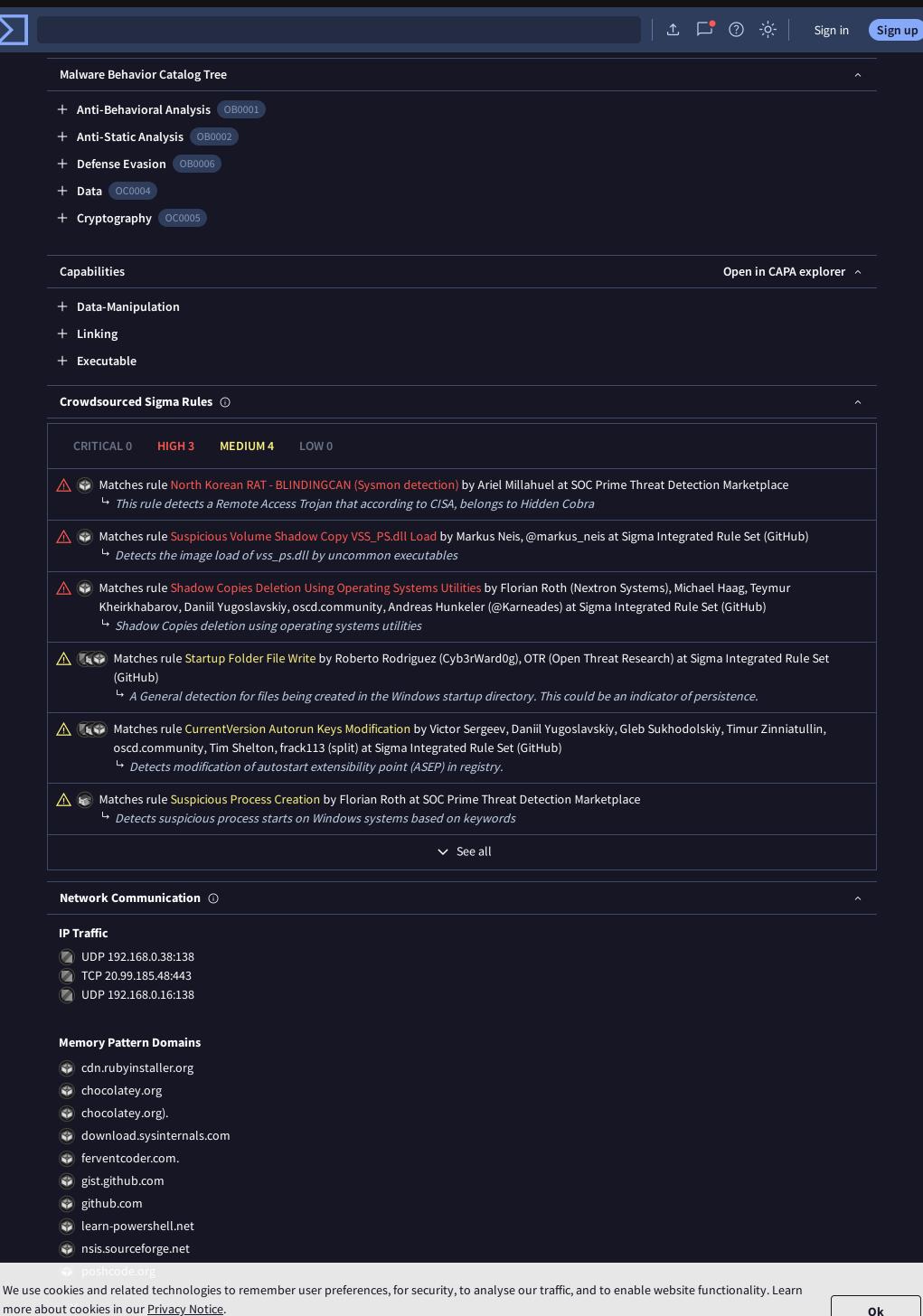
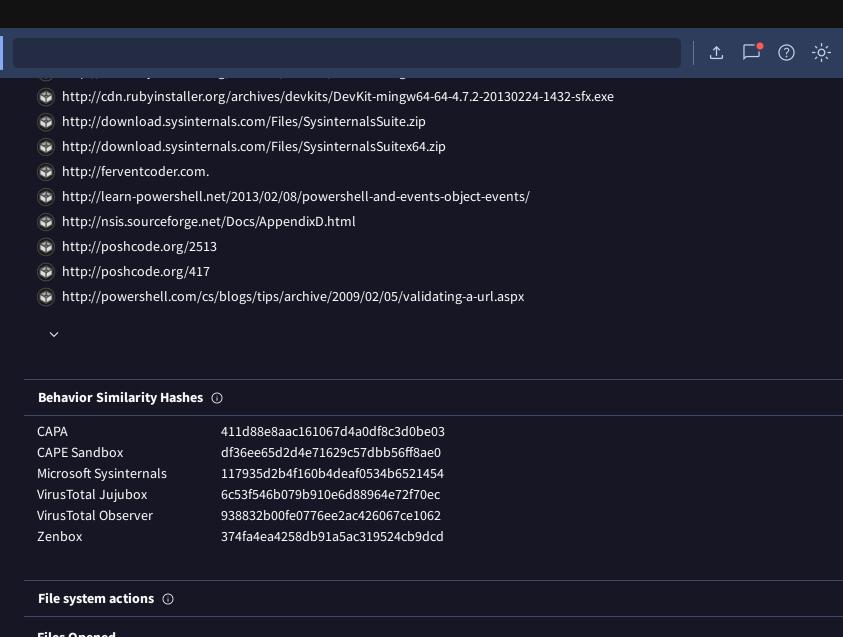


