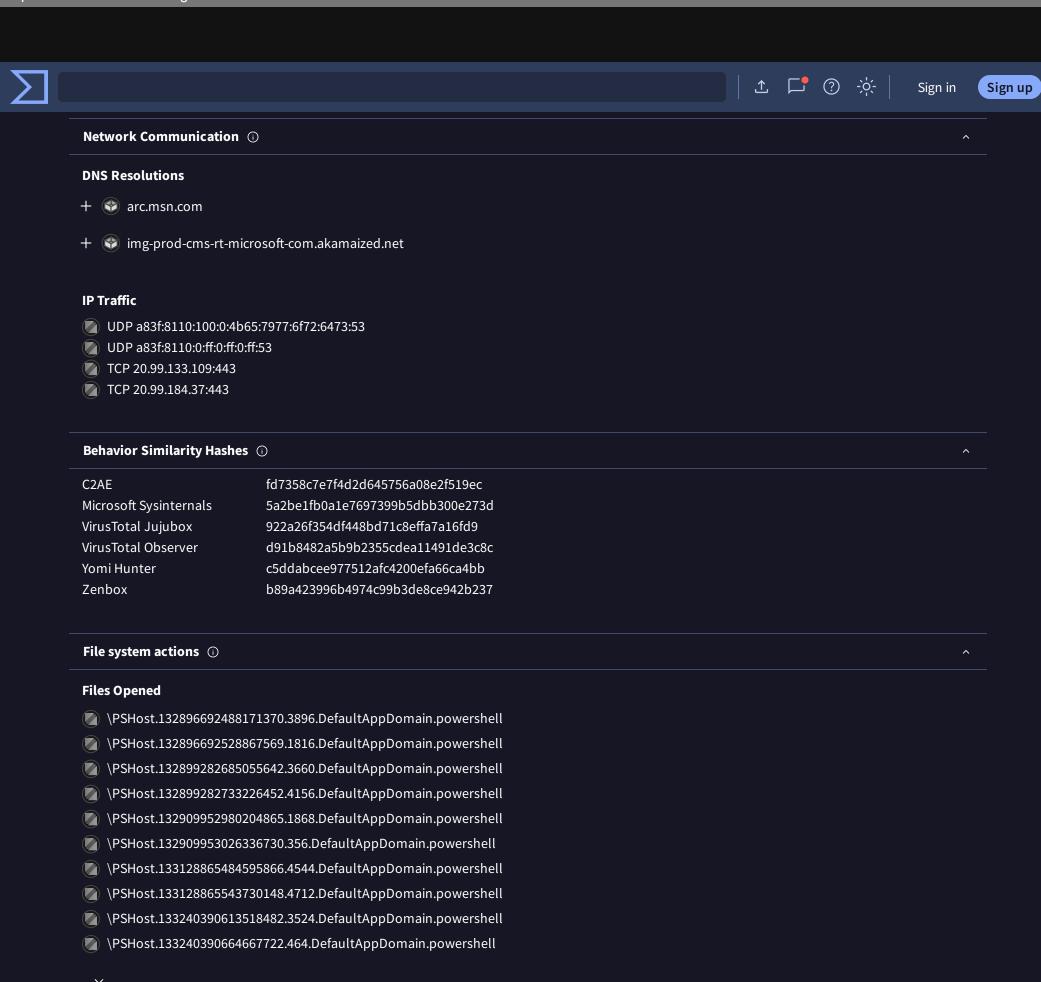


Page 1 of 6



Files Written

- C:\lIJl5Cu_bEookddlGZZ_mHGCvJquxTe2vMxaKIA-3Fr_.key.7afuy
- © C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\UPnP Device Host\upnphost\udhisapi.dll
- © C:\Windows\System32\Tasks\Microsoft\Windows\DiskDiagnostic\Microsoft-Windows-DiskDiagnosticDataCollector
- \Sessions\1\BaseNamedObjects
- C:\\$SysReset\Logs\PushButtonReset.etl.ScnniJjW-VMGDgGzyyuXmilDxWOGUw9x4FJKIdEe8Qf_AAAAAAAAAAAAA.7afuy
- 😵 C:\\$SysReset\Logs\PushButtonReset.etl.XA2g6upQ0ynCFXMefzxsXMgpVLmLGhgsLQjX9clmBsn_KAAAACgAAAA0.7afuy
- C:\\$SysReset\Logs\SessionID.xml.ScnniJjW-VMGDgGzyyuXmilDxWOGUw9x4FJKIdEe8Qf_GgAAABoAAAA0.7afuy
- 😵 C:\\$SysReset\Logs\SessionID.xml.XA2g6upQ0ynCFXMefzxsXMgpVLmLGhgsLQjX9clmBsn_KAAAACgAAAA0.7afuy
- 😵 C:\\$SysReset\Logs\Timestamp.xml.ScnniJjW-VMGDgGzyyuXmilDxWOGUw9x4FJKldEe8Qf_AAAAAAAAAAA0.7afuy
- C:\\$SysReset\Logs\Timestamp.xml.XA2g6upQ0ynCFXMefzxsXMgpVLmLGhgsLQjX9clmBsn_KAAAACgAAAA0.7afuy

