a864282fea5a536510ae86c77ce46f7827687783628e4f2ceb5bf2c41b8cd3c6

Sign in | Sign up

61 / 72

Community Score -248

61/72 security vendors flagged this file as malicious

Reanalyze | Similar | More

a864282fea5a536510ae86c77ce46f7827687783628e4f2ceb…
a864282fea5a536510ae86c77ce46f7827687783628e4f2ceb…

Size 1.20 MB

Last Analysis Date 4 days ago

EXE

peexe | detect-debug-environment | overlay | 64bits | idle | checks-cpu-name

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY 25+

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Display grouped sandbox reports

C2AE	0	0	0	0	0	0
CAPA	0	5	0	0	0	0
CAPE San…	0	2	0	0	47	0
Microsoft …	0	0	0	0	99+	32
VMRay	1	3	0	0	51	0
VirusTotal…	0	0	0	0	1	0
VirusTotal…	0	0	0	0	0	0
Yomi Hun…	1	1	0	2	1	5
Zenbox	0	5	0	0	99+	0

Activity Summary — Download Artifacts | Full Reports | Help

2 Detections
1 RANSOM | 1 MALWARE

Mitre Signatures
1 HIGH | 6 LOW | 30 INFO

IDS Rules
NOT FOUND

Sigma Rules
1 MEDIUM | 1 LOW

Dropped Files
229 OTHER | 1 PDF | 1 CAB | 1 DOS_COM | 1 TEXT

Network comms
4 HTTP | 2 DNS | 31 IP

Behavior Tags

checks-cpu-name | detect-debug-environment | idle

Dynamic Analysis Sandbox Detections

- The sandbox VMRay flags this file as: RANSOM
- The sandbox Yomi Hunter flags this file as: MALWARE

MITRE ATT&CK Tactics and Techniques

+ Execution TA0002
+ Persistence TA0003
+ Defense Evasion TA0005

+ Command and Control TA0011
+ Impact TA0040

Malware Behavior Catalog Tree

+ Anti-Static Analysis OB0002
+ Defense Evasion OB0006
+ Discovery OB0007
+ Persistence OB0012
+ File System OC0001
+ Memory OC0002
+ Process OC0003
+ Data OC0004
+ Cryptography OC0005
+ Operating System OC0008

Capabilities

Open in CAPA explorer

+ Anti-Analysis
+ Data-Manipulation
+ Host-Interaction
+ Load-Code
+ Persistence
+ Executable

Crowdsourced Sigma Rules

CRITICAL 0 HIGH 0 MEDIUM 1 LOW 1

⚠ Matches rule Change PowerShell Policies to an Insecure Level - PowerShell by frack113 at Sigma Integrated Rule Set (GitHub)
↳ *Detects use of Set-ExecutionPolicy to set insecure policies*

⚠ Matches rule Suspicious Get-WmiObject by frack113 at Sigma Integrated Rule Set (GitHub)
↳ *The infrastructure for management data and operations that enables local and remote management of Windows personal computers and servers*

Network Communication

HTTP Requests

+ GET http://crt.sectigo.com/SectigoPublicCodeSigningCAR36.crt 200
+ GET http://crt.sectigo.com/SectigoPublicCodeSigningRootR46.p7c 200
+ GET http://www.microsoft.com/pki/certs/MicCodSigPCA_08-31-2010.crt 200
+ GET http://www.microsoft.com/pki/certs/MicrosoftTimeStampPCA.crt 200

DNS Resolutions

+ www.microsoft.com
+ crt.sectigo.com

IP Traffic

TCP 20.99.184.37:443
TCP 20.99.133.109:443

TCP 20.69.140.28:443
TCP 104.86.182.43:443
UDP a83f:8110:0:0:2000:0:0:0:53

Behavior Similarity Hashes

C2AE	7eb58e30b74038daa9b31b5d9df78cf2
CAPA	41f82c351584bdd117b936b48489a757
CAPE Sandbox	5e6afe797f1d4fafb0031fffd577e349
Microsoft Sysinternals	2b4fd448ff1c2cdadcc75d5c73c6ffa4
VirusTotal Jujubox	d60fa210338046819c735c5a1f84bd90
VirusTotal Observer	e3dd6fa01f4e1fc3c861b8b4d9896dfc
VMRay	21fd45f2ac9f5b30cbde57a791f35159
Yomi Hunter	63cf7de0621220a676cf34f532329eb7
Zenbox	01b4c6db9877411c4652986295330728

File system actions

A:\
B:\
C:\
C:\$Recycle.Bin
C:*
C:\Config.Msi
C:\Config.Msi*
C:\Config.Msi\13d55b.rbf
C:\Config.Msi\13d55b.rbf.rhysida
C:\Config.Msi\13d55c.rbf

