AllaKore(d) the SideCopy Train

team-cymru.com/post/allakore-d-the-sidecopy-train

S2 Research Team

April 19, 2023

Identifying Connected Infrastructure and Management Activities

Introduction

This blog post seeks to build on recent public reporting on campaigns attributed to SideCopy, a Pakistani-linked threat group. SideCopy has been active since 2019, primarily targeting South Asian countries, with a focus on India and Afghanistan. The group's name comes from its use of an infection chain that mimics that of SideWinder APT, an Indian-linked threat group.

The distinction between SideWinder and SideCopy was first made by security researcher @Sebdraven and is documented here.

Some reports suggest that SideCopy may be a subdivision of Transparent Tribe (APT36), with similar tactics and techniques observed.

The S2 Research Team has blogged previously on the activities of Transparent Tribe:

- Transparent Tribe APT Infrastructure Mapping - Part One
- Transparent Tribe APT Infrastructure Mapping - Part Two

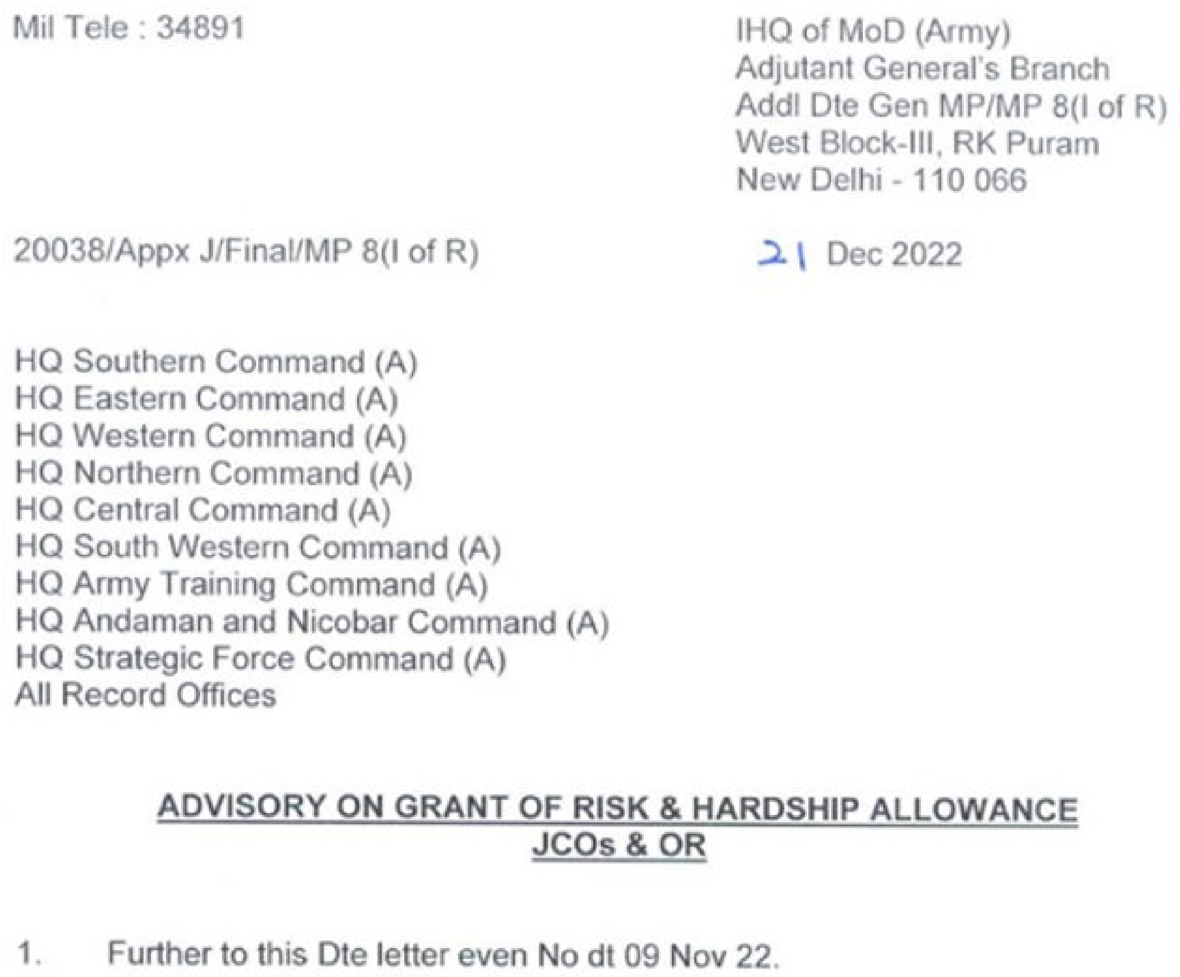
In this post we share the discoveries of our S2 Threat Research Team after examining analysis by the Chinese cyber security company QiAnXin, published on 20 March 2023, which detailed a SideCopy attack chain used to deploy AllaKore RAT. AllaKore RAT is an open-source remote access tool which has been modified for the purposes of SideCopy operations, and is commonly observed in their intrusions.

