Untangling KNOTWEED: European private-sector offensive actor using 0-day exploits

⋮ 7/27/2022

The Microsoft Threat Intelligence Center (MSTIC) and the Microsoft Security Response Center (MSRC) found a private-sector offensive actor (PSOA) using multiple Windows and Adobe 0-day exploits, including one for the recently patched CVE-2022-22047, in limited and targeted attacks against European and Central American customers. The PSOA, which MSTIC tracks as KNOTWEED, developed malware called Subzero which was used in these attacks.

This blog details Microsoft's analysis of the observed KNOTWEED activity and related malware used in targeted attacks against our customers. This information is shared with our customers and industry partners to improve detection of these attacks. Customers are encouraged to expedite deployment of the July 2022 Microsoft security updates to protect their systems against exploits using CVE-2022-22047. Microsoft Defender Antivirus and Microsoft Defender for Endpoint have also implemented detections against KNOTWEED's malware and tools.

PSOAs, which Microsoft also refers to as cyber mercenaries, sell hacking tools or services through a variety of business models. Two common models for this type of actor are access-as-a-service and hack-for-hire. In access-as-a-service, the actor sells full end-to-end hacking tools that can be used by the purchaser in operations, with the PSOA not involved in any targeting or running of the operation. In hack-for-hire, detailed information is provided by the purchaser to the actor, who then runs the targeted operations. Based on observed attacks and news reports, MSTIC believes that KNOTWEED may blend these models: they sell the Subzero malware to third parties but have also been observed using KNOTWEED-associated infrastructure in some attacks, suggesting more direct involvement.

Who is KNOTWEED?

KNOTWEED is an Austria-based PSOA named DSIRF. The DSIRF website [web archive link] says they provide services *"to multinational corporations in the technology, retail, energy and financial sectors*" and that they have "*a set of highly sophisticated techniques in gathering and analyzing information.*" They publicly offer several services including "*an enhanced due diligence and risk analysis process through providing a deep understanding of individuals and entities"* and *"highly sophisticated Red Teams to challenge your company's most critical assets."*

However, multiple news reports have linked DSIRF to the development and attempted sale of a malware toolset called Subzero. MSTIC found the Subzero malware being deployed through a variety of methods, including 0-day exploits in Windows and Adobe Reader, in 2021 and 2022. As part of our investigation into the utility of this malware, Microsoft's communications with a Subzero victim revealed that they had not commissioned any red teaming or penetration testing, and confirmed that it was unauthorized, malicious activity. Observed victims to date include law firms, banks, and strategic consultancies in countries such as Austria, the United Kingdom, and Panama. It's

important to note that the identification of targets in a country doesn't necessarily mean that a DSIRF customer resides in the same country, as international targeting is common.

MSTIC has found multiple links between DSIRF and the exploits and malware used in these attacks. These include command-and-control infrastructure used by the malware directly linking to DSIRF, a DSIRF-associated GitHub account being used in one attack, a code signing certificate issued to DSIRF being used to sign an exploit, and other open-source news reports attributing Subzero to DSIRF.

Observed actor activity

KNOTWEED initial access

MSTIC found KNOTWEED's Subzero malware deployed in a variety of ways. In the succeeding sections, the different stages of Subzero are referred to by their Microsoft Defender detection names: *Jumplump* for the persistent loader and *Corelump* for the main malware.

KNOTWEED exploits in 2022

In May 2022, MSTIC found an Adobe Reader remote code execution (RCE) and a 0-day Windows privilege escalation exploit chain being used in an attack that led to the deployment of Subzero. The exploits were packaged into a PDF document that was sent to the victim via email. Microsoft was not able to acquire the PDF or Adobe Reader RCE portion of the exploit chain, but the victim's Adobe Reader version was released in January 2022, meaning that the exploit used was either a 1-day exploit developed between January and May, or a 0-day exploit. Based on KNOTWEED's extensive use of other 0-days, we assess with medium confidence that the Adobe Reader RCE is a 0-day exploit. The Windows exploit was analyzed by MSRC, found to be a 0-day exploit, and then patched in July 2022 as CVE-2022-22047. Interestingly, there were indications in the Windows exploit code that it was also designed to be used from Chromium-based browsers, although we've seen no evidence of browser-based attacks.

