **Size :** 156.088 Kilobytes.
C:\Users\User\AppData\Local\Temp\CabDEDC.Tmp **C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506**	**Type :** Microsoft Cabinet archive data, 53830 bytes, 1 file **MD5 :** 1e7ee2d082541f087a725ac2803dc927 **SHA-1 :** d2a18b0a6599d280998a7fc94037becf64c597e9 **SHA-256 :** 0a43fb2fe8f01af0409ddb8dba9fd4529edb44d2 **SHA-512 :** efcde3ef128d14c4a44c7a3a4b7783f5ffa6956c71 **Size :** 53.83 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\DE0101390D8E4B74E3DD39ACA5B00000_BCA65E535E79DBF987FC1C7A3D60D995	**Type :** data **MD5 :** 199e8b405fa2b4152f112a13dbbd3f4a **SHA-1 :** d88a8c686b39221e4c82a3770d1a0a7d6a4d735e **SHA-256 :** 97750d9e319949548ab96069c8e8b5664373358 **SHA-512 :** c229469021bf0379a0bf015e923e20ed17fb593f1 **Size :** 0.426 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\8890A77645B73478F5B1DED18ACBF795_B95A585585762F8B2D72E152F328449A	**Type :** data **MD5 :** 7651ec7c50322901f193a0cecdb4399d **SHA-1 :** 9988dc69ad92f9725da360bcd16b64c5778d98e4 **SHA-256 :** 974ab187bdf159d7e350a297dea64137b9eb911 **SHA-512 :** 77946438d57d5fb209ca0badae1617e4adf9b98 **Size :** 0.471 Kilobytes.
C:\Users\User\AppData\Local\Temp\Installoptions.Jdat	**Type :** ASCII text, with no line terminators **MD5 :** 1674fb1f9aa6d15b4633146fa59e9d10 **SHA-1 :** ef400d05f7dfce5207d6b79efef32e60a160293d **SHA-256 :** d208065b8751532cd4581c56cb59bb1088dfe44 **SHA-512 :** 72a21cf7e7b50f82f7ecafd28ff800b90d80f8df50 **Size :** 0.28 Kilobytes.
C:\Users\User\AppData\Local\Temp\SAVAPI\On_access\Win32\Vista\Avgio.Dll **C:\Users\User\AppData\Local\Temp\SAVAPI\On_access\Win32\Win7\Avgio.Dll**	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 34422e1f23ed76278b1aa384c89f91b4 **SHA-1 :** 90bb3198aea8e07f925be0bcf629ac8ff575c58f **SHA-256 :** 3f35b2236d3e5b72867b7ca3c7de631496cf889c **SHA-512 :** 85c44d1a48348491446abd4f7b4960cc40778aa4 **Size :** 61.872 Kilobytes.
C:\Users\User\AppData\Local\Temp\SAVAPI\On_access\Win32\Vista\Avkmgr.Inf	**Type :** ASCII text, with CRLF line terminators **MD5 :** 8e3186c24c98b5dac17e16b47c1f9e5e **SHA-1 :** 88459b1607eb2265d02d607251f53ed63df7d092 **SHA-256 :** 9bf53be587bf77d602189f9a125e0f72fafc3792c **SHA-512 :** 84cfac0cebbd40d7b8887c2bdd7fb8f0352c9f8e7 **Size :** 1.888 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\SAVAPI\On_access\Win32\Win7\Avgntflt.Cat	**Type :** data **MD5 :** 3c409d00694b76be7b6252bab303fbf0 **SHA-1 :** ddc34a91fc94e2f59e6aeccc42f4db08466fbb98 **SHA-256 :** 23b8dd9f1a8de76dc8202ea385163c4ea1b7854 **SHA-512 :** cb058bed634a8c36ba1098696d3798a4f45e96c **Size :** 0.679 Kilobytes.
C:\Users\User\AppData\Local\Temp\SAVAPI\Aevdf.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 5d11a07597b4f21061a3e5528637e4a2 **SHA-1 :** dad1d9b61381d5539e856e8bd43803b15e6c7c5d **SHA-256 :** 7b9047bb4778ed8b5e696617e5e542e3d846b6 **SHA-512 :** 41b03a7f6d0bd5ddd5987063b6fad6e61cba1d6 **Size :** 154.264 Kilobytes.