Key Findings

- Identification of additional malware samples and C2 infrastructure associated with SideCopy targeting of the Indian Ministry of Defense
- Evidence of management activity sourced from mobile IPs located in Pakistan, centered around a key IP address (**66.219.22.252**) connected to SideCopy's use of Action RAT
- Further credence provided to the assessment that SideCopy is a Pakistani-linked threat actor group, involved state-level espionage activities

India in the Crosshairs

As discussed in the analysis by QiAnXin, spear phishing was used as the initial delivery method for this campaign. Examining the lures involved, the targets appear to be users in India, specifically in the Ministry of Defence.



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)

21 Dec 2022

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.

Figure 1: Example PDF Lure (https://twitter.com/jaydinbas/status/1629149627848044550)

In a bid to further understanding of this campaign, we will not seek to repeat analysis of the infection chain. Instead we will focus on the two tools which were ultimately dropped, examining threat telemetry surrounding their associated command and control (C2) infrastructure.

DUser.dll (Action RAT)

The first tool, identified as Action RAT in analysis by Cyble, is dropped onto the victim machine alongside a benign executable which is used to sideload it, in order to avoid detection. Action RAT's capabilities include the ability to receive commands from the C2 server, to retrieve information from the victim machine, to execute further payloads, and to upload information back to the C2.

We found two samples of Action RAT (loaded as DUser.dll), including the sample analyzed by Cyble.

> **Cyble Sample Stage 1:** feeadc91373732d65883c8351a6454a77a063ff5 (DRDO - K4 Missile Clean room.pptx.lnk) **C2:** www.cornerstonebeverly[.]org **Action RAT:** 3c4c8cbab1983c775e6a76166f7b3c84dde8c8c5 (DUser.dll) **C2:** 144.91.72.17:8080 (Contabo GmbH)

> **Sample Two Stage 1:** 0d68a135b1f4be18481cf44ed02bcbf82aeb542e (Cyber Advisory - Profiles (Pic and Mob No) of PIOs.docx.lnk) **C2:** www.kwalityproducts[.]com **Action RAT:** cb031561fd76643885671922db7d5b840060334d (DUser.dll) **C2:** 84.46.250.78:8080 (Contabo GmbH)

Examining threat telemetry for the two C2 IPs **144.91.72.17** and **84.46.250.78** we observed initial victim connections on 06 February 2023 and 15 March 2023 respectively.

In total we observed 18 distinct victims, all located in India, connecting to the C2 servers - highlighting the targeted nature of the campaign.

Further to this activity we also observed 37 distinct IPs (again all located in India) connecting to **144.91.72.17**:9468 in activity which commenced on 07 January 2023. Of the 37 IPs, two were observed connecting to the Action RAT port (TCP/8080).

We were unable to identify a sample talking to TCP/9468 of **144.91.72.17**, however we would hypothesize that this IP was used for C2 communications with another tool associated with SideCopy activities.

Management Hints?

Examining outbound activity from **144.91.72.17** and **84.46.250.78**, we observed connections from **84.46.250.78** to **66.219.22.252**:82 (IMMEDION, US). Whilst **66.219.22.252** is assigned to an American provider, WHOIS data places it in Pakistan.

Further examining connections to **66.219.22.252**:82, we observed communications sourced from 17 distinct IPs assigned to Pakistani mobile providers and four Proton VPN nodes during the period of interest.

All of the Proton VPN nodes and all but three of the Pakistani mobile IPs were also observed connecting to **66.219.22.252**:3389 within the same time period. Port 3389 (RDP) is often observed open on SideCopy (and Transparent Tribe) C2 servers, and is believed to be utilized for management purposes by the threat actors.