The CVE-2022-22047 vulnerability is related to an issue with activation context caching in the Client Server Run-Time Subsystem (CSRSS) on Windows. At a high level, the vulnerability could enable an attacker to provide a crafted assembly manifest, which would create a malicious activation context in the activation context cache, for an arbitrary process. This cached context is used the next time the process spawned.

CVE-2022-22047 was used in KNOTWEED related attacks for privilege escalation. The vulnerability also provided the ability to escape sandboxes (with some caveats, as discussed below) and achieve system-level code execution. The exploit chain starts with writing a malicious DLL to disk from the sandboxed Adobe Reader renderer process. The CVE-2022-22047 exploit was then used to target a system process by providing an application manifest with an undocumented attribute that specified the path of the malicious DLL. Then, when the system process next spawned, the attribute in the malicious activation context was used, the malicious DLL was loaded from the given path, and system-level code execution was achieved.

It's important to note that exploiting CVE-2022-22047 requires attackers to be able to write a DLL to disk. However, in the threat model of sandboxes, such as that of Adobe Reader and Chromium, the ability to write out files where the attacker *cannot* control the path isn't considered dangerous. Hence, these sandboxes aren't a barrier to the exploitation of CVE-2022-22047.

KNOTWEED exploits in 2021

In 2021, MSRC received a report of two Windows privilege escalation exploits (CVE-2021-31199 and CVE-2021-31201) being used in conjunction with an Adobe Reader exploit (CVE-2021-28550), all of which were patched in June 2021. MSTIC was able to confirm the use of these in an exploit chain used to deploy Subzero.

We were later able to link the deployment of Subzero to a fourth exploit, one related to a Windows privilege escalation vulnerability in the Windows Update Medic Service (CVE-2021-36948), which allowed an attacker to force the service to load an arbitrary signed DLL. The malicious DLL used in the attacks was signed by 'DSIRF GmbH'.

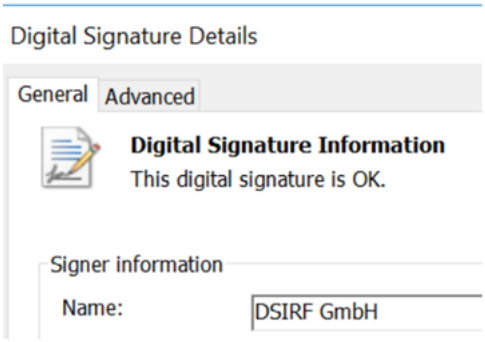

Figure 1. Valid digital signature from DSIRF on Medic Service exploit DLL

Malicious Excel documents

In addition to the exploit chains, another method of access that led to the deployment of Subzero was an Excel file masquerading as a real estate document. The file contained a malicious macro that was obfuscated with large chunks of benign comments from the Kama Sutra, string obfuscation, and use of Excel 4.0 macros.

```
Public Function DestinyPrevious(ReligiousDesire As Byte, BlowsSoftened As
Boolean) As String
'telling her about medicines for getting children, by talking to her
'about other people, by tales of various kinds, by stories about the
'wives of other men, and by praising her beauty, wisdom, generosity, and
'good nature, and then saying to her: "It is indeed a pity that you, who
'are so excellent a woman in every way, should be possessed of a husband
```

```
Function SeasonsOther(VatsagulmasDifficulty As String)
SeasonsOther = ExecuteExcel4Macro(VatsagulmasDifficulty)
```

Figure 2: Two examples of KNOTWEED Excel macro obfuscation

After de-obfuscating strings at runtime, the VBA macro uses the *ExecuteExcel4Macro* function to call native Win32 functions to load shellcode into memory allocated using *VirtualAlloc*. Each opcode is individually copied into a newly allocated buffer using *memset* before *CreateThread* is called to execute the shellcode.

```
"CALL(""ntdll"",""memset"",""JJJJ"",131072,232, 1)"  // 0xE8 0x00 0x00 0x00 0x00 call $+5
```

Figure 3: Copying opcodes

```
"CALL(""Kernel32"",""CreateThread"",""JJJJJJB"",0,0,131072,0,0,0)"
```

Figure 4: Calling CreateThread on shellcode

The following section describes the shellcode executed by the macro.

