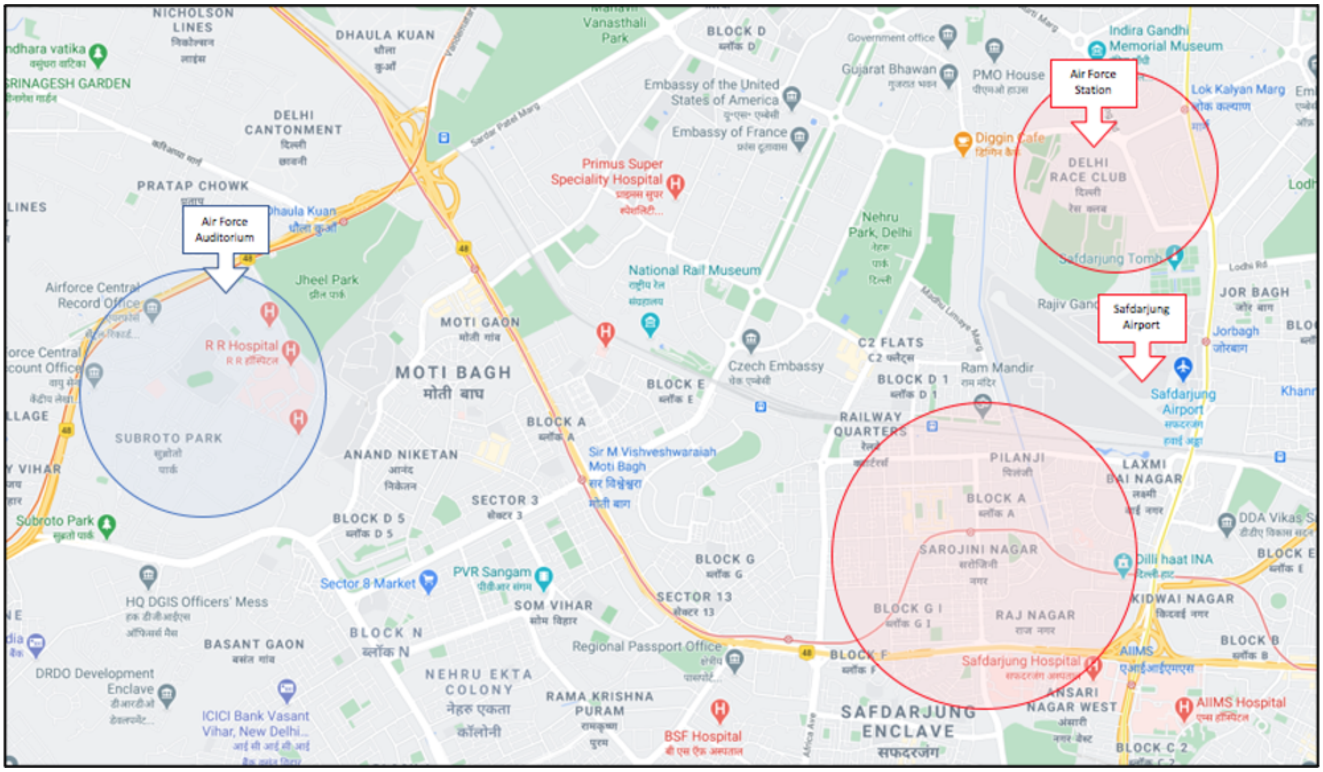
Transparent Tribe APT Infrastructure Mapping

team-cymru.com/blog/2021/04/16/transparent-tribe-apt-infrastructure-mapping/

S2 Research Team View all posts by S2 Research Team April 16, 2021



Introduction

Transparent Tribe (APT36, Mythic Leopard, ProjectM, Operation C-Major) is the name given to a threat actor group largely targeting Indian entities and assets. Transparent Tribe has also been known to target entities in Afghanistan and social activists in Pakistan, the latter of which points towards the assumed attribution of Pakistani intelligence. Tools used by this group include CrimsonRAT, ObliqueRAT, PeppyRAT and AndroidRAT, with most campaigns discovered relying on spear-phishing and social-engineering of victims. Over the coming months Team Cymru's S2 analytic unit will be focusing on the infrastructure behind these known toolsets.