*These findings are therefore indicative of management of **66.219.22.252** by actors likely located in Pakistan, in addition to actors unknown accessing via Proton VPN infrastructure.*

Examining the communications sourced from the Pakistani mobile IPs, to **66.219.22.252**:82 and **66.219.22.252**:3389, we can start to build a general pattern of life, illustrated in Figure 2 below.

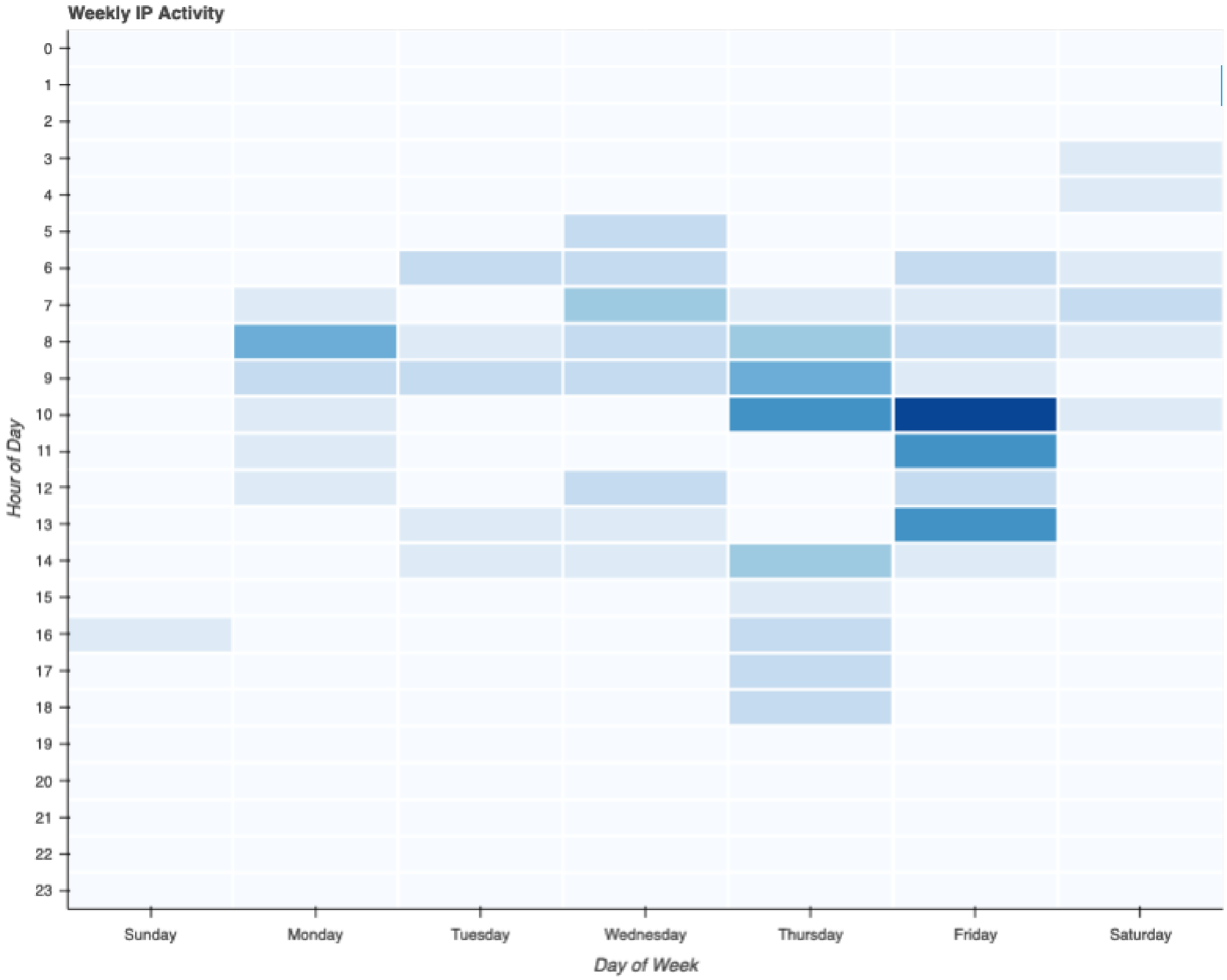


Figure 2: Pattern of Life for Management of 66.219.22.252

The timings in Figure 2 shown above are based on UTC, which is 5 hours behind Pakistan Standard Time. Therefore, Figure 2 demonstrates that management of **66.219.22.252** occurs between Monday to Saturday, from roughly 10AM to 7PM - with some exceptions on Thursdays.