KNOTWEED malware and tactics, techniques, and procedures (TTPs)

Corelump downloader and loader shellcode

The downloader shellcode is the initial shellcode executed from either the exploit chains or malicious Excel documents. The shellcode's purpose is to retrieve the *Corelump* second-stage malware from the actor's command-and-control (C2) server. The downloader shellcode downloads a JPEG image that contains extra encrypted data appended to the end of the file (past the *0xFF 0xD9* marker that signifies the end of a JPEG file). The JPEG is then written to the user's *%TEMP%* directory.

Figure 5: One of the images embedded with the loader shellcode and Corelump

The downloader shellcode searches for a 16-byte marker immediately following the end of JPEG. After finding the marker, the downloader shellcode RC4 decrypts the loader shellcode using the next 16 bytes as the RC4 key. Finally, the loader shellcode RC4 decrypts the *Corelump* malware using a second RC4 key and manually loads it into memory.

Corelump malware

Corelump is the main payload and resides exclusively in memory to evade detection. It contains a variety of capabilities including keylogging, capturing screenshots, exfiltrating files, running a remote shell, and running arbitrary plugins downloaded from KNOTWEED's C2 server.

As part of installation, *Corelump* makes copies of legitimate Windows DLLs and overwrites sections of them with malicious code. As part of this process, *Corelump* also modifies the fields in the PE header to accommodate the nefarious changes, such as adding new exported functions, disabling Control Flow Guard, and modifying the image file checksum with a computed value from *CheckSumMappedFile.* These trojanized binaries (*Jumplump*) are dropped

to disk in *C:\Windows\System32\spool\drivers\color*, and COM registry keys are modified for persistence (see the Behaviors section for more information on COM hijacking).

Jumplump loader

Jumplump is responsible for loading *Corelump* into memory from the JPEG file in the %TEMP% directory. If *Corelump* is not present, *Jumplump* attempts to download it again from the C2 server. Both *Jumplump* and the downloader shellcode are heavily obfuscated to make analysis difficult, with most instructions being followed by a jmp to another instruction/jmp combination, giving a convoluted control flow throughout the program.

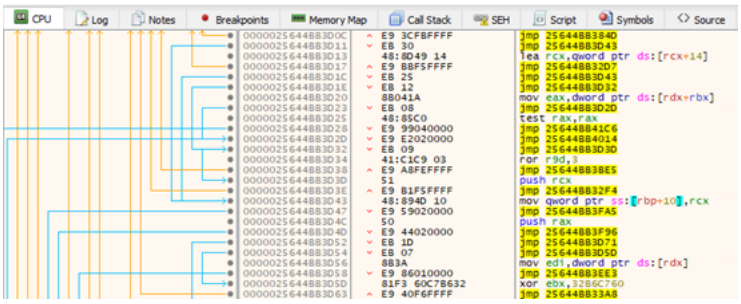

Figure 6: Disassembly showing the jmp/instruction obfuscation used in Jumplump

Mex and PassLib

KNOTWEED was also observed using the bespoke utility tools Mex and PassLib. These tools are developed by KNOTWEED and bear capabilities that are derived from publicly available sources. Mex, for example, is a command-line tool containing several red teaming or security plugins copied from GitHub (listed below):

Chisel	mimikatz	SharpHound3
Curl	Ping Castle	SharpOxidResolver
Grouper2	Rubeus	PharpPrinter
Internal Monologue	SCShell	SpoolSample
Inveigh	Seatbelt	StandIn
Lockless	SharpExec	

PassLib is a custom password stealer tool capable of dumping credentials from a variety of sources including web browsers, email clients, LSASS, LSA secrets, and the Windows credential manager.

Post-compromise actions

In victims where KNOTWEED malware had been used, a variety of post-compromise actions were observed:

- Setting of *UseLogonCredential* to “1” to enable plaintext credentials:
  - *reg add HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogonCredential /t REG_DWORD /d 1 /f*
- Credential dumping via *comsvcs.dll*:
  - *rundll32.exe C:\Windows\System32\comsvcs.dll, MiniDump*
- Attempt to access emails with dumped credentials from a KNOTWEED IP address
- Using Curl to download KNOTWEED tooling from public file shares such as *vultrobjects[.]com*
- Running PowerShell scripts directly from a GitHub gist created by an account associated with DSIRF

KNOTWEED infrastructure connections to DSIRF

Pivoting off a known command-and-control domain identified by MSTIC, *acrobatrelay[.]com*, RiskIQ expanded the view of KNOTWEED’s attack infrastructure. Leveraging unique patterns in the use of SSL certificates and other network fingerprints specific to the group and associated with that domain, RiskIQ identified a host of additional IP addresses under the control of KNOTWEED. This infrastructure, largely hosted by Digital Ocean and Choopa, has been actively serving malware since at least February of 2020 and continues through the time of this writing.