C:\Users\User\AppData\Local\Temp\SAVAPI\Avupdate-Savapilib-Engine.Conf	**Type :** ASCII text, with CRLF line terminators **MD5 :** fb1148d236eeb45c0d4959ef6aa23f35 **SHA-1 :** a014016cc6d764dafad7a0e1b16ee5c6a248e153 **SHA-256 :** 6573f1b8300d6021c94ad95526c4794a22d8a1a5 **SHA-512 :** 6146a79fc42d8293320c37a19082e25c429853e9 **Size :** 0.439 Kilobytes.
C:\Users\User\AppData\Local\Temp\SAVAPI\On_access\Win32\Vista\Avgntflt.Inf **C:\Users\User\AppData\Local\Temp\SAVAPI\On_access\Win32\Win7\Avgntflt.Inf**	**Type :** ASCII text, with CRLF line terminators **MD5 :** 426afad8ddd9684b69343b6ace8ccf42 **SHA-1 :** 9d27a659baa6d568095f718338b0cebc0884222c **SHA-256 :** fb73541bcd549ce91979add972a9d449b6237b6 **SHA-512 :** e5a2a33afea572f628ff5fcbe755c146b7c1ed30cc **Size :** 2.463 Kilobytes.
C:\Users\User\AppData\Local\Temp\Data\Prefs.Jdat	**Type :** ASCII text, with very long lines, with no line terminators **MD5 :** b501edf9453a8bbc1f5a11d52d181c57 **SHA-1 :** ec3b101ee8508283d39cd554fe51307f675a57d6 **SHA-256 :** ba9ef5be6aa4f02a532cd670897dffbfc261a9d53 **SHA-512 :** 6e03c22e85ab756d7852918a4cfb92bd3ae3d11 **Size :** 1.135 Kilobytes.
C:\Users\User\AppData\Local\Temp\SAVAPI\Msvcp120.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** fd5cabbe52272bd76007b68186ebaf00 **SHA-1 :** efd1e306c1092c17f6944cc6bf9a1bfad4d14613 **SHA-256 :** 87c42ca155473e4e71857d03497c8cbc28fa8ff7f **SHA-512 :** 1563c8257d85274267089cd4aeac0884a2a300ff **Size :** 455.328 Kilobytes.
C:\Users\User\AppData\Local\Temp\SAVAPI\Aemvdb.Dat	**Type :** data **MD5 :** b61b1e20d17b6062f8edc1428bf2223f **SHA-1 :** 6ccbdd36ce0cfeef36ab85a899b88b7f0a34e940 **SHA-256 :** 30389b79614655252fb847a07f7fadc872378390 **SHA-512 :** 5634655f5e4f429b535748d3a081d5f4ca35fcaca **Size :** 1.793 Kilobytes.
C:\Users\User\AppData\Local\Temp\SAVAPI\On_access\Win32\Vista\Avkmgr.Sys	**Type :** PE32 executable (native) Intel 80386, for MS Windows **MD5 :** 185cb049fa670298e2948ca3141d7ac1 **SHA-1 :** ebc875c3064c5c8b49f14f63727cd593412f3e27 **SHA-256 :** dccd32487e6b227c21ce55df2136adc657f138ae **SHA-512 :** 70c8d03f4dac37b17eee887f722798f01fc82838a **Size :** 35.84 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\SAVAPI\On_access\Utils\On-Access-Drivers-Pre.Cmd	**Type :** ASCII text, with CRLF line terminators **MD5 :** aed5c61ed2b8180ef67b33309e5058f3 **SHA-1 :** bed94b2e42fe7989351bd1ac205be01a70b906e1 **SHA-256 :** cb26d0fd7d24078f42be753ffa4acc19bdc385a69 **SHA-512 :** 0bb2cbad22c63a21251ce731545ddee235c68ae **Size :** 4.641 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	67eb0a16282599d3ead2977d264598fa31dd83f0
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
SHA1:	67eb0a16282599d3ead2977d264598fa31dd83f0
MD5:	ecebc09fec5652d173f5287faafb9c57
First Seen Date:	2018-06-22 06:16:03.690516 (about a year ago)
Number Of Clients Seen:	3
Last Analysis Date:	2018-06-22 06:16:03.690516 (about a year ago)
Human Expert Analysis Date:	2019-01-23 03:23:53.889743 (5 months ago)
Human Expert Analysis Result:	Malware

