Notorious SideCopy APT group sets sights on India's DRDO

: 3/21/2023

Threat Actors Use DLL Sideloading to Fly Under the Radar

SideCopy APT is a Threat Actor(TA) from Pakistan that has been active since 2019, focusing on targeting South Asian nations, especially India and Afghanistan. The SideCopy APT gets its name from the infection chain, which imitates that of the SideWinder APT. Some reports suggest that this actor shares characteristics with Transparent Tribe (APT36) and could potentially be a sub-group of that threat actor.

Recently, Cyble Research and Intelligence Labs (CRIL) came across a Twitter post of an ongoing campaign by SideCopy APT against the "Defence Research and Development Organisation" of the Indian government.

DRDO is a government agency tasked with researching and developing advanced technologies for use by the Indian Armed Forces. Its focus includes creating cutting-edge defense systems such as missiles, radars, electronic warfare and communication systems, naval and aerospace systems. The agency plays a significant role in India's defense industry, contributing to the country's military strength and self-sufficiency in defense technology.

The initial infection starts with a spam email containing the link to the malicious file hosted on the compromised website. The link allows users to download a ZIP file containing a LNK file named "DRDO – K4 Missile Clean room.pptx.lnk" from the below URL:

- *hxxps[:]//www[.]cornerstonebeverly[.]org/js/files/DRDO-K4-Missile-Clean-room[.]zip*

The delivery mechanism of the SideCopy APT attack via a spam email is illustrated in the figure below.

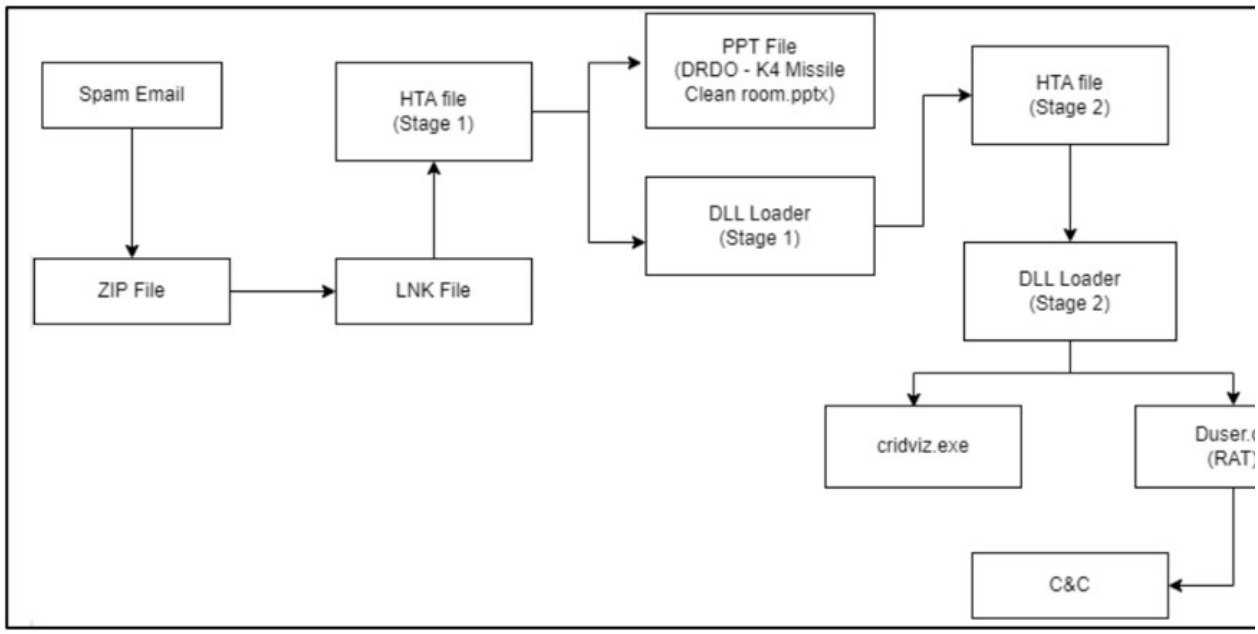

Figure 1 – Infection chain

Initial Infection

The infection process begins with the user extracting a zip file and then running the .lnk file on their machine.