RiskIQ next utilized passive DNS data to determine which domains those IPs resolved to at the time they were malicious. This process yielded several domains with direct links to DSIRF, including *demo3[.]dsirf[.]eu* (the company’s own website), and several subdomains that appear to have been used for malware development, including *debugmex[.]dsirflabs[.]eu* (likely a server used for debugging malware with the bespoke utility tool Mex) and *szstaging[.]dsirflabs[.]eu* (likely a server used to stage Subzero malware).

Detection and prevention

Microsoft will continue to monitor KNOTWEED activity and implement protections for our customers. The current detections and IOCs detailed below are in place and protecting Microsoft customers across our security products.

Additional advanced hunting queries are also provided below to help organizations extend their protections and investigations of these attacks.

Behaviors

Corelump drops the *Jumplump* loader DLLs to *C:\Windows\System32\spool\drivers\color*. This is a common directory used by malware as well as some legitimate programs, so writes of PE files to the folder should be monitored.

Jumplump uses COM hijacking for persistence, modifying COM registry keys to point to the *Jumplump* DLL in *C:\Windows\System32\spool\drivers\color*. Modifications of default system CLSID values should be monitored to detect this technique (e.g., *HKLM\SOFTWARE\Classes\CLSID\{GUID}\InProcServer32 Default* value). The five CLSIDs used by *Jumplump* are listed below with their original clean values on Windows 11:

- {ddc05a5a-351a-4e06-8eaf-54ec1bc2dcea} = "*%SystemRoot%\System32\ApplicationFrame.dll*"
- {1f486a52-3cb1-48fd-8f50-b8dc300d9f9d} = "*%SystemRoot%\system32\propsys.dll*"
- {4590f811-1d3a-11d0-891f-00aa004b2e24} = "*%SystemRoot%\system32\wbem\wbemprox.dll*"
- {4de225bf-cf59-4cfc-85f7-68b90f185355} = "*%SystemRoot%\system32\wbem\wmiprvsd.dll*"
- {F56F6FDD-AA9D-4618-A949-C1B91AF43B1A} = "*%SystemRoot%\System32\Actioncenter.dll*"

Many of the post-compromise actions can be detected based on their command lines. Customers should monitor for possible malicious activity such as PowerShell executing scripts from internet locations, modification of commonly abused registry keys such as *HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest,* and LSASS credential dumping via minidumps.

Recommended customer actions

The techniques used by the actor and described in the Observed actor activity section can be mitigated by adopting the security considerations provided below:

- All customers should prioritize patching of CVE-2022-22047.
- Confirm that Microsoft Defender Antivirus is updated to security intelligence update **1.371.503.0** or later to detect the related indicators.
- Use the included indicators of compromise to investigate whether they exist in your environment and assess for potential intrusion.
- Change Excel macro security settings to control which macros run and under what circumstances when you open a workbook. Customers can also stop malicious XLM or VBA macros by ensuring runtime macro scanning by Antimalware Scan Interface (AMSI) is on. This feature—enabled by default—is on if the Group Policy setting for Macro Run Time Scan Scope is set to "Enable for All Files" or "Enable for Low Trust Files".
- Enable multifactor authentication (MFA) to mitigate potentially compromised credentials and ensure that MFA is enforced for all remote connectivity. *Note:* Microsoft strongly encourages all customers download and use password-less solutions like Microsoft Authenticator to secure accounts.
- Review all authentication activity for remote access infrastructure, with a particular focus on accounts configured with single factor authentication, to confirm authenticity and investigate any anomalous activity.

Indicators of compromise (IOCs)

The following list provides IOCs observed during our investigation. We encourage our customers to investigate these indicators in their environments and implement detections and protections to identify past related activity and prevent future attacks against their systems. All sample hashes are available in VirusTotal.