This is the first article of a two-part series on Transparent Tribe's CrimsonRAT infrastructure.

We have been tracking CrimsonRAT , Transparent Tribe's most ubiquitous remote access tool, over a number of months. This blog will present our high-level observations based on a study of 23 CrimsonRAT command and control (C2) servers. Our intention is to provide supporting context to existing Transparent Tribe reporting and IOCs, to aide in future threat reconnaissance activities against this group.

Key Observations

- C2s hosted with a number of different VPS providers – most commonly Contabo, ColoCrossing, Pi Net and QuadraNet.
- Port 3389 was observed open on 83% of the CrimsonRAT C2 servers.
- A total of 62 distinct beacon ports were observed, with minimal evidence of port re-use across C2s
- Traffic to ip-api[.]com, used in the IP geolocation of victims, noted from C2 172.245.87.12
- A review of a recent Transparent Tribe campaign reveals the targeted nature of the group's activities.

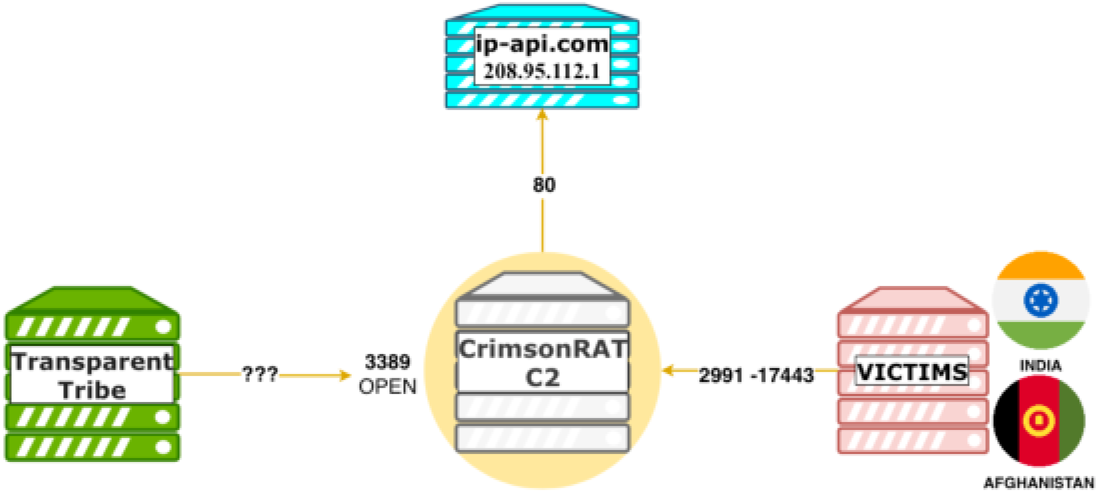


Figure 1:

Summary of Findings

Please note that details of all 23 CrimsonRAT C2 servers are provided in the technical appendix at the end of this blog.

CrimsonRAT C2 Hosting

When examining the IP attribution of CrimsonRAT C2 servers, it is apparent that TRANSPARENT TRIBE actors have sought to spread their infrastructure across a number of distinct providers, likely to provide some resilience to their operations. Whilst eight different providers were observed (Figure 2), there was a degree of preference noted for Contabo (5 servers), QuadraNet (4), Pi Net (4) and ColoCrossing (3).

