Double Action, Triple Infection, and a New RAT: SideCopy’s Persistent Targeting of Indian Defence

seqrite.com/blog/double-action-triple-infection-and-a-new-rat-sidecopys-persistent-targeting-of-indian-defence

Sathwik Ram Prakki

June 15, 2023

15 June 2023

Written by Sathwik Ram Prakki

APT, Government, Malware

Estimated reading time: 4 minutes

Overview

A new attack campaign of SideCopy APT has been discovered targeting the Indian Defence sector. The group utilizes phishing email attachments & URLs as the infection vector to download malicious archive files leading to the deployment of two different Action RAT payloads and a new .NET-based RAT. There are three infection chains with themes utilized: DRDO’s “Invitation Performa,” which is part of its Defence Procurement Procedure (DPP), a honeytrap lure, and also the Indian Military with “Selection of Officers for Foreign Assignments” theme.

The ongoing campaign came to light after a senior DRDO scientist was arrested for leaking sensitive information to Pakistani agents who honey trapped him. “Honey Trap” has increased significantly on social media platforms like Facebook, Twitter, WhatsApp, etc., with millions of illegitimate accounts used as bots or baits.

Similarly, in March 2023, the same infection chain was utilized targeting DRDO, with the decoy theme being “HVAC Air Conditioning Design Basis Report” for its K4 Missile Clean Room. Another theme used in the same month was “Advisory on Grant of Risk & Hardship Allowance JCOs & ORs.” Even in April, they targeted Defence Ministry with the theme “Saudi Arabia Delegation with Indian Armed Forces Medical Officials.”

SideCopy has been known for persistently targeting Indian Defence (Military and Armed Forces) since its discovery in 2019.

Key Findings

- Three infection chains lead to the same payloads hosted on the domain elfinindia[.]com.
- The infection chain is shown below, where an archive file contains a malicious shortcut (LNK) file masqueraded as DOCX, PNG, and PDF, respectively. The LNK files trigger MSHTA to execute remote HTA files on this domain.