Once the .lnk file is executed, it triggers a command that launches “mshta.exe” to connect to a specific URL, shown in the figure below.

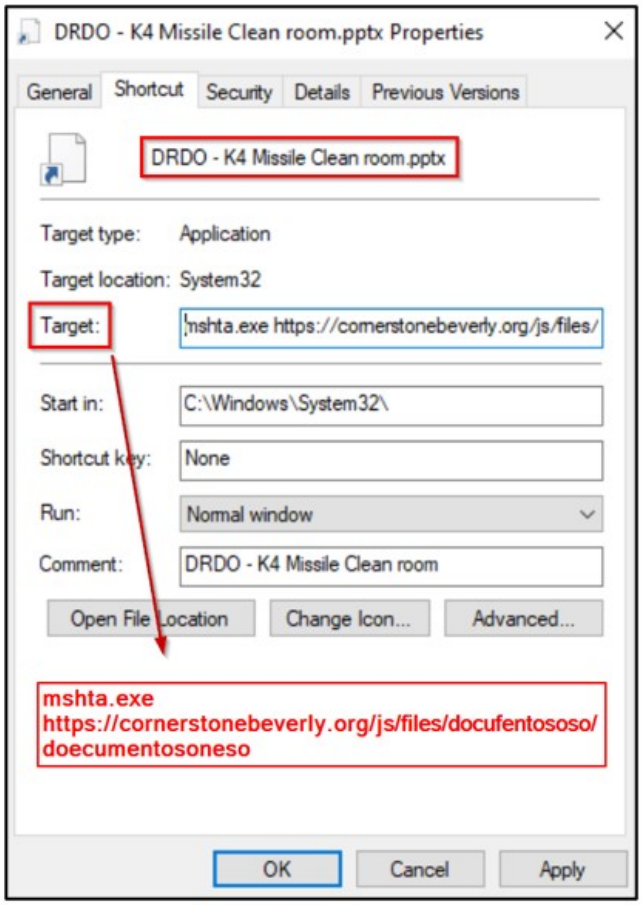

Figure 2 – Target command to launch MSHTA

After redirection, the URL eventually establishes a connection with the following URL:

- *hxxps[:]//www[.]cornerstonebeverly[.]org/js/files/docufentososo/doecumentosoneso/pantomime[.]hta*

Subsequently, the hta file is downloaded and executed in the path mentioned below:

- *c:\users\<Admin>\appdata\local\microsoft\windows\temporary internet files\content.ie5\nxzxrd2m\pantomime.hta*

The figure below displays a code snippet from the “pantomime.hta” file, including the compressed Microsoft PowerPoint file encoded in Base64 format.

Figure 3 – Code snippet of pantomime.hta file

After execution, the hta file decodes and decompresses the PPT file encoded in Base64 format. Consequently, it saves the decompressed Microsoft PowerPoint file in the “%temp%” folder under the name “DRDO – K4 Missile Clean room.pptx” and launches it, as shown in Figure 4. The TAs are enticing users with a DRDO PowerPoint document and covertly engaging in malicious activities in the background through the “pantomime.hta” file.