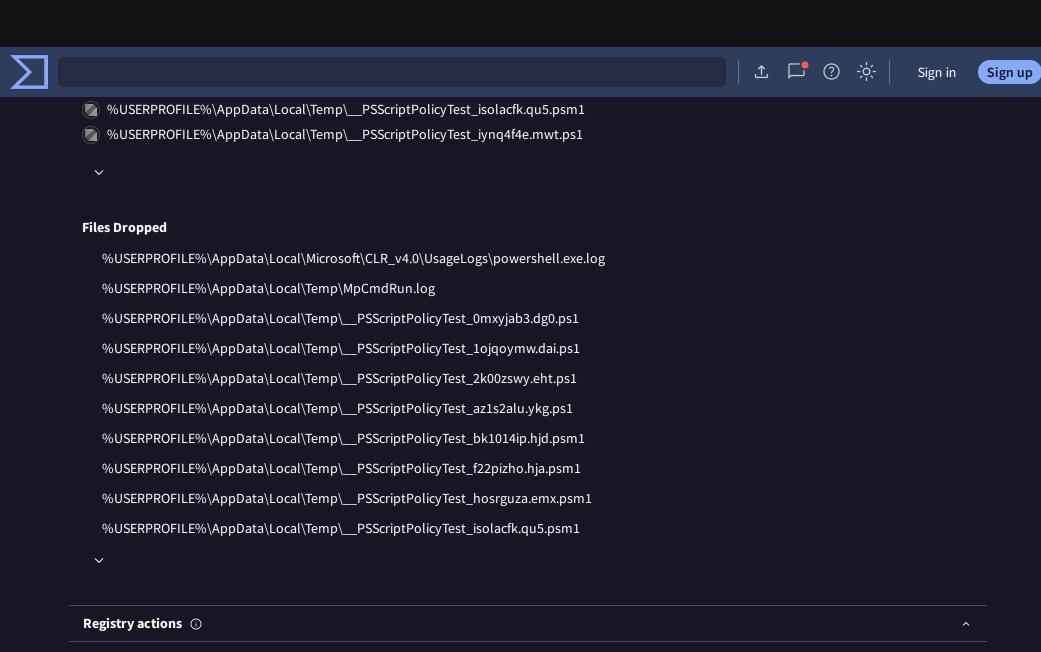
Files Deleted

- %USERPROFILE%\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\powershell.exe.log
- %USERPROFILE%\AppData\Local\Temp__PSScriptPolicyTest_0mxyjab3.dg0.ps1