VALKYRIE COMODO

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	3
File Type Enum	6
Debug Artifacts	[]
Number Of Sections	3
Trid	[[64.6, u'Win64 Executable (generic)'], [15.4, u'Win32 Dynamic Link Library (generic)'], [10.5, u'Win32 Executable (generic)'], [4.6, u'Generic Win/DOS Executable'], [4.6, u'DOS Executable Generic']]
Compilation Time Stamp	0x5B213D32 [Wed Jun 13 15:50:10 2018 UTC]
LegalCopyright	Copyright \xa9 2017
Assembly Version	4.8.12.0
InternalName	TotalAV.exe
FileVersion	4.8.12.0
CompanyName	TotalAV
LegalTrademarks	
Comments	
ProductName	TotalAV Ultimate Antivirus
ProductVersion	4.8.12.0
FileDescription	TotalAV Ultimate Antivirus User Interface
OriginalFilename	TotalAV.exe
Translation	0x0000 0x04b0
Entry Point	0xa3410e (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	9440936
Ssdeep	196608:qf8p2DUd6HYvcu65om09o6Q2F6aTegF/L:qCuUd66k5op
Sha256	4bd67897d472c928a374aefdc87af07dfab51a9bb2cffcc47be1283e29344c9c
Exifinfo	[{u'EXE:FileSubtype': 0, u'File:FilePermissions': u'rw-r--r--', u'SourceFile': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/6/7/e/b/67eb0a16282599d3ead2977d264598fa31dd83f0', u'EXE:OriginalFileName': u'TotalAV.exe', u'EXE:ProductName': u'TotalAV Ultimate Antivirus', u'EXE:InternalName': u'TotalAV.exe', u'File:MIMEType': u'application/octet-stream', u'File:FileAccessDate': u'2018:06:22 06:13:10+00:00', u'EXE:InitializedDataSize': 2790400, u'File:FileModifyDate': u'2018:06:22 06:13:09+00:00', u'EXE:AssemblyVersion': u'4.8.12.0', u'EXE:FileVersionNumber': u'4.8.12.0', u'EXE:FileVersion': u'4.8.12.0', u'File:FileSize': u'9.0 MB', u'EXE:CharacterSet': u'Unicode', u'EXE:MachineType': u'Intel 386 or later, and compatibles', u'EXE:FileOS': u'Windows NT 32-bit', u'EXE:LegalTrademarks': u'', u'EXE:ProductVersion': u'4.8.12.0', u'EXE:ObjectFileType': u'Executable application', u'File:FileType': u'Win32 EXE', u'EXE:CompanyName': u'TotalAV', u'File:FileName': u'67eb0a16282599d3ead2977d264598fa31dd83f0', u'EXE:ImageVersion': 0.0, u'File:FileTypeExtension': u'exe', u'EXE:OSVersion': 4.0, u'EXE:PEType': u'PE32', u'EXE:TimeStamp': u'2018:06:13 15:50:10+00:00', u'EXE:FileFlagsMask': u'0x003f', u'EXE:LegalCopyright': u'Copyright \xa9 2017', u'EXE:LinkerVersion': 8.0, u'EXE:FileFlags': u'(none)', u'EXE:Subsystem': u'Windows GUI', u'File:Directory': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/6/7/e/b', u'EXE:FileDescription': u'TotalAV Ultimate Antivirus User Interface', u'EXE:EntryPoint': u'0x63410e', u'EXE:SubsystemVersion': 4.0, u'EXE:CodeSize': 6496768, u'EXE:Comments': u'', u'File:FileInodeChangeDate': u'2018:06:22 06:13:09+00:00', u'EXE:UninitializedDataSize': 0, u'EXE:LanguageCode': u'Neutral', u'ExifTool:ExifToolVersion': 10.1, u'EXE:ProductVersionNumber': u'4.8.12.0'}]
Mime Type	application/x-dosexec
Imphash	f34d5f2d4577ed6d9ceec516c1f5a744