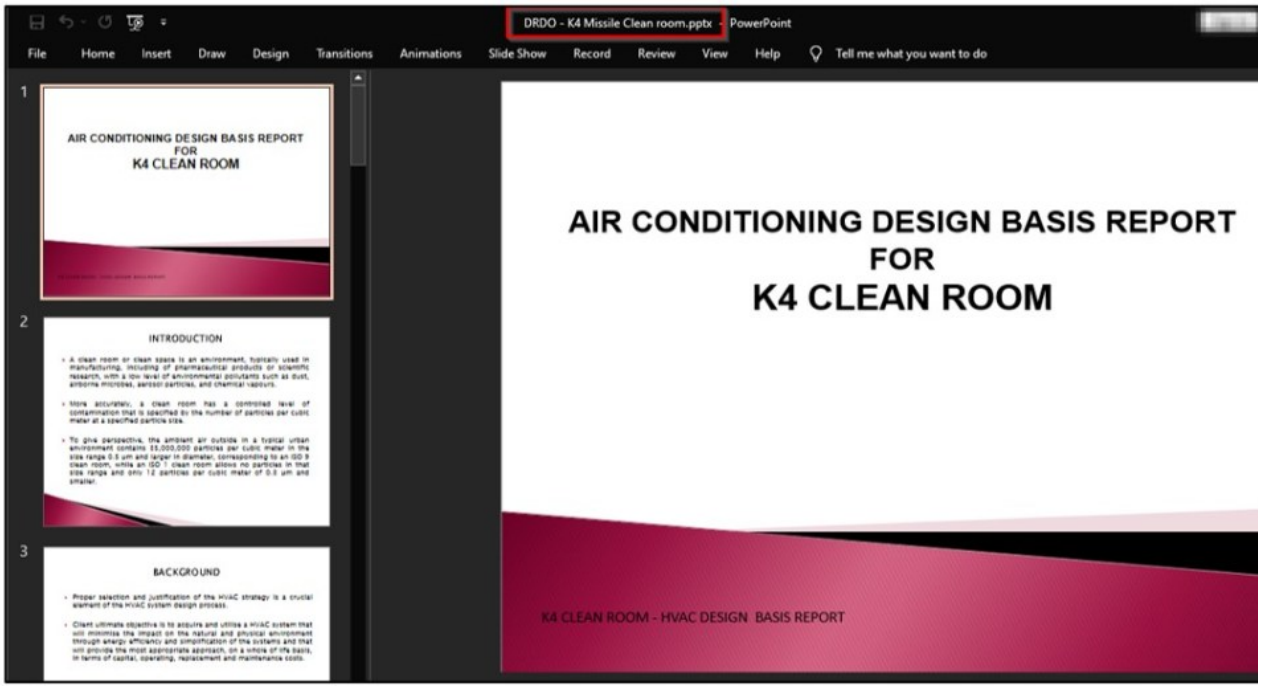

Figure 4 – DRDO – K4 Missile Clean room MS PowerPoint slides

The hta file, aside from dropping the PPT file, carries out a concatenation operation and decodes the Base64-encoded content of the DLL file named, “hta.dll”. When the decoding is complete, the DLL file is loaded into memory and triggered using the *DynamicInvoke* method. This method creates an instance of a class called “WorkInProgress”.

Upon execution, the “hta.dll” file drops another .hta file named “jquery.hta” under the directory “C:\ProgramData\HP” and executes it through “mshta.exe”.

When executed, the “jquery.hta” file carries out the concatenation operation and decodes the Base64-encoded content of the loader DLL file named “PreBotHta.dll”, as it did before for “hta.dll”. Once decoded, the “PreBotHta.dll” file is loaded into the memory and invoked using the *DynamicInvoke* method. This method creates an instance of a class called “DraftingPad.”

It also uses a WMI query, specifically “Select * From AntiVirus,” to gather the names of installed antivirus products.

The below figure shows the code snippet of “jquery.hta” file.