Files Written

C:/ps.xml.rhysida
c:/msocache/all users/{90160000-002c-0409-0000-0000000ff1ce}-c/proof.en/proof.xml.rhysida
c:/msocache/all users/{90160000-002c-0409-0000-0000000ff1ce}-c/proofing.xml.rhysida
c:/msocache/all users/{90160000-0044-0409-0000-0000000ff1ce}-c/setup.xml.rhysida
c:/msocache/all users/{90160000-0090-0409-0000-0000000ff1ce}-c/setup.xml.rhysida
c:/users/all users/microsoft help/ms.winword.16.1033.hxn.rhysida
c:/users/all users/microsoft/network/downloader/qmgr0.dat.rhysida
c:/users/all users/microsoft/office/clicktorunpackagelocker
c:/users/all users/microsoft/windows defender/scans/history/mput/mputhistory/09/287.rhysida
c:/users/all users/microsoft/windows defender/scans/history/mput/mputhistory/10/267.rhysida

Files Deleted

C:\ps.xml
%USERPROFILE%\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\powershell.exe.log
%USERPROFILE%\AppData\Local\Microsoft\Windows\INetCache\IE\KLT1I0ZU\update50[1].xml
%USERPROFILE%\AppData\Local\Temp__PSScriptPolicyTest_11kjispw.bg4.psm1
%USERPROFILE%\AppData\Local\Temp__PSScriptPolicyTest_1qupz0cm.4vw.psm1
%USERPROFILE%\AppData\Local\Temp__PSScriptPolicyTest_3ha1mk0v.ud3.ps1
%USERPROFILE%\AppData\Local\Temp__PSScriptPolicyTest_3wp4i1x3.esa.ps1
%USERPROFILE%\AppData\Local\Temp__PSScriptPolicyTest_4qgmf5vd.zcd.ps1
%USERPROFILE%\AppData\Local\Temp__PSScriptPolicyTest_535uyj3g.lf0.ps1
%USERPROFILE%\AppData\Local\Temp__PSScriptPolicyTest_53w2vlvj.z0r.psm1

Files Dropped

13d55b.rbf.rhysida
13d55c.rbf.rhysida
13d55d.rbf.rhysida
13d55e.rbf.rhysida
13d55f.rbf.rhysida
13d563.rbf.rhysida
13d564.rbf.rhysida
13d567.rbf.rhysida
13d568.rbf.rhysida
13d569.rbf.rhysida

Registry actions

HKLM\Software\Microsoft\Windows\Windows Error Reporting\WMR
HKEY_CURRENT_USER\Control Panel\Desktop
HKEY_CURRENT_USER\Control Panel\Desktop\Wallpaper
HKEY_CURRENT_USER\Control Panel\Desktop\WallpaperStyle
HKEY_CURRENT_USER\Conttol Panel\Desktop
HKEY_CURRENT_USER\Software\Microsoft\Command Processor
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\AutoRun
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\CompletionChar
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DefaultColor

Registry Keys Set

HKEY_CURRENT_USER\Control Panel\Desktop\Wallpaper
HKEY_CURRENT_USER\Control Panel\Desktop\WallpaperStyle
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop\NoChangingWallPaper
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop\NoChangingWallPaper
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\Wallpaper
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\WallpaperStyle

Process and service actions

Processes Created

%SAMPLEPATH%\a864282fea5a536510ae86c77ce46f7827687783628e4f2ceb5bf2c41b8cd3c6.exe
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
C:\Windows\System32\cmd.exe
C:\Windows\System32\reg.exe
C:\Windows\System32\rundll32.exe
C:\Windows\System32\wuapihost.exe
C:\Windows\system32\cmd.exe /c cmd.exe /c reg add "HKCU\Control Panel\Desktop" /v Wallpaper /t REG_SZ /d "C:\Users\Public\bg.jpg" /f
C:\Windows\system32\cmd.exe /c cmd.exe /c reg add "HKCU\Control Panel\Desktop" /v WallpaperStyle /t REG_SZ /d 2 /f
C:\Windows\system32\cmd.exe /c cmd.exe /c reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop" /v NoChangingWallPaper /t REG_SZ /d 1 /f
C:\Windows\system32\cmd.exe /c cmd.exe /c reg add "HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop" /v NoChangingWallPaper /t REG_SZ /d 1 /f