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x2000	0x632114	0x632200	6.34606548956	65795fd3d987a402c05cfb18963f9512
.rsrc	0x636000	0x2a91ac	0x2a9200	6.08055099799	4af01ee069508e2d2ff8d93c84c445af
.reloc	0x8e0000	0xc	0x200	0.101910425663	a2751cc536fc27dc66458308dab2e5ea

PE Imports

- mscoree.dll
  - _CorExeMain

PE Resources

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 6513644, u'sha256': u'33b7491354f12bac92f2bea5b5c8b9264ec36835ff49eefeb36b5566cb714791', u'type': u'dBase III DBT, version number 0, next free block index 40', u'size': 1640}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 6515284, u'sha256': u'0c15334841ec1bde9305a70dce30db5de5e2d385109b4bb723f23d5f4748cb7a', u'type': u'data', u'size': 744}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 6516028, u'sha256': u'9d243bd50af2bbd043d2b388f11dfdf3ef2dfd30ab11726fa15cfed00e70e68b', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 296}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 6516324, u'sha256': u'3a2dabb489238bae99449c23340da615663474e09bf641fdcee4acb647b60947', u'type': u'dBase III DBT, version number 0, next free block index 40', u'size': 74792}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 6591116, u'sha256': u'44476bc0d01de527f6bb93d01594a5585e3cbf90245955f3bd5632b1c72c9ee3', u'type': u'dBase III DBT, version number 0, next free block index 40', u'size': 3752}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 6594868, u'sha256': u'6869ed72781fe16431ad4b268ba82a951d6acaec46da5dd50e983f21b088a045', u'type': u'dBase III DBT, version number 0, next free block index 40', u'size': 2216}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 6597084, u'sha256': u'6ac6557d25978a5b206095094381e4d87b9ccc62a79b4e63bf94d476f00ecfc2', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1384}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 6598468, u'sha256': u'9a5d2dcc85ffdf224752a44a12d3e4423317214038741612537028aa91ee1fba', u'type': u'data', u'size': 9640}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 6608108, u'sha256': u'89c09838cb633ed5101788d3b81576be15c488ac14502e98a0ecd09a141fe39a', u'type': u'data', u'size': 4264}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 6612372, u'sha256': u'b5eb69e11fb3455b6884645ac0c668017637d58ae3efa4a2cca271d425b0f02b', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1128}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_RCDATA', u'offset': 6613500, u'sha256': u'133986a26f9bb96836c9b1c578909e724f704450142aa1673af1cd611edda536', u'type': u'ASCII text, with no line terminators', u'size': 43}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_RCDATA', u'offset': 6613544, u'sha256': u'b59043a36e406564e1187609711c3f7137bb2fc63768e305f0e73e3654d78db5', u'type': u'ASCII text, with CRLF line terminators', u'size': 857}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_RCDATA', u'offset': 6614404, u'sha256': u'47e4703552931bb814d4ef2c57a42360b7059ba8da15b2afd96f17d8fe8acf1e', u'type': u'ASCII text, with very long lines, with no line terminators', u'size': 2683559}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_ICON', u'offset': 9297964, u'sha256': u'ff04be4a7bb195c3c8e75dd51720c0b6f660732b70dadbb0219ca43b85974779', u'type': u'MS Windows icon resource - 10 icons, 48x48, 16 colors', u'size': 146}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_VERSION', u'offset': 9298112, u'sha256': u'3f469bf9891a0895283c000e140a1ba9a741e80feeeb3763d8de7f580e8ec274', u'type': u'data', u'size': 932}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_MANIFEST', u'offset': 9299044, u'sha256': u'1e106f6a6ee8c49ce90fcf6721818d4ceeef3796ef3037576c1cba32a711f6b6', u'type': u'XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators', u'size': 3398}