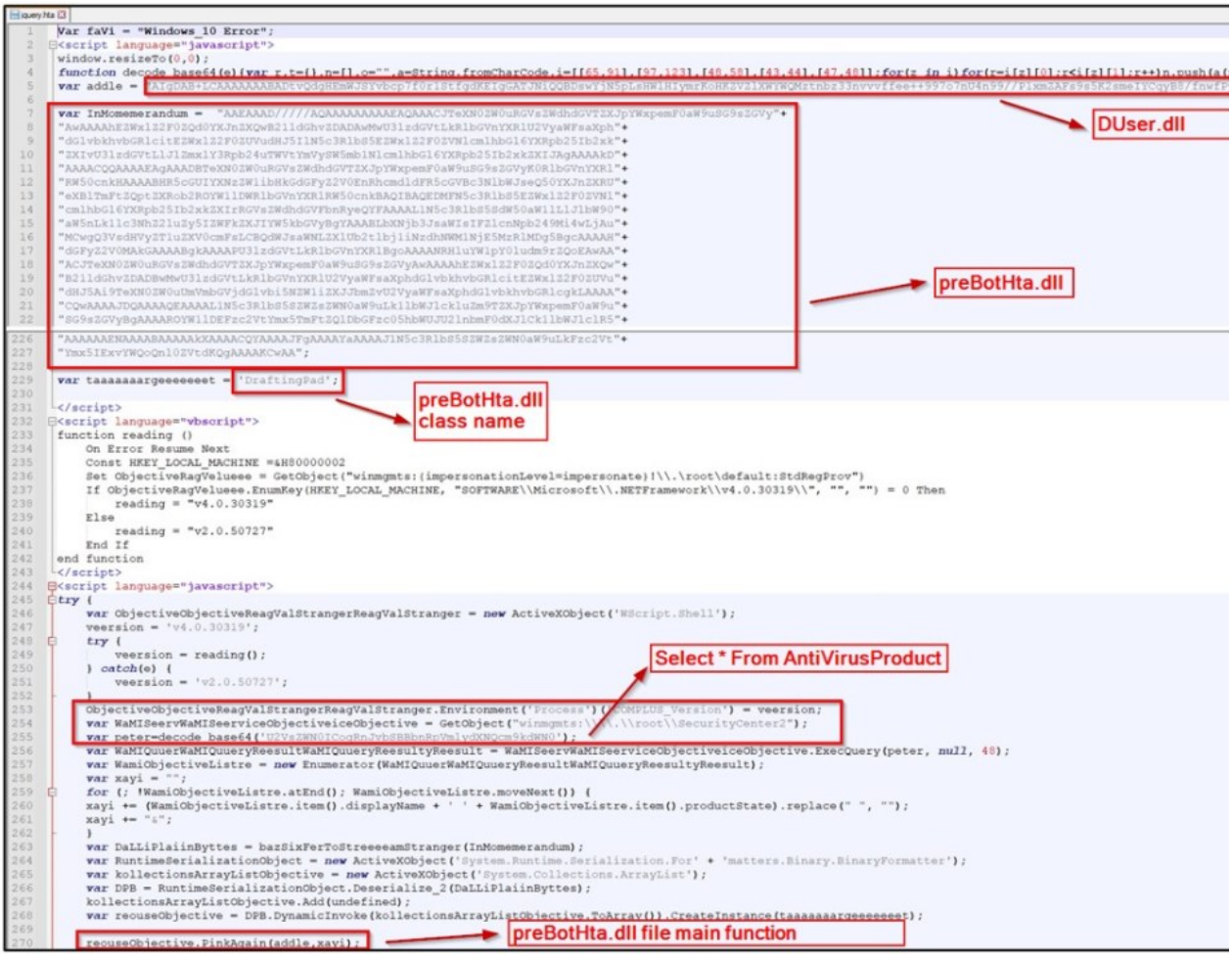

Figure 5 – Code snippet of jquery.hta file

Finally, the “jquery.hta” file executes the *PinkAgain()* function of the loader “PreBotHta.dll” file, passing AntiVirus names and a Base64 encoded payload called “DUser.dll” as arguments.

The below figure shows the code snippet of the loaded “PreBotHta.dll” file.