Shell Commands

"%SAMPLEPATH%\a864282fea5a536510ae86c77ce46f7827687783628e4f2ceb5bf2c41b8cd3c6.exe"
C:\Windows\System32\wuapihost.exe -Embedding
C:\Windows\system32\cmd.exe /c cmd.exe /c reg add "HKCU\Control Panel\Desktop" /v Wallpaper /t REG_SZ /d "%USERPROFILE%\bg.jpg" /f
C:\Windows\system32\cmd.exe /c cmd.exe /c reg add "HKCU\Control Panel\Desktop" /v WallpaperStyle /t REG_SZ /d 2 /f
C:\Windows\system32\cmd.exe /c cmd.exe /c reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop" /v NoChangingWallPaper /t REG_SZ /d 1 /f
C:\Windows\system32\cmd.exe /c cmd.exe /c reg add "HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop" /v NoChangingWallPaper /t REG_SZ /d 1 /f
C:\Windows\system32\cmd.exe /c cmd.exe /c reg add "HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v Wallpaper /t REG_SZ /d "%USERPROFILE%\bg.jpg" /f
C:\Windows\system32\cmd.exe /c cmd.exe /c reg add "HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v WallpaperStyle /t REG_SZ /d 2 /f
C:\Windows\system32\cmd.exe /c cmd.exe /c reg delete "HKCU\Conttol Panel\Desktop" /v Wallpaper /f
C:\Windows\system32\cmd.exe /c cmd.exe /c reg delete "HKCU\Conttol Panel\Desktop" /v WallpaperStyle /f

"%ProgramFiles(x86)%\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe" --type=renderer --shell-broker-channel=broker_pdfshell_sha74876e6-9512-4e82-a4e3-45426292ebab /b /id 1116_1997204729 /if pdfshell_shc4b4712c-7909-4ce6-ac86-5b788d9d794d

"%ProgramFiles(x86)%\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe" /b /id 1116_1997204729 /if pdfshell_shc4b4712c-7909-4ce6-ac86-5b788d9d794d --shell-broker-channel=broker_pdfshell_sha74876e6-9512-4e82-a4e3-45426292ebab

%windir%\System32\svchost.exe -k WerSvcGroup

%windir%\system32\DllHost.exe /Processid:{AB8902B4-09CA-4BB6-B78D-A8F59079A8D5}

%SAMPLEPATH%\a864282fea5a536510ae86c77ce46f7827687783628e4f2ceb5bf2c41b8cd3c6.exe

<unknown process>

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

C:\Windows\System32\cmd.exe

C:\Windows\System32\conhost.exe

Processes Tree

2268 - %windir%\System32\svchost.exe -k WerSvcGroup

2708 - %CONHOST% "173386383914252272-46167420-1876866685112441837465065931118211867722212829 13"

2640 - %SAMPLEPATH%

2756 - %windir%\system32\DllHost.exe /Processid:{AB8902B4-09CA-4BB6-B78D-A8F59079A8D5}

2012 - wmiadap.exe /F /T /R

1072 - %windir%\system32\wbem\wmiprvse.exe

2788 - "%ProgramFiles(x86)%\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe" /b /id 1116_1997204729 /if pdfshell_shc4b4712c-7909-4ce6-ac86-5b788d9d794d --shell-broker-channel=broker_pdfshell_sha74876e6-9512-4e82-a4e3-45426292ebab

↳ 2828 - "%ProgramFiles(x86)%\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe" --type=renderer --shell-broker-channel=broker_pdfshell_sha74876e6-9512-4e82-a4e3-45426292ebab /b /id 1116_1997204729 /if pdfshell_shc4b4712c-7909-4ce6-ac86-5b788d9d794d

2932 - "%ProgramFiles(x86)%\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe" C:\tmp\CriticalBreachDetected.pdf

↳ 2356 - "%ProgramFiles(x86)%\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --backgroundcolor=16514043

Synchronization mechanisms & Signals

Mutexes Opened

Global\PowerShell_CommandAnalysis_Lock_S-1-5-21-1560258661-3990802383-1811730007-1000

Modules loaded

Runtime Modules

KERNEL32.DLL

%SAMPLEPATH%\a864282fea5a536510ae86c77ce46f7827687783628e4f2ceb5bf2c41b8cd3c6.exe

C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\999d72a4e033bba86d05407570c67cba\System.Management.Automat

ADVAPI32.dll

API-MS-Win-Security-LSALookup-L1-1-0.dll

C:\Windows\Microsoft.NET\Framework64\v4.0.30319\OLEAUT32.dll

C:\Windows\Microsoft.NET\Framework64\v4.0.30319\clr.dll

C:\Windows\Microsoft.NET\Framework64\v4.0.30319\clrjit.dll

C:\Windows\Microsoft.NET\Framework64\v4.0.30319\en-US\mscorrc.dll

C:\Windows\Microsoft.NET\Framework64\v4.0.30319\en\mscorrc.dll

Highlighted actions

Calls Highlighted

MoveFileA

GetSystemMetrics

Sleep

Highlighted Text

"C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe"

"a864282fea5a536510ae86c77ce46f7827687783628e4f2ceb5bf2c41b8cd3c6.bin.exe"