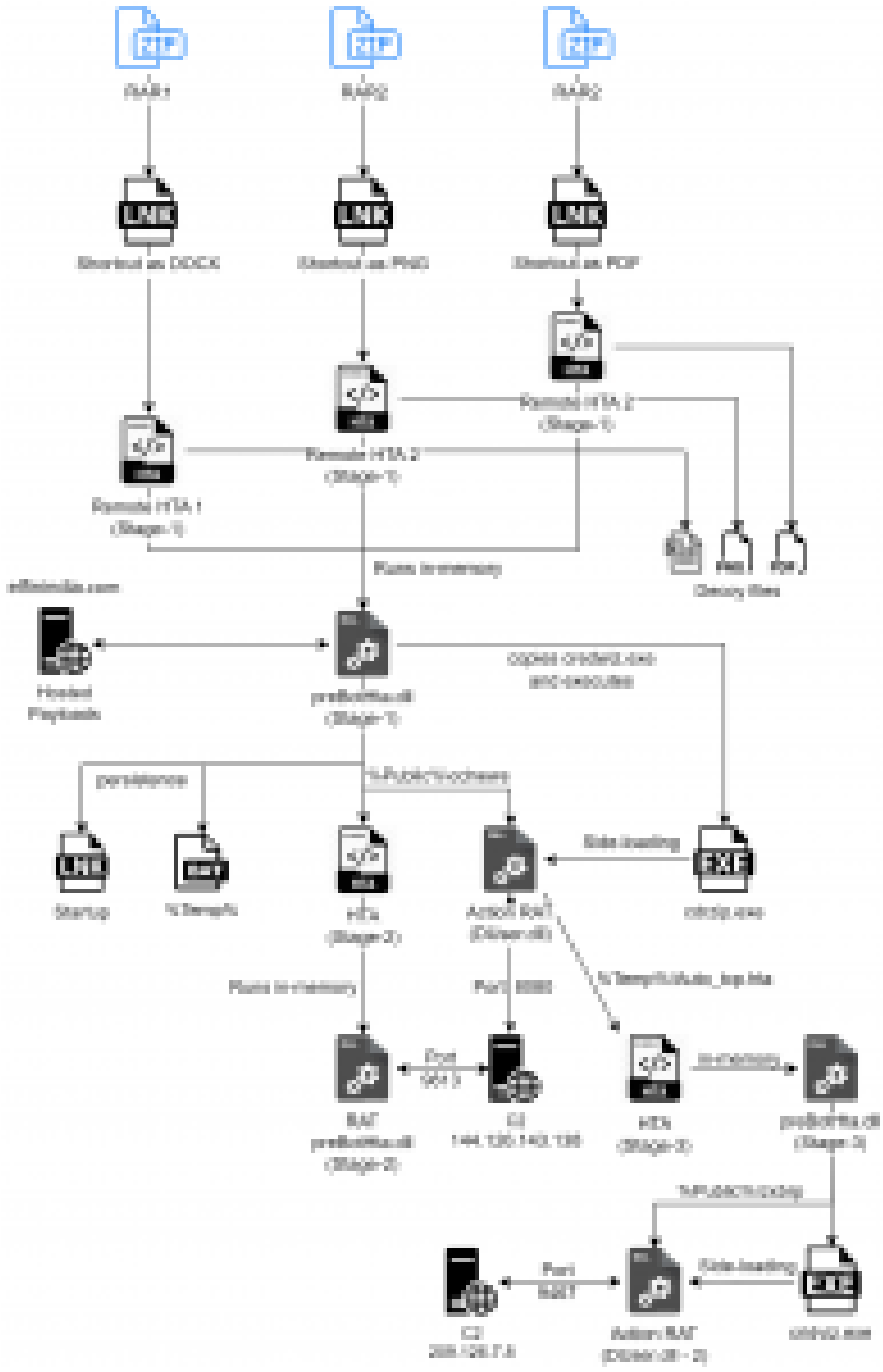

Fig. 1 – Infection Process

- The deployment of two variants of Action RAT and a new .NET-based RAT that supports 18 C2 commands has been observed.

- Action RAT downloads and executes a larger variant that exfiltrates all documents and images inside the Desktop, Documents, and Download directories. The legitimate ‘credwiz.exe’ file is utilized to sideload both the RATs.
- C2 infra has a known hostname commonly found, and all the TTPs directly point to SideCopy’s known infection throughout the years.

Summary

This year, SideCopy has been actively targeting India, especially the defence sector. The same attack chain targets victims in spear-phishing campaigns and honeytrap lures. As Pakistani agents have increasingly used honey traps to lure defence personnel, one can only anticipate the magnitude of damage it can cause. Hence, it is imperative to take the necessary steps to end it. Pakistan and many other threat actors around the globe are using honeytraps, with recent cases found stealing intelligence in this form of cyber espionage. An in-depth analysis of the latest infection chain and a comparison with previous variants can be found in our whitepaper.

IOC

Archive	
05eb7152bc79936bea431a4d8c97fb7b	Personal.zip
4c926c0081f7d2bf6fc718e1969b05be	Performa’s feedback.zip
db49c75c40951617c4025678eb0abe90	Asigma dated 22 May 23.zip
LNK	
1afc64e248b3e6e675fa31d516f0ee63	pessonal pic.png.lnk
49f3f2e28b9e284b4898fafa452322c0	Performa’s feedback.docx.lnk
becbf20da475d21e2eba3b1fe48148eb	Asigma dated 22 May 23 .pdf.lnk
HTA	
FCD0CD0E8F9E837CE40846457815CFC9	xml.hta
BEC31F7EDC2032CF1B25EB19AAE23032	d.hta (Chain-1)
C808F7C2C8B88C92ABF095F10AFAE803	d.hta (Chain-2)

4559EF3F2D05AA31F017C02ABBE46FCB	d.hta (Chain-3)
F20267EC56D865008BA073DB494DB05E	Auto_tcp.hta
4F8D22C965DFB1A6A19B8DB202A24717	Auto_tcp.hta
DLL	
86D4046E17D7191F7198D506F06B7854	preBotHta.dll (Stage-1)
28B35C143CF63CA2939FB62229D31D71	preBotHta.dll (Stage-2) (New RAT)
582C0913E00C0D95B5541F4F79F6EDD5	preBotHta.dll (Stage-3)
8f670928bc503b6db60fb8f12e22916e	DUser.dll (Action RAT)
13D4E8754FEF340CF3CF4F5A68AC9CDD	DUser.dll (Action RAT)
5D5B1AFF4CBE03602DF102DF8262F565	DUser.dll (Action RAT)
BAT	
D95A685F12B39484D64C58EB9867E751	test.bat
BDA677D18E98D141BAB6C7BABD5ABD2B	test.bat
Others	
5580052F2109E9A56A77A83587D7D6E2	d.txt
E5D3F3D0F26A9596DA76D7F2463E611B	h.txt
Domain	
elfinindia[.]com	Hosted Malicious files
IP	

144.126.143[.]138:8080 144.126.143[.]138:9813 66.219.22[.]252:9467 209.126.7[.]8:9467	C2
URL	
hxxps://elfinindia[.]com/wp-includes/files/	
hxxps://elfinindia[.]com/wp-includes/files/pictures/personal/Personal.zip	
hxxps://elfinindia[.]com/wp-includes/files/pictures/man/d.hta	
hxxps://elfinindia[.]com/wp-includes/files/man/d.hta	
hxxps://elfinindia[.]com/wp-includes/files/fa/d.hta	
hxxps://elfinindia[.]com/wp-includes/files/oth/hl/h.txt	
hxxps://elfinindia[.]com/wp-includes/files/oth/dl/d.txt	
hxxps://elfinindia[.]com/wp-includes/files/oth/av/	
PDB	
E:\Packers\CyberLink\Latest Source\Multithread Protocol Architecture\side projects\First Stage\HTTP Arsenal Main\Clinet\app\Release\app.pdb	
EXE (Legitimate)	
9B726550E4C82BBEB045150E75FEE720	cdrzip.exe / cridviz.exe
Decoy Files	
C5C2D8EB9F359E33C4F487F0D938C90C	Invitation Performa vis a vis feedback.docx
2461F858671CBFFDF9088FA7E955F400	myPic.jpeg
D77C15419409B315AC4E1CFAF9A02C87	2696 – 22 May 23.pdf

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.