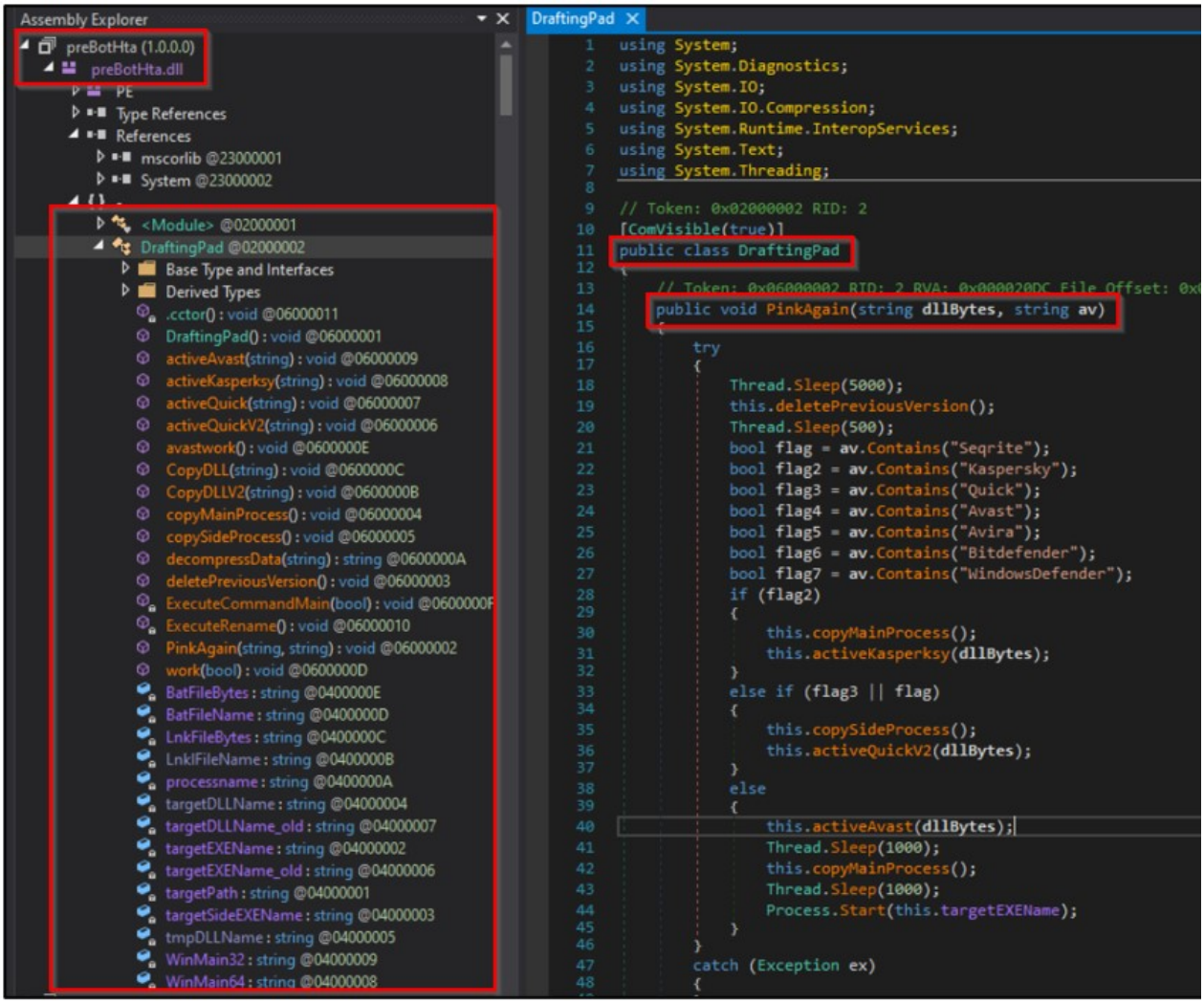

Figure 6 – Loaded PreBotHta.dll file in memory

DLL SideLoading

The PinkAgain() function has code to copy the legitimate and essential “credwiz.exe” file, which is a part of the Windows operating system, and copies it to the following location as “cridviz.exe”. The legitimate file “credwiz.exe” is primarily used to create and restore Windows user account credentials backups. Typically, it loads a legitimate file named “Duser.dll.”