These data points are potentially indicative of the threat actors accessing their infrastructure within a typical working week cadence, suggesting that management is undertaken professionally.

Finally, when analyzing threat telemetry data for **66.219.22.252**, we also observed inbound connections to TCP/8080 and TCP/9467 sourced from IP addresses assigned to Indian providers. TCP/9467 is noteworthy given its similarity to the activity observed on

144.91.72.17:9468 which we assess to be indicative of SideCopy C2 communications.

The findings in this section derived from threat telemetry data are summarized below in Figure 2.

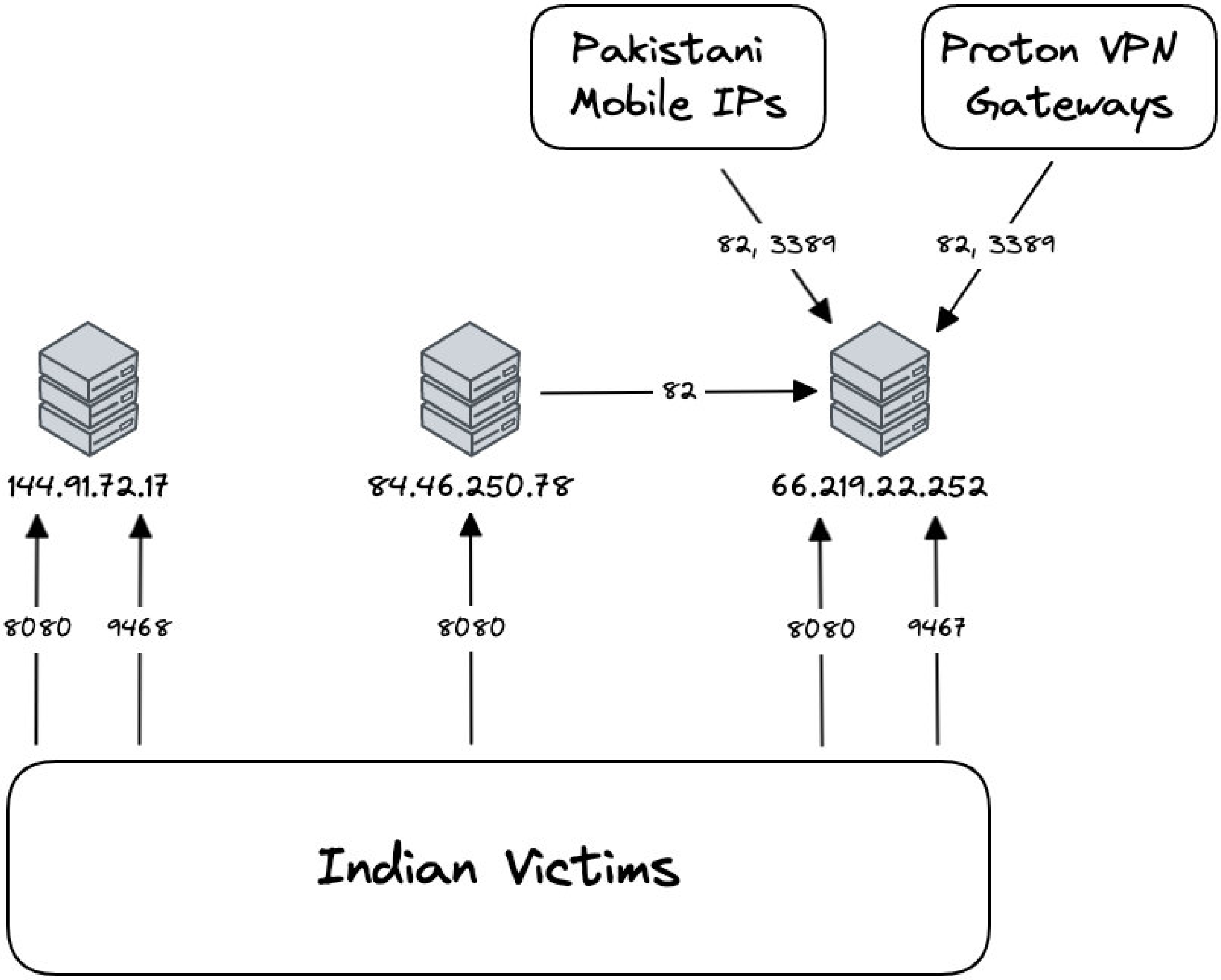


Figure 3: Threat Telemetry Data Associated with the Action RAT C2s

AllaKore RAT

According to QiAnXin's analysis, DUser.dll is also used to load and execute a version of AllaKore RAT, which is dropped on the victim machine via separate infrastructure. AllaKore RAT's capabilities include functionality which allows for keylogging, screenshotting, and remote access of the victim machine, with an ability to also upload stolen information to the C2 server.