CERTIFICATE VALIDATION

- Success ✔

[+] Protected Antivirus Limited	
Status	NoError ✔
Start Date	2018-02-02 02:00:00
End Date	2019-12-31 02:00:00
Sha256	7b89ffe1ea5674ac8587de4e1a4050c216fe46cfc8567699e10abfac7efff625
Serial	0F03A447407371DB5338A3931F638AB7
Subject Key Identifier	62 9c 16 b2 92 94 1b 4b f4 d8 05 88 a4 13 82 7a f5 dd 6e 45
Issuer Name	DigiCert EV Code Signing CA
Issuer Key Identifier	ad 69 06 70 fc 80 1b 16 b3 a9 18 94 6b 94 02 86 5e f7 27 8c
Crl link	http://crl3.digicert.com/EVCodeSigning-g1.crl,http://crl4.digicert.com/EVCodeSigning-g1.crl
Key Usage	Digital Signature (80)
Extended Usage	Code Signing (1.3.6.1.5.5.7.3.3)

[+] DigiCert EV Code Signing CA	
Status	NoError ✔
Start Date	2012-04-18 03:00:00
End Date	2027-04-18 03:00:00
Sha256	90fd3ff1106fb03910c1772abc31faf3cbebb3270e61282baf37c7327e918d50
Serial	0DD0E3374AC95BDBFA6B434B2A48EC06
Subject Key Identifie...	ad 69 06 70 fc 80 1b 16 b3 a9 18 94 6b 94 02 86 5e f7 27 8c
Issuer Name	DigiCert High Assurance EV Root CA
Issuer Key Identifier	b1 3e c3 69 03 f8 bf 47 01 d4 98 26 1a 08 02 ef 63 64 2b c3
Crl link	http://crl3.digicert.com/DigiCertHighAssuranceEVRootCA.crl,http://crl4.digicert.com/DigiCertHighAssuranceEVRootCA.
Key Usage	Digital Signature,Certificate Signing,Off-line CRL Signing,CRL Signing (86)
Extended Usage	Code Signing (1.3.6.1.5.5.7.3.3)

[+] DigiCert High Assurance EV Root CA	
Status	NoError ✔
Start Date	2006-11-10 02:00:00
End Date	2031-11-10 02:00:00
Sha256	ed960860d0e06c89fa3ff7723437b6812c6d7e1ad370c7885b1251d2e1c2a938
Serial	02AC5C266A0B409B8F0B79F2AE462577
Subject Key Identifier	b1 3e c3 69 03 f8 bf 47 01 d4 98 26 1a 08 02 ef 63 64 2b c3
Issuer Name	DigiCert High Assurance EV Root CA
Issuer Key Identifier	b1 3e c3 69 03 f8 bf 47 01 d4 98 26 1a 08 02 ef 63 64 2b c3
Crl link	undefined
Key Usage	Digital Signature,Certificate Signing,Off-line CRL Signing,CRL Signing (86)
Extended Usage	undefined

[+] DigiCert High Assurance EV Root CA	
Status	RevocationStatusUnknown ✖
Start Date	2011-04-15 10:45:33
End Date	2021-04-15 10:55:33
Sha256	a0507ad7c69b099b1471457945155838bb2a3cd40e7a4e32b38b9e4582e8bd30
Serial	61204DB4000000000027
Subject Key Identifier	b1 3e c3 69 03 f8 bf 47 01 d4 98 26 1a 08 02 ef 63 64 2b c3
Issuer Name	Microsoft Code Verification Root
Issuer Key Identifier	62 fb 0a 21 5b 7f 43 6e 11 da 09 54 50 6b f5 d2 96 71 f1 9e
Crl link	http://crl.microsoft.com/pki/crl/products/MicrosoftCodeVerifRoot.crl
Key Usage	Digital Signature,Certificate Signing,Off-line CRL Signing,CRL Signing (86)
Extended Usage	undefined

SCREENSHOTS