However, in this case, the malware takes Base64 encoded argument, decodes it, and saves it as “Duser.dll” in the location where “cridviz.exe” was dropped previously. The dropped malicious file “Duser.dll” is a variant of the Action Rat Malware family responsible for performing malicious activities in the victim’s machine. During its execution, the loader drops both files in the below directory.

- C:\\Users\\Public\\hp\\cridviz.exe
- C:\\Users\\Public\\hp\\DUser.dll

Furthermore, the loader utilizes various directories to drop the files “credwiz.exe” and “DUser.dll” using different names based on the type of AntiVirus software installed on the victim’s machine. TAs commonly use the tactic to increase the effectiveness of their attacks and avoid detection by security software.

The specific directories and filenames used by the loader, as indicated below.

- C:\\Users\\Public\\hp\\rekeywiz.exe
- C:\\Users\\Public\\hp\\rech.dat
- C:\\ProgramData\\Intel\\cridviz.exe
- C:\\ProgramData\\Intel\\DUser.dll

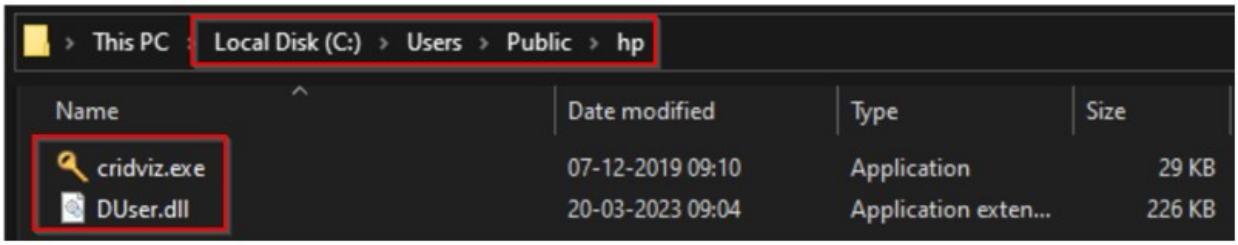

Figure 7 – Files dropped by PreBotHta.dll

Once the necessary files have been dropped onto the victim's system, the "cridviz.exe" process is initiated, which then proceeds to sideload the malicious payload "Duser.dll", as shown in the figure below.