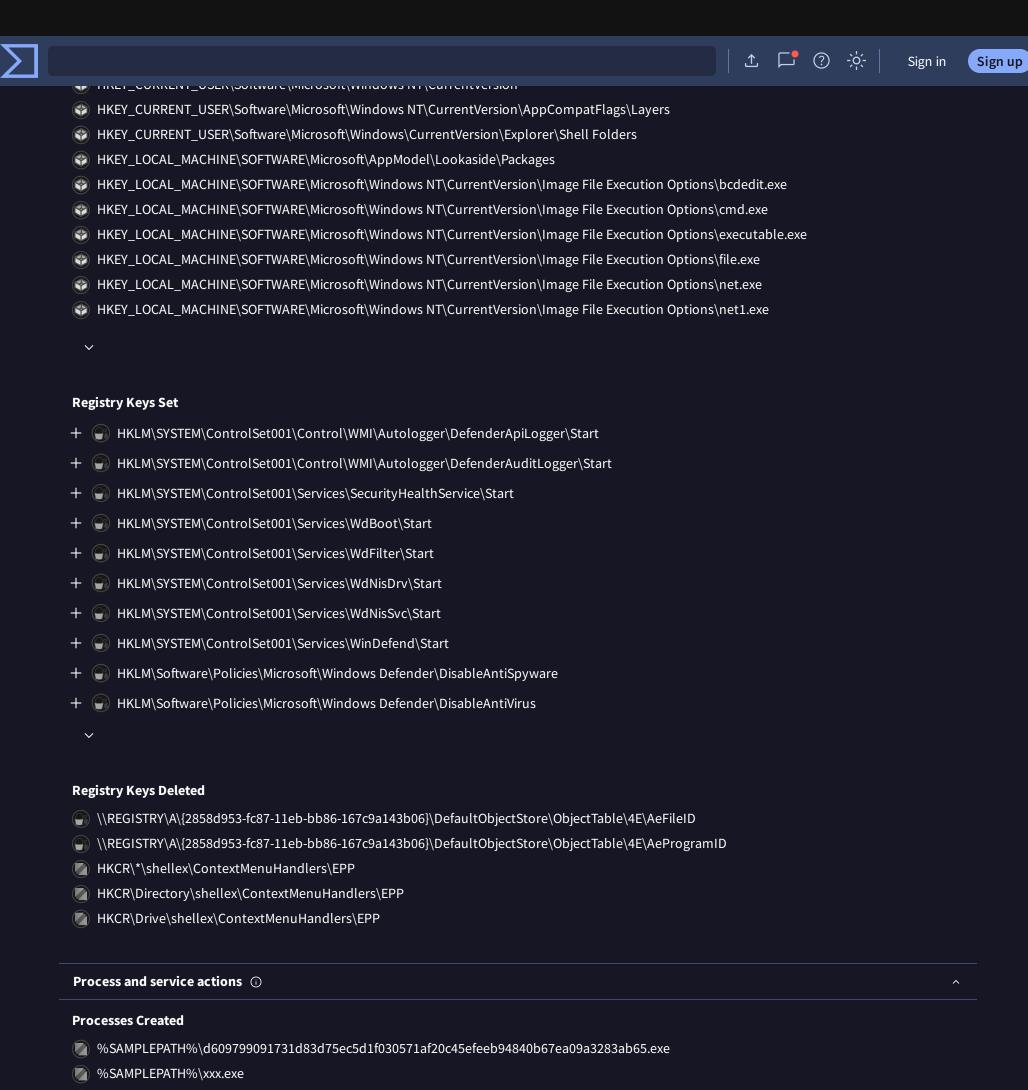
%USERPROFILE%\AppData\Local\Temp__PSScriptPolicyTest_1ojqoymw.dai.ps1

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 <u>Privacy Notice</u>.

%USERPROFILE%\AppData\Local\Temp\ PSScriptPolicyTest_bk1014ip.hid.psm



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 <u>Privacy Notice</u>.