We use cookies and related technologies to remember user preferences, for security, to analyse our traffic, and to enable website functionality. Learn more about cookies in our <u>Privacy Notice</u>.



Page 2 of 6



#### **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

V

%USERPROFILE%\AppData\Local\Microsoft\Windows\Caches\{3DA71D5A-20CC-432F-A115-DFE92379E91F}.3.ver0x00000000000018.db.id-584D2235.[aerossh@nerdmail.co].AeR

%USERPROFILE%\AppData\Local\Microsoft\Windows\Caches\{3DA71D5A-20CC-432F-A115-DFE92379E91F}.3.ver0x0000000000019.db.id-

584D2235.[aerossh@nerdmail.co].AeR

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 <a href="Privacy Notice">Privacy Notice</a>.

C:\Program Files\Common Files\Microsoft Shared\Stationery\Desktop.in

Ok

Sign in

Sign up













- 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** ①

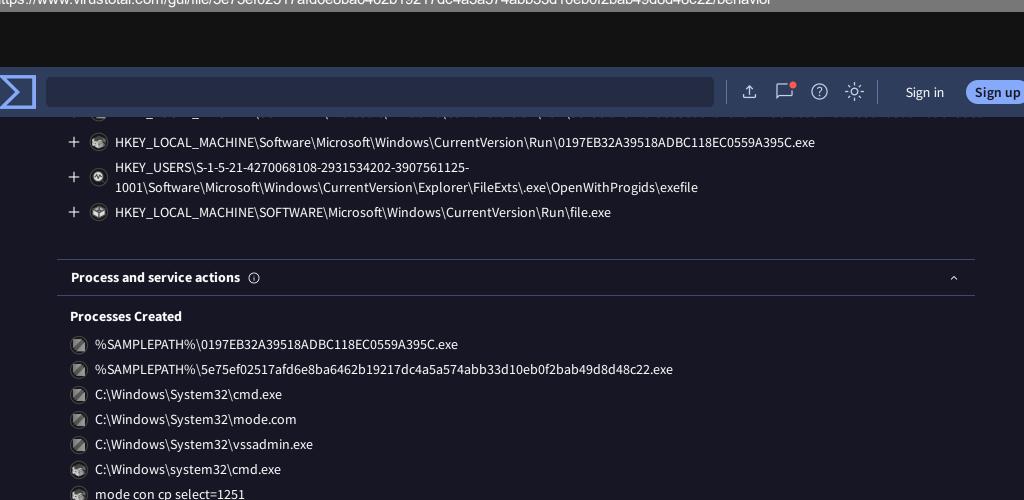
## **Registry Keys Opened**

- HKEY CURRENT USER\Network
- HKEY\_CURRENI\_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

V

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.



#### **Shell Commands**

- mode con cp select=1251
- "%SAMPLEPATH%\0197EB32A39518ADBC118EC0559A395C.exe"
- "%SAMPLEPATH%\5e75ef02517afd6e8ba6462b19217dc4a5a574abb33d10eb0f2bab49d8d48c22.exe"

"C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\file.exe"

- C:\Windows\system32\cmd.exe"
- vssadmin delete shadows /all /quiet

wssadmin delete shadows /all /quiet

"C:\Windows\System32\file.exe"

