62 / 71

Community Score -39

62/71 security vendors flagged this file as malicious

Reanalyze Similar More

5e75ef02517afd6e8ba6462b19217dc4a5a574abb33d10eb…

file.exe

Size 92.50 KB

Last Analysis Date 9 months ago

EXE

peexe persistence checks-user-input detect-debug-environment long-sleeps checks-cpu-name

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 11

Display grouped sandbox reports

CAPA	0	2	0	0	0	0
CAPE San…	0	7	0	0	0	0
Microsoft …	0	0	0	2	99+	3
VirusTotal…	0	0	0	3	21	0
VirusTotal…	0	0	0	0	0	0
Zenbox	4	6	0	6	82	0

Activity Summary

Download Artifacts Full Reports Help

4 Detections
1 MALWARE 1 RANSOM 1 ADWARE 1 EVADER

Mitre Signatures
7 LOW 24 INFO

IDS Rules
NOT FOUND

Sigma Rules
3 HIGH 4 MEDIUM

Dropped Files
202 OTHER 1 DOS_COM 1 PE_EXE

Network comms
3 IP

Behavior Tags
checks-cpu-name checks-user-input detect-debug-environment long-sleeps persistence

Dynamic Analysis Sandbox Detections
The sandbox Zenbox flags this file as: MALWARE RANSOM ADWARE EVADER

MITRE ATT&CK Tactics and Techniques
- Execution TA0002
- Persistence TA0003
- Privilege Escalation TA0004
- Defense Evasion TA0005
- Credential Access TA0006
- Discovery TA0007
- Collection TA0009
- Command and Control TA0011

Malware Behavior Catalog Tree

- Anti-Behavioral Analysis OB0001
- Anti-Static Analysis OB0002
- Defense Evasion OB0006
- Data OC0004
- Cryptography OC0005

Capabilities

Open in CAPA explorer

- Data-Manipulation
- Linking
- Executable

Crowdsourced Sigma Rules

CRITICAL 0 HIGH 3 MEDIUM 4 LOW 0

Matches rule North Korean RAT - BLINDINGCAN (Sysmon detection) by Ariel Millahuel at SOC Prime Threat Detection Marketplace
↳ *This rule detects a Remote Access Trojan that according to CISA, belongs to Hidden Cobra*

Matches rule Suspicious Volume Shadow Copy VSS_PS.dll Load by Markus Neis, @markus_neis at Sigma Integrated Rule Set (GitHub)
↳ *Detects the image load of vss_ps.dll by uncommon executables*

Matches rule Shadow Copies Deletion Using Operating Systems Utilities by Florian Roth (Nextron Systems), Michael Haag, Teymur Kheirkhabarov, Daniil Yugoslavskiy, oscd.community, Andreas Hunkeler (@Karneades) at Sigma Integrated Rule Set (GitHub)
↳ *Shadow Copies deletion using operating systems utilities*

Matches rule Startup Folder File Write by Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research) at Sigma Integrated Rule Set (GitHub)
↳ *A General detection for files being created in the Windows startup directory. This could be an indicator of persistence.*

Matches rule CurrentVersion Autorun Keys Modification by Victor Sergeev, Daniil Yugoslavskiy, Gleb Sukhodolskiy, Timur Zinniatullin, oscd.community, Tim Shelton, frack113 (split) at Sigma Integrated Rule Set (GitHub)
↳ *Detects modification of autostart extensibility point (ASEP) in registry.*

Matches rule Suspicious Process Creation by Florian Roth at SOC Prime Threat Detection Marketplace
↳ *Detects suspicious process starts on Windows systems based on keywords*

See all

Network Communication

IP Traffic

- UDP 192.168.0.38:138
- TCP 20.99.185.48:443
- UDP 192.168.0.16:138

Memory Pattern Domains

- cdn.rubyinstaller.org
- chocolatey.org
- chocolatey.org).
- download.sysinternals.com
- ferventcoder.com.
- gist.github.com
- github.com
- learn-powershell.net
- nsis.sourceforge.net
- poshcode.org

- http://cdn.rubyinstaller.org/archives/devkits/DevKit-mingw64-64-4.7.2-20130224-1432-sfx.exe
- http://download.sysinternals.com/Files/SysinternalsSuite.zip
- http://download.sysinternals.com/Files/SysinternalsSuitex64.zip
- http://ferventcoder.com.
- http://learn-powershell.net/2013/02/08/powershell-and-events-object-events/
- http://nsis.sourceforge.net/Docs/AppendixD.html
- http://poshcode.org/2513
- http://poshcode.org/417
- http://powershell.com/cs/blogs/tips/archive/2009/02/05/validating-a-url.aspx