Indicator	Type	Description
78c255a98003a101fa5ba3f49c50c6922b52ede601edac5db036ab72efc57629	SHA-256	Malicious Excel document and VBA
0588f61dc7e4b24554cffe4ea56d043d8f6139d2569bc180d4a77cf75b68792f	SHA-256	Malicious Excel document and VBA
441a3810b9e89bae12eea285a63f92e98181e9fb9efd6c57ef6d265435484964	SHA-256	Jumplump malware
cbae79f66f724e0fe1705d6b5db3cc8a4e89f6bdf4c37004aa1d45eeab26e84b	SHA-256	Jumplump malware
fd6515a71530b8329e2c0104d0866c5c6f87546d4b44cc17bbb03e64663b11fc	SHA-256	Jumplump malware
5d169e083faa73f2920c8593fb95f599dad93d34a6aa2b0f794be978e44c8206	SHA-256	Jumplump malware
7f29b69eb1af1cc6c1998bad980640bfe779525fd5bb775bc36a0ce3789a8bfc	SHA-256	Jumplump malware
02a59fe2c94151a08d75a692b550e66a8738eb47f0001234c600b562bf8c227d	SHA-256	Jumplump malware

Indicator	Type	Description
7f84bf6a016ca15e654fb5ebc36fd7407cb32c69a0335a32bfc36cb91e36184d	SHA-256	Jumplump malware
afab2e77dc14831f1719e746042063a8ec107de0e9730249d5681d07f598e5ec	SHA-256	Jumplump malware
894138dfeee756e366c65a197b4dbef8816406bc32697fac6621601debe17d53	SHA-256	Jumplump malware
4611340fdade4e36f074f75294194b64dcf2ec0db00f3d958956b4b0d6586431	SHA-256	Jumplump malware
c96ae21b4cf2e28eec222cfe6ca903c4767a068630a73eca58424f9a975c6b7d	SHA-256	Corelump malware
fa30be45c5c5a8f679b42ae85410f6099f66fe2b38eb7aa460bcc022babb41ca	SHA-256	Mex tool
e64bea4032cf2694e85ede1745811e7585d3580821a00ae1b9123bb3d2d442d6	SHA-256	Passlib tool
acrobatrelay[.]com	Domain	C2
finconsult[.]cc	Domain	C2
realmetaldns[.]com	Domain	C2

NOTE: These indicators should not be considered exhaustive for this observed activity.

Detections

Microsoft Defender Antivirus

Microsoft Defender Antivirus detects the malware tools and implants used by KNOTWEED starting with signature build **1.371.503.0** as the following family names:

- *Backdoor:O97M/JumplumpDropper*
- *Trojan:Win32/Jumplump*
- *Trojan:Win32/Corelump*
- *HackTool:Win32/Mexlib*
- *Trojan:Win32/Medcerc*
- *Behavior:Win32/SuspModuleLoad*

Microsoft Defender for Endpoint

Microsoft Defender for Endpoint customers may see the following alerts as an indication of a possible attack. These alerts are not necessarily an indication of KNOTWEED compromise:

- *COM Hijacking* – Detects multiple behaviors, including *JumpLump* malware persistence techniques.
- *Possible privilege escalation using CTF module* – Detects a possible privilege escalation behavior associated with CVE-2022-2204; also detects an attempt to perform local privilege escalation by launching an elevated process and loading an untrusted module to perform malicious activities
- *KNOTWEED actor activity detected* – Detects KNOTWEED actor activities
- *WDigest configuration change* – Detects potential retrieval of clear text password from changes to *UseLogonCredential* registry key
- *Sensitive credential memory read* – Detects LSASS credential dumping via minidumps
- *Suspicious Curl behavior* – Detects the use of Curl to download KNOTWEED tooling from public file shares
- *Suspicious screen capture activity* – Detects *Corelump* behavior of capturing screenshots of the compromised system

Hunting queries

Microsoft Sentinel

The following resources are available to Microsoft Sentinel customers to identify the activity outlined in the blog post.