## **Processes Terminated**

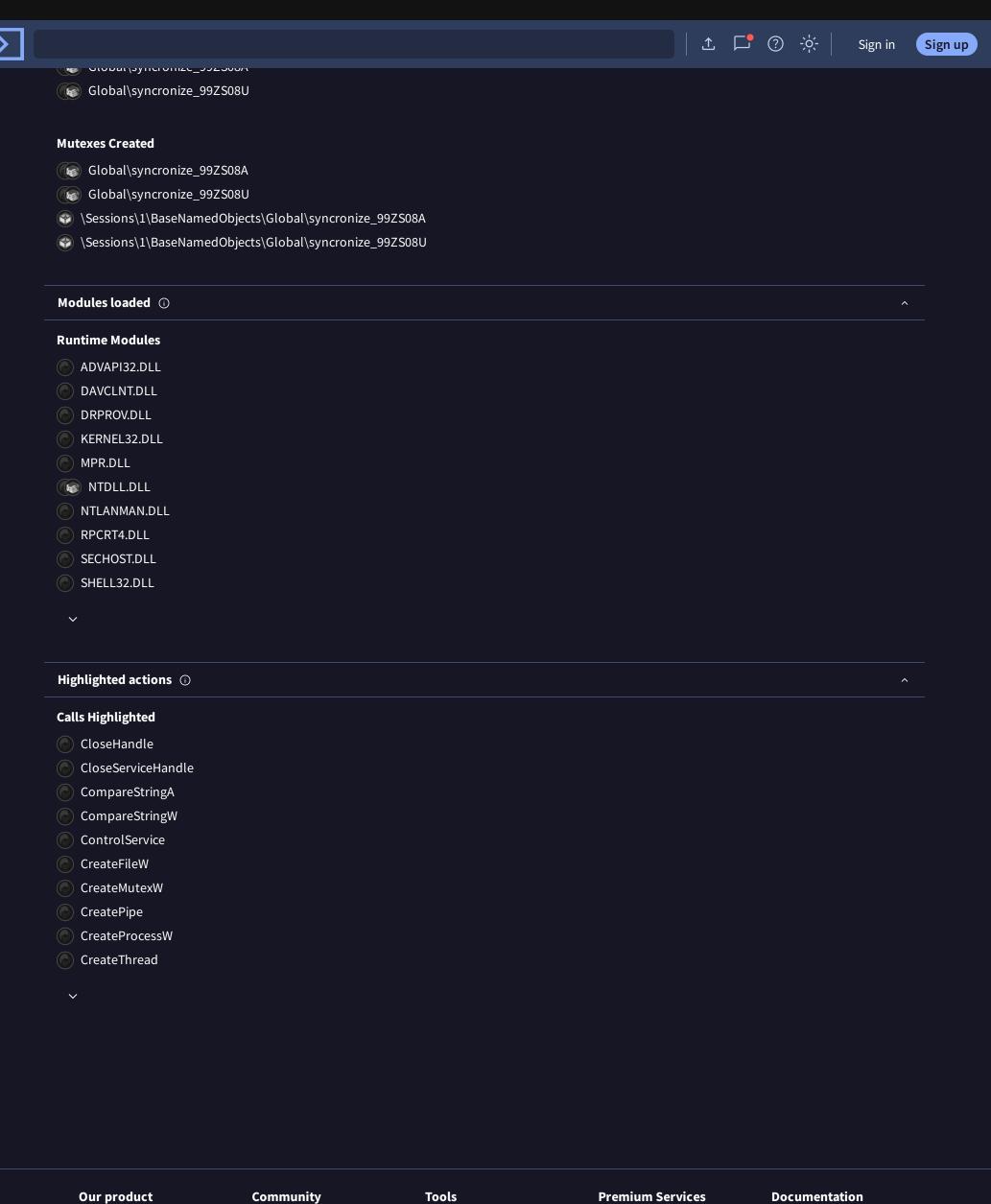
- C:\Windows\System32\cmd.exe
- C:\Windows\System32\conhost.exe
- C:\Windows\System32\mode.com
- C:\Windows\System32\vssadmin.exe
- mode con cp select=1251
- ② 2064 mode con cp select=1251
- 2108 vssadmin delete shadows /all /quiet
- 2204 "C:\Windows\system32\cmd.exe"
- C:\Windows\System32\file.exe

## **Processes Tree**

- 1504 "C:\Users\<USER>\AppData\Local\Temp\tmpqdokmwzg.exe"
- ☐ → 1252 "C:\Windows\system32\cmd.exe"
- 2788 %WINDIR%\explorer.exe

- 2964 0197EB32A39518ADBC118EC0559A395C.exe
- □ 2204 C:\Windows\system32\cmd.exe
- ⇒ 2108 vssadmin delete shadows /all /quiet

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>. Signals



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

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>.