Behavior Similarity Hashes

CAPA	411d88e8aac161067d4a0df8c3d0be03
CAPE Sandbox	df36ee65d2d4e71629c57dbb56ff8ae0
Microsoft Sysinternals	117935d2b4f160b4deaf0534b6521454
VirusTotal Jujubox	6c53f546b079b910e6d88964e72f70ec
VirusTotal Observer	938832b00fe0776ee2ac426067ce1062
Zenbox	374fa4ea4258db91a5ac319524cb9dcd

File system actions

Files Opened

- \Device\NamedPipe\
- \Device\RdpDr
- <Anonymous Pipe>
- C:\$Recycle.Bin\
- C:\$Recycle.Bin\S-1-5-21-4270068108-2931534202-3907561125-1001\
- C:\$Recycle.Bin\S-1-5-21-4270068108-2931534202-3907561125-1001\desktop.ini
- C:\$Recycle.Bin\S-1-5-21-4270068108-2931534202-3907561125-1001\desktop.ini.id-ACFEEEC3.[aerossh@nerdmail.co].AeR
- C:\Config.Msi\
- C:\Documents and Settings\
- C:\PerfLogs\

Files Written

- C:\$Recycle.Bin\S-1-5-21-4270068108-2931534202-3907561125-1001\desktop.ini.id-ACFEEEC3.[aerossh@nerdmail.co].AeR
- C:\Program Files\Common Files\Microsoft Shared\Stationery\Desktop.ini.id-ACFEEEC3.[aerossh@nerdmail.co].AeR
- C:\Program Files\Common Files\Microsoft Shared\VC\msdia100.dll.id-ACFEEEC3.[aerossh@nerdmail.co].AeR
- C:\Program Files\Common Files\Microsoft Shared\VC\msdia90.dll.id-ACFEEEC3.[aerossh@nerdmail.co].AeR
- C:\Program Files\desktop.ini.id-ACFEEEC3.[aerossh@nerdmail.co].AeR
- C:\Program Files\dotnet\LICENSE.txt.id-ACFEEEC3.[aerossh@nerdmail.co].AeR
- C:\Program Files\dotnet\dotnet.exe.id-ACFEEEC3.[aerossh@nerdmail.co].AeR
- C:\Program Files\dotnet\host\fxr\5.0.15\hostfxr.dll.id-ACFEEEC3.[aerossh@nerdmail.co].AeR
- C:\Program Files\dotnet\host\fxr\6.0.3\hostfxr.dll.id-ACFEEEC3.[aerossh@nerdmail.co].AeR
- C:\Program Files\dotnet\shared\Microsoft.NETCore.App\5.0.15\.version.id-ACFEEEC3.[aerossh@nerdmail.co].AeR

Files Deleted

- %USERPROFILE%\AppData\Local\Microsoft\Windows\Caches\{3DA71D5A-20CC-432F-A115-DFE92379E91F}.3.ver0x0000000000000018.db.id-584D2235.[aerossh@nerdmail.co].AeR
- %USERPROFILE%\AppData\Local\Microsoft\Windows\Caches\{3DA71D5A-20CC-432F-A115-DFE92379E91F}.3.ver0x0000000000000019.db.id-584D2235.[aerossh@nerdmail.co].AeR
- C:\$Recycle.Bin\S-1-5-21-4270068108-2931534202-3907561125-1001\desktop.ini
- C:\Program Files\Common Files\Microsoft Shared\Stationery\Desktop.ini

C:\Program Files\desktop.ini
C:\Program Files\dotnet\LICENSE.txt
C:\Program Files\dotnet\ThirdPartyNotices.txt

Files Copied

C:\Program Files\Common Files\Microsoft Shared\ink\FlickAnimation.avi
C:\Program Files\Common Files\Microsoft Shared\ink\InkObj.dll
C:\Program Files\Common Files\Microsoft Shared\ink\hwruklm.dat
C:\Program Files\Common Files\Microsoft Shared\ink\hwruksh.dat
C:\Program Files\Common Files\Microsoft Shared\ink\hwrusalm.dat
C:\Program Files\Common Files\Microsoft Shared\ink\hwrusash.dat
C:\Program Files\Common Files\Microsoft Shared\ink\micaut.dll
C:\Program Files\Common Files\Microsoft Shared\ink\mraut.dll
C:\Program Files\DVD Maker\Shared\DvdStyles\Performance\Title_Page.wmv
C:\Program Files\DVD Maker\Shared\DvdStyles\Performance\Title_Page_PAL.wmv