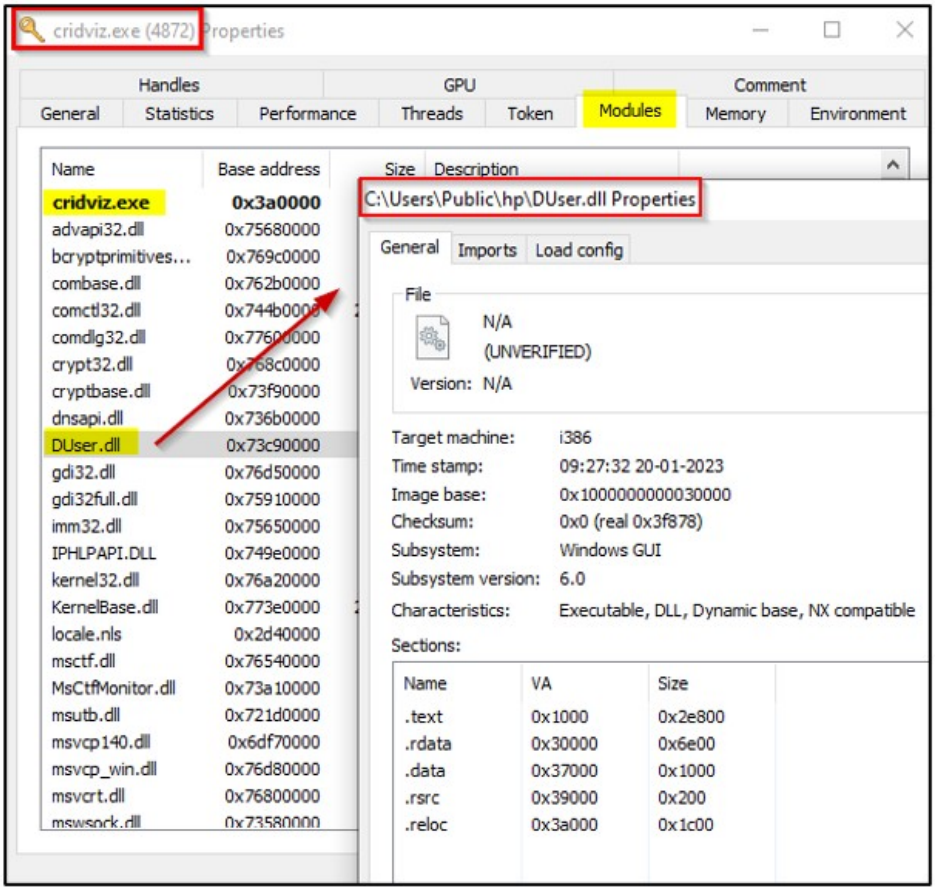

Figure 8 – cridviz.exe side loading DUser.dll

Action RAT Payload

To begin its malicious operation, the RAT first gathers information about the victim's machine, such as its hostname, username, operating system version, and installed antivirus products. This data is then transmitted to the Command-and-Control(C&C) server via HTTP request, as below.

- *hxxp[:]//144[.]91[.]72[.]17:8080/streamcmd?AV=[Redacted]&OS=[Redacted]&Vesrion=[Redacted]&detail=[Redacted]*

Afterward, the malicious process enters a loop and remains idle until it receives commands from the server, which it executes. The RAT possesses the ability to perform any of the following operations upon receiving commands from the C&C:

- Execute: Carry out commands sent from the server
- Download: Retrieve and install additional payloads
- Drives: Obtain information about the available drives
- GetFiles: Retrieve information about specific files
- Execute: Launch a designated payload using *CreateProcessW()*
- Upload: Transmit files to the server

In addition, the loader DLL was utilized to deploy a recently developed information-stealing malware called AuTo Stealer. This malware can gather PDF documents, Office/text/database files, and images and transmit the stolen information via HTTP or TCP.

Persistence

This loader DLL file also drops a batch file named “test.bat” in the %temp% directory, which creates an auto startup entry for the “cridviz.exe” file using the “reg.exe” utility, as shown in the figure below.

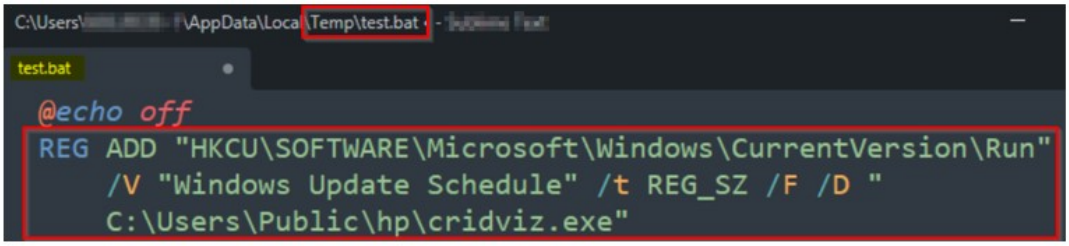

Figure 9 – Run entry for Persistence

Conclusion

SideCopy is an APT group that emulates the tactics of the Sidewinder APT to distribute its own malware. Its attack patterns typically involve the use of malicious LNK files to initiate a complex chain of infection using multiple HTAs and loader DLLs, ultimately leading to the deployment of final payloads. This group has been observed to target government and military officials in India and Afghanistan specifically. The APT group continuously evolves its techniques while incorporating new tools into its arsenal.