Microsoft Defender Antivirus detections related to KNOTWEED

This query identifies occurrences of Microsoft Defender Antivirus detections listed in this blog post:

https://github.com/Azure/Azure-Sentinel/blob/master/Detections/MultipleDataSources/KNOTWEEDAVDetection.yaml

File hash IOCs related to KNOTWEED

This query identifies matches based on file hash IOCs related to KNOTWEED across a range of common Microsoft Sentinel data sets:

https://github.com/Azure/Azure-Sentinel/blob/master/Detections/MultipleDataSources/KNOTWEEDFileHashesJuly2022.yaml

Domain IOCs related to KNOTWEED

This query identifies matches based on domain IOCs related to KNOTWEED across a range of common Microsoft Sentinel data sets:

https://github.com/Azure/Azure-Sentinel/blob/master/Detections/MultipleDataSources/KNOTWEEDC2DomainsJuly2022.yaml

COM registry key modified to point to Color Profile folder

This query identifies modifications to COM registry keys to point to executable files in *C:\Windows\System32\spool\drivers\color*:

https://github.com/Azure/Azure-Sentinel/blob/master/Detections/MultipleDataSources/COMRegistryKeyModifiedtoPointtoFileinColorDrivers.yaml

PE file dropped in Color Profile folder

This query looks for PE files being created in the *C:\Windows\System32\spool\drivers\color* folder:

https://github.com/Azure/Azure-Sentinel/blob/master/Detections/DeviceFileEvents/PEfiledroppedinColorDriversFolder.yaml

Abnormally large JPEG downloaded from new source

This query looks for downloads of JPEG files from remote sources, where the file size is abnormally large, and not from a common source:

https://github.com/Azure/Azure-Sentinel/blob/master/Hunting%20Queries/CommonSecurityLog/AbnormallyLargeJPEGFiledDownloadedfromNewSource.yaml

Downloading new file using Curl

This query looks for new files being downloaded using Curl.

https://github.com/Azure/Azure-Sentinel/blob/master/Hunting%20Queries/MultipleDataSources/DownloadofNewFileUsingCurl.yaml

Suspected credential dumping

This query looks for attackers using comsvcs.dll to dump credentials from memory

https://github.com/Azure/Azure-Sentinel/blob/master/Hunting%20Queries/SecurityEvent/SuspectedLSASSDump.yaml

Downgrade to plaintext credentials

This query looks for registry key being set to enabled plain text credentials

https://github.com/Azure/Azure-Sentinel/blob/master/Detections/SecurityEvent/WDigestDowngradeAttack.yaml

Microsoft 365 Defender advanced hunting

Microsoft 365 Defender customers can run the following advanced hunting queries to locate IOCs and related malicious activity in their environments.

Microsoft Defender Antivirus detections related to KNOTWEED

This query identifies detection of related malware and tools by Microsoft Defender Antivirus:

https://github.com/Azure/Azure-Sentinel/blob/master/Hunting%20Queries/Microsoft%20365%20Defender/Campaigns/KNOTWEED/KNOTWEED-AVDetections.yaml

File hash IOCs related to KNOTWEED

This query surfaces KNOTWEED file hash IOCs across Microsoft Defender for Endpoint tables:

https://github.com/Azure/Azure-Sentinel/blob/master/Hunting%20Queries/Microsoft%20365%20Defender/Campaigns/KNOTWEED/KNOTWEED-FileHashIOCsJuly2022.yaml

Domain IOCs related to KNOTWEED

This query identifies matches based on domain IOCs related to KNOTWEED against Microsoft Defender for Endpoint device network connections:

https://github.com/Azure/Azure-Sentinel/blob/master/Hunting%20Queries/Microsoft%20365%20Defender/Campaigns/KNOTWEED/KNOTWEED-

DomainIOCsJuly2022.yaml

COM registry key modified to point to Color Profile folder

This query identifies modifications to COM registry keys to point to executable files in *C:\Windows\System32\spool\drivers\color*:

https://github.com/Azure/Azure-Sentinel/blob/master/Hunting%20Queries/Microsoft%20365%20Defender/Campaigns/KNOTWEED/KNOTWEED-COMRegistryKeyModifiedtoPointtoColorProfileFolder.yaml

PE file dropped in Color Profile folder

This query looks for PE files being created in the *C:\Windows\System32\spool\drivers\color\ folder*:

https://github.com/Azure/Azure-Sentinel/blob/master/Hunting%20Queries/Microsoft%20365%20Defender/Campaigns/KNOTWEED/KNOTWEED-PEFileDroppedinColorProfileFolder.yaml

Downloading new file using Curl

This query looks for new files being downloaded using Curl.

https://github.com/Azure/Azure-Sentinel/blob/master/Hunting%20Queries/Microsoft%20365%20Defender/Campaigns/KNOTWEED/KNOTWEED-DownloadingnewfileusingCurl.yaml