Files Dropped

%SAMPLEPATH%\0197EB32A39518ADBC118EC0559A395C.id-584D2235.[aerossh@nerdmail.co].AeR

%SAMPLEPATH%\5e75ef02517afd6e8ba6462b19217dc4a5a574abb33d10eb0f2bab49d8d48c22.id-584D2235.[aerossh@nerdmail.co].AeR

%SAMPLEPATH%\findings.xml.id-584D2235.[aerossh@nerdmail.co].AeR

%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\0197EB32A39518ADBC118EC0559A395C.exe

%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\5e75ef02517afd6e8ba6462b19217dc4a5a574abb33d10eb0f2bab49d8d48c22.exe

C:\$Recycle.Bin\%SID%294\desktop.ini.id-584D2235.[aerossh@nerdmail.co].AeR

C:\$Recycle.Bin\%SID%\desktop.ini.id-584D2235.[aerossh@nerdmail.co].AeR

C:\$Recycle.Bin\S-1-5-18\desktop.ini.id-584D2235.[aerossh@nerdmail.co].AeR

C:\BOOTNXT.id-584D2235.[aerossh@nerdmail.co].AeR

C:\Boot\BOOTSTAT.DAT.id-584D2235.[aerossh@nerdmail.co].AeR

Registry actions

Registry Keys Opened

HKEY_CURRENT_USER\Network
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
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DelayedExpansion
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DisableUNCCheck
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\EnableExtensions
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\PathCompletionChar
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders

Registry Keys Set

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\tmpvk6c9hgm.exe

+ HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\0197EB32A39518ADBC118EC0559A395C.exe
+ HKEY_USERS\S-1-5-21-4270068108-2931534202-3907561125-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.exe\OpenWithProgids\exefile
+ HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\file.exe

Process and service actions

Processes Created

%SAMPLEPATH%\0197EB32A39518ADBC118EC0559A395C.exe
%SAMPLEPATH%\5e75ef02517afd6e8ba6462b19217dc4a5a574abb33d10eb0f2bab49d8d48c22.exe
C:\Windows\System32\cmd.exe
C:\Windows\System32\mode.com
C:\Windows\System32\vssadmin.exe
C:\Windows\system32\cmd.exe
mode con cp select=1251
vssadmin delete shadows /all /quiet
"C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\file.exe"
"C:\Windows\System32\file.exe"

Shell Commands

mode con cp select=1251
"%SAMPLEPATH%\0197EB32A39518ADBC118EC0559A395C.exe"
"%SAMPLEPATH%\5e75ef02517afd6e8ba6462b19217dc4a5a574abb33d10eb0f2bab49d8d48c22.exe"
"C:\Windows\system32\cmd.exe"
vssadmin delete shadows /all /quiet

Processes Terminated

C:\Windows\System32\cmd.exe
C:\Windows\System32\conhost.exe
C:\Windows\System32\mode.com
C:\Windows\System32\vssadmin.exe
mode con cp select=1251
2064 - mode con cp select=1251
2108 - vssadmin delete shadows /all /quiet
2204 - "C:\Windows\system32\cmd.exe"
C:\Windows\System32\file.exe

Processes Tree

1504 - "C:\Users\<USER>\AppData\Local\Temp\tmpqdokmwzg.exe"
↳ 1252 - "C:\Windows\system32\cmd.exe"
2788 - %WINDIR%\explorer.exe
↳ 2440 - %SAMPLEPATH%\0197EB32A39518ADBC118EC0559A395C.exe
↳ 3232 - C:\Windows\System32\cmd.exe
↳ 3856 - C:\Windows\System32\mode.com
↳ 3144 - C:\Windows\System32\vssadmin.exe
2964 - 0197EB32A39518ADBC118EC0559A395C.exe
↳ 2204 - C:\Windows\system32\cmd.exe
↳ 2108 - vssadmin delete shadows /all /quiet

Global\syncronize_99ZS08U

Mutexes Created

Global\syncronize_99ZS08A
Global\syncronize_99ZS08U
\Sessions\1\BaseNamedObjects\Global\syncronize_99ZS08A
\Sessions\1\BaseNamedObjects\Global\syncronize_99ZS08U

Modules loaded

Runtime Modules

ADVAPI32.DLL
DAVCLNT.DLL
DRPROV.DLL
KERNEL32.DLL
MPR.DLL
NTDLL.DLL
NTLANMAN.DLL
RPCRT4.DLL
SECHOST.DLL
SHELL32.DLL

Highlighted actions

Calls Highlighted

CloseHandle
CloseServiceHandle
CompareStringA
CompareStringW
ControlService
CreateFileW
CreateMutexW
CreatePipe
CreateProcessW
CreateThread