CRIL continues to monitor the most recent APT attacks, phishing attacks, or malware strains in circulation and regularly publishes informative blog posts with practical insights to help protect users from these well-known attacks.

Our Recommendations

We have listed some essential cybersecurity best practices that create the first line of control against attackers. We recommend that our readers follow the best practices as mentioned below:

- Avoid downloading pirated software from warez/torrent websites. The “Hack Tool” present on sites such as YouTube, torrent sites, etc., mainly contains such malware.
- Use strong passwords and enforce multi-factor authentication wherever possible.
- Turn on the automatic software update feature on your computer, mobile, and other connected devices.
- Use a reputed antivirus and internet security software package on your connected devices, including PC, laptop, and mobile.
- Refrain from opening untrusted links and email attachments without first verifying their authenticity.
- Educate employees on protecting themselves from threats like phishing/untrusted URLs.
- Block URLs that could be used to spread the malware, e.g., Torrent/Warez.
- Monitor the beacon on the network level to block data exfiltration by malware or TAs.
- Enable Data Loss Prevention (DLP) Solutions on the employees’ systems.

MITRE ATT&CK® Techniques

Tactic	Technique ID	Technique Name
Initial Access	T1566	Spearphishing Attachment
Execution	T1204	User Execution
	T1047	Windows Management Instrumentation
	T1170	Mshta
	T1129	Shared Modules
Defense Evasion	T1036	Masquerading
	T1218	System Binary Proxy Execution
Persistence	T1547	Registry Run Keys / Startup Folder
Discovery	T1016	System Network Configuration
	T1057	Discovery Process Discovery
Collection	T1185	Browser Session Hijacking

Command and Control	T1071	Application Layer Protocol
	T1105	Ingress Tool Transfer

Indicators Of Compromise

Indicators	Indicator type	Descr
0725318b4f5c312eeaf5ec9795a7e919 9902348fc5dffe10a94a3f4be219dc42330ed480 9aed0c5a047959ef38ec0555ccb647688c67557a6f8f60f691ab0ec096833cce	MD5 SHA1 SHA256	DRDC Missil room.:
ab11b91f97d7672da1c5b42c9ecc6d2e feeadc91373732d65883c8351a6454a77a063ff5 a2e55cbd385971904abf619404be7ee8078ce9e3e46226d4d86d96ff31f6bb9a	MD5 SHA1 SHA256	DRDC Missil room.
cbaa7fc86e4f1a30a155f60323fdb72a d7dcea1c35475caa85e9298e44b63d3ce43fb2f0 e88835e21c431d00a9b465d2e8bed746b6369892e33be10bc7ebbda6e8185819	MD5 SHA1 SHA256	panto (Stage
036da574b5967c71951f4e14d000398c e612dbb34e01b41e46359019db9340e17e0390b8 85faf414ed0ba9c58b9e7d4dc7388ba5597598c93b701d367d8382717fb485ec	MD5 SHA1 SHA256	jquery (Stage
2e19b7a2bbdc8082024d259e27e86911 3c4c8cbab1983c775e6a76166f7b3c84dde8c8c5 865e041b41b9c370a4eed91a9a407bd44a94e16e236e07be05e87de319a4486c	MD5 SHA1 SHA256	DUser (Actio
hxxps[:]//www[.]cornerstonebeverly[.]org/js/files/DRDO-K4-Missile-Clean-room[.]zip	URL	Malici ZIP fil downl
hxxps[:]//www[.]cornerstonebeverly[.]org/js/files/docufentososo/doecumentosoneso	URL	Target comm URL i file
hxxps[:]//www[.]cornerstonebeverly[.]org/js/files/docufentososo/doecumentosoneso/pantomime.hta	URL	Redire downl HTA fi
144[.]91[.]72[.]17:8080	IP:Port	C&C