

46

/ 68

Community Score

-38

⚠️ 46/68 security vendors flagged this file as malicious

Reanalyze

Similar

More


d609799091731d83d75ec5d1f030571af20c45efeeb94840b...

Size

4.09 MB

Last Analysis Date

1 year ago



xxx.exe

peexe

64bits

runtime-modules

assembly

direct-cpu-clock-access

checks-user-input

- DETECTION
- DETAILS
- RELATIONS
- BEHAVIOR
- COMMUNITY7

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

Display grouped sandbox reports

<input checked="" type="checkbox"/>		C2AE	 0	 0	 0	 0	 0	 0	<input checked="" type="checkbox"/>		Microsoft ...	 0	 0	 0	 0	 47	 4
<input checked="" type="checkbox"/>		VirusTotal...	 0	 0	 0	 0	 0	 0	<input checked="" type="checkbox"/>		VirusTotal...	 0	 0	 0	 0	 0	 0
<input checked="" type="checkbox"/>		Yomi Hun...	 0	 0	 0	 0	 0	 0	<input checked="" type="checkbox"/>		Zenbox	 3	 8	 0	 0	 99+	 2

Activity Summary

Download ArtifactsFull ReportsHelp

⚠️ 3 Detections

1 MALWARE1 RANSOM1 EVADER

📅 IDS Rules

NOT FOUND

📁 Dropped Files

47 OTHER1 TEXT1 PDF1 PE_EXE1 XML1 JAR1 ZIP1 TTF1 JAVASCRIPT

📜 Mitre Signatures

6 LOW25 INFO

📄 Sigma Rules

NOT FOUND

🌐 Network comms

2 DNS4 IP

Behavior Tags

calls-wmichecks-cpu-namechecks-user-inputdetect-debug-environmentdirect-cpu-clock-accessruntime-modules

Dynamic Analysis Sandbox Detections

⚠️ The sandbox Zenbox flags this file as: MALWARE RANSOM EVADER

MITRE ATT&CK Tactics and Techniques

+ ExecutionTA0002

+ PersistenceTA0003

+ Privilege EscalationTA0004

+ Defense EvasionTA0005

+ Credential AccessTA0006

+ DiscoveryTA0007

+ Collection

↑

?

Sign inSign up

%USERPROFILE%\AppData\Local\Temp__PSScriptPolicyTest_isolacfk.qu5.psm1

%USERPROFILE%\AppData\Local\Temp__PSScriptPolicyTest_iynq4f4e.mwt.ps1

▼

Files Dropped

%USERPROFILE%\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\powershell.exe.log

%USERPROFILE%\AppData\Local\Temp\MpCmdRun.log

%USERPROFILE%\AppData\Local\Temp__PSScriptPolicyTest_0mxyjab3.dg0.ps1

%USERPROFILE%\AppData\Local\Temp__PSScriptPolicyTest_1ojqoymw.dai.ps1

%USERPROFILE%\AppData\Local\Temp__PSScriptPolicyTest_2k00zswy.eht.ps1

%USERPROFILE%\AppData\Local\Temp__PSScriptPolicyTest_az1s2alu.ykg.ps1

%USERPROFILE%\AppData\Local\Temp__PSScriptPolicyTest_bk1014ip.hjd.psm1

%USERPROFILE%\AppData\Local\Temp__PSScriptPolicyTest_f22pizho.hja.psm1

%USERPROFILE%\AppData\Local\Temp__PSScriptPolicyTest_hosrguza.emx.psm1

%USERPROFILE%\AppData\Local\Temp__PSScriptPolicyTest_isolacfk.qu5.psm1

▼

Registry actions ⓘ

^

↑

💬

?

☀

Sign in

Sign up

C:\Windows\system32\net1 stop "UI0Detect" /y

C:\Windows\system32\net1 stop "UnistoreSvc_173d3" /y

C:\Windows\system32\net1 stop "UnistoreSvc_17422" /y

Processes Injected

%SAMPLEPATH%\d609799091731d83d75ec5d1f030571af20c45efeeb94840b67ea09a3283ab65.exe

%SAMPLEPATH%\xxx.exe

Processes Terminated

wmiadap.exe /F /T /R

C:\Program Files\Windows Defender\MpCmdRun.exe

C:\Windows\System32\VSSVC.exe

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

C:\Windows\System32\bcdedit.exe

C:\Windows\System32\cmd.exe

C:\Windows\System32\conhost.exe

C:\Windows\System32\net.exe

C:\Windows\System32\net1.exe

Processes Tree

2768 - %CONHOST% "961471805-395531161-1565322554-997437775-164933045-1894327277504017605-596914945

2764 - %CONHOST% "1854457122-109302098511484862486600991714399864621264650935-285949995-1495499425

2836 -

2464 - wmiadap.exe /F /T /R

2696 - %SAMPLEPATH%

↳ 284 - cmd.exe /c powershell Set-MpPreference -DisableIOAVProtection \$true

↳ 2828 - powershell Set-MpPreference -DisableIOAVProtection \$true

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

2828 - %WINDIR%\explorer.exe

↳ 2480 - %SAMPLEPATH%\xxx.exe

Modules loaded ⓘ

Runtime Modules

%SAMPLEPATH%\d609799091731d83d75ec5d1f030571af20c45efeeb94840b67ea09a3283ab65.exe

C:\Windows\System32\wbem\wmiutils.dll

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

API-MS-WIN-Service-Management-L1-1-0.dll

API-MS-Win-Core-LocalRegistry-L1-1-0.dll

C:\Windows\System32\wship6.dll

C:\Windows\System32\wshqos.dll

C:\Windows\System32\wshtcpip.dll

C:\Windows\system32\tzres.dll

advapi32.dll

We use cookies and related technologies to remember user preferences, for security, to analyse our traffic, and to enable website functionality. Learn more about cookies in our [Privacy Notice](#).

Ok

Page 5 of 6