We found two samples of AllaKore RAT, both of which were referenced by QiAnXin.

> **Sample One Dropped via:** f369ee5fc8dcf5a9e95d85dadff5a095a0e3a760 (hta.dll) **C2:** www.kcps[.]edu[.]in **AllaKore RAT:** ea844939dc428e6fdb6624d717d0286e4dcae9b1 (simsre.exe) **C2:** 89.117.63.146:9921

> **Sample Two Dropped via:** f369ee5fc8dcf5a9e95d85dadff5a095a0e3a760 (hta.dll) **C2:** www.kcps[.]edu[.]in **AllaKore RAT:** 972d85b5736ae8bdf06a9d74f2a3356829ce2095 (sicsmdb.exe) **C2:** 185.229.119.60:9134

Examining threat telemetry data for the two C2 IPs **89.117.63.146** and **185.229.119.60** we observed initial victim connections on 06 January 2023 and 22 February 2023 respectively.

In total we observed 236 distinct victims, all located in India, connecting to the C2 servers. When compared to the victim numbers for the Action RAT C2s, it could be assessed that AllaKore RAT is deployed more widely and via other means outside of the scope of the infection chain described by QiAnXin.

Further to this activity we also observed 455 distinct IPs (again all located in India) connecting to **89.117.63.146**:7439 and **185.229.119.60**:7469 in activity which commenced at the same time as the activity on the ports associated with the AllaKore RAT samples.

We were unable to identify samples talking to TCP/7439 of **89.117.63.146** and TCP/7469 of **185.229.119.60**, however as previously we would hypothesize that this IP was used for C2 communications with another tool associated with SideCopy activities.

Conclusion

In this blog post we have sought to illustrate the following points:

- We have good evidence to demonstrate this particular SideCopy campaign, highlighted first by others in the industry, was successful in targeting Indian users. This finding is based on observations within our threat telemetry data, indicating victim connections to the C2 servers.
- Victim activity predated the public reporting of this campaign, in some cases by several months. This continues to support the statistics about attacker dwell time, and highlights the importance of retrospective analysis of data logs.
- There is specific evidence to demonstrate that the Action RAT infrastructure, connected to SideCopy, is managed by users accessing the Internet from Pakistan.
- Pivots on known threat actor infrastructure can lead to the identification of further, previously unknown infrastructure, in addition to hints at attribution and management.

Recommendations

- We would recommend that cyber defenders, particularly those located in countries / regions which SideCopy operations are known to target, use the IOCs mentioned in this blog to hunt against their own data holdings (including historical logs), and to preemptively block malicious activity.
- Users of Pure Signal Recon can examine this campaign by querying against the domains and IP addresses referenced in the IOC section below. Further pivots into other currently unknown infrastructure may be possible as this threat actor undertakes future campaigns.

Indicators of Compromise

Malware Hashes (SHA1)

0d68a135b1f4be18481cf44ed02bcbf82aeb542e

3c4c8cbab1983c775e6a76166f7b3c84dde8c8c5

972d85b5736ae8bdf06a9d74f2a3356829ce2095

cb031561fd76643885671922db7d5b840060334d

ea844939dc428e6fdb6624d717d0286e4dcae9b1

f369ee5fc8dcf5a9e95d85dadff5a095a0e3a760

f369ee5fc8dcf5a9e95d85dadff5a095a0e3a760

feeadc91373732d65883c8351a6454a77a063ff5

Domains

www.cornerstonebeverly[.]org

www.kwalityproducts[.]com

www.kcps[.]edu[.]in

IP Addresses (with port pairings 🍷)

144.91.72.17:8080

144.91.72.17:9468

185.229.119.60:9134

66.219.22.252:8080

66.219.22.252:9467

84.46.250.78:8080

89.117.63.146:9921