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

C:\Windows\System32\bcdedit.exe

C:\Windows\System32\cmd.exe

C:\Windows\System32\net.exe

C:\Windows\System32\net1.exe

C:\Windows\System32\reg.exe

C:\Windows\System32\sc.exe

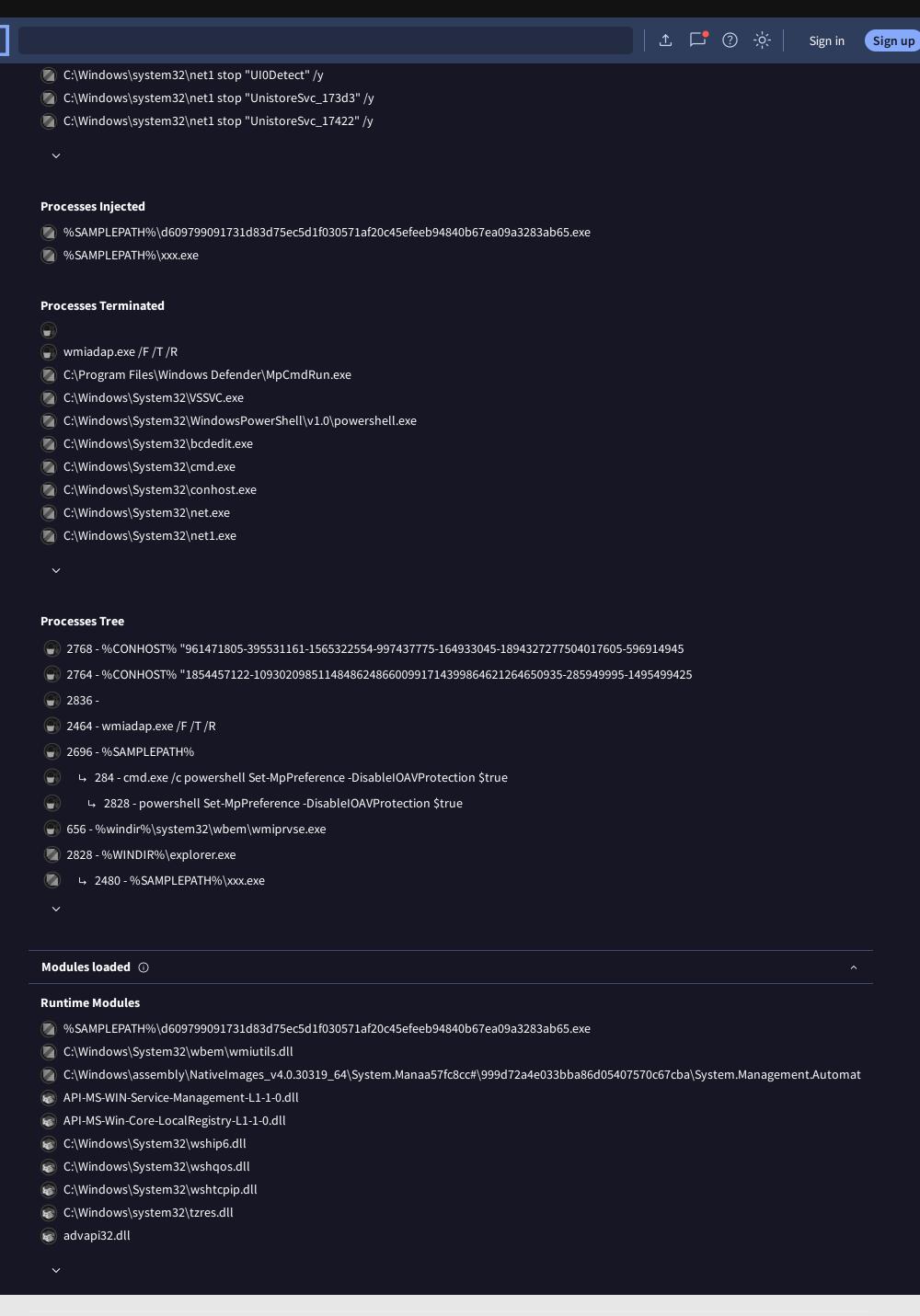
C:\Windows\System32\schtasks.exe

Shell Commands

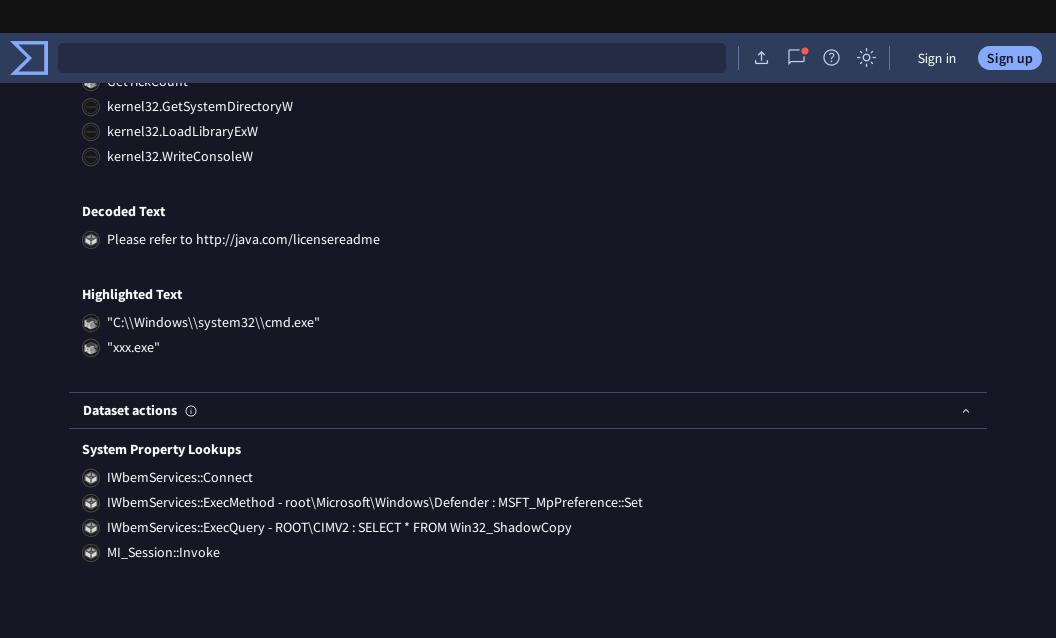
V

"%SAMPLEPATH%\d609799091731d83d75ec5d1f030571af20c45efeeb94840b67ea09a3283ab65.exe"

We use cookies and related technologies to remember user preferences, for security, to analyse our traffic, and to enable website functionality. Learn Cookies in our Privacy Notice.



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 <u>Privacy Notice</u>.



Our product	Community	10015	Premium Services	Documentation
Contact Us	Join Community	API Scripts	Get a demo	Searching
Get Support	Vote and Comment	YARA	Intelligence	Reports
How It Works	Contributors	Desktop Apps	Hunting	API v3 v2
ToS Privacy Notice	Top Users	Browser Extensions	Graph	Use Cases
Blog Releases	Community Buzz	Mobile App	API v3 v2	

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 <u>Privacy Notice</u>.