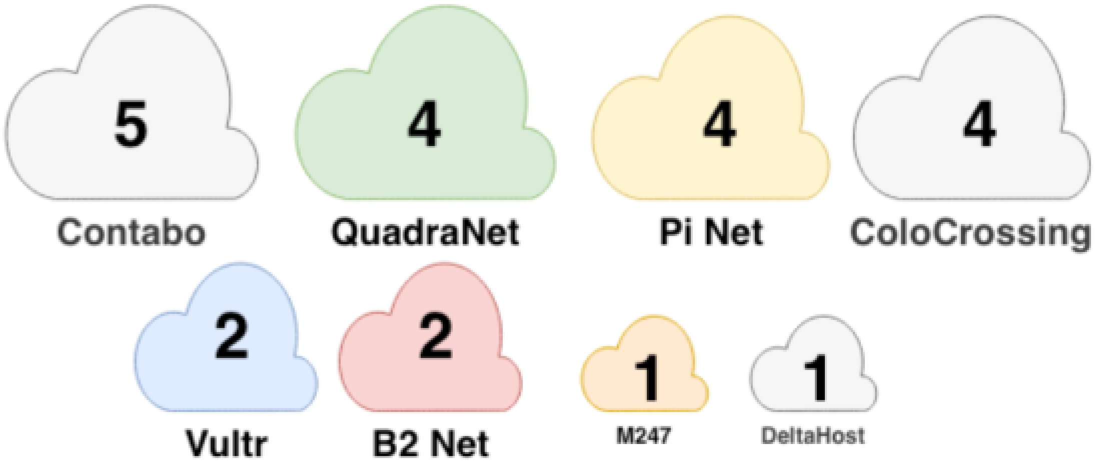


Figure 2: Summary of Hosting Providers

When actors consider which hosting provider to use, many factors likely enter their decision-making process; accepted payment methods, geographical diversity, local privacy laws, and the probability of law enforcement disruption, to name a few.

One caveat for these findings is that whilst specific providers have been mentioned, based on available Whois information, in some cases the ranges used by Transparent Tribe may have been sub-leased to other providers.

Port 3389

When reviewing open ports on the CrimsonRAT C2 server set, Port 3389, commonly associated with the Remote Desktop Protocol (RDP), was observed open in 83% of cases (19 of 23). Whilst this finding may be coincidental, the observed prevalence suggests it is a possible prerequisite for the functionality of the C2 server or it's administration.

Transparent Tribe are known to run different versions of a .NET application which acts as the CrimsonRAT command-and-control panel. This is a GUI application which is used to manage components of the tool on victim hosts (see https://securelist.com/transparent-tribe-part-1/98127/). As an interactive session is required to interface with this application, one hypothesis is that the actors require RDP access to the CrimsonRAT command-and-control panel.

Furthermore, the majority of CrimsonRAT servers were found to be running Windows Server 2012R2.

We are currently conducting an analysis of ongoing and historic connections to CrimsonRAT C2s on Port 3389. The goal of this analysis is to identify any potential uses by Transparent Tribe actors (thus identifying higher order infrastructure), as well as separating this activity from the regular scanning of Port 3389, which takes place on the Internet every day.

Beacon Ports

A typical CrimsonRAT payload can have up to five pre-configured callback ports for communications with the C2 server. We have witnessed minimal evidence of port re-use across samples and the C2s we have analyzed, with only four ports being used more than once: 3878, 4586, 6818 and 8666. It's possible these ports are seemingly randomly selected by the operator.

In total, 62 distinct beacon ports were identified across the 23 C2 servers, from the lower end of 2991 to the higher end of 54131 – although the majority of ports were clustered between 2991 and 17443.

C2 172.245.87.12 (ip-api[.]com Usage)

In addition to inbound victim traffic to C2 **172.245.87.12** (AS-COLOCROSSING, US), we also observed outbound connections to **ip-api[.]com** (208.95.112.1) on Port 80, during the period 12 December 2020 – 06 March 2021.

This finding supports the presence of server version 'A' (as described in the aforementioned Securelist blog) on this particular C2 – which is known to use **ip-api[.]com** for performing IP geolocation lookups of victims when they beacon in.

Our own analysis of the CrimsonRAT server source code identifies that the **ip-api[.]com** lookup occurs automatically when a new victim calls into the controller and that these results are then cached so that further lookups are not required. These lookups can therefore be represented as evidence of 'new' victims with associated timestamp information providing an indication as to when an initial compromise has taken place. It is possible that multiple lookups could occur for the same victim when their IP address changes due to dynamic assignments.

Based on our coverage of C2 **172.245.87.12** we see victim IPs assigned to Indian providers beaconing to the configured ports (as described above). Therefore, using a conversion from UTC to Indian Standard Time (IST) – UTC+05:30, we can see that victims have been newly compromised during 'usual' office hours:

Time Correlation:

- 2020-12-12 03:39:17 UTC = 09:09:17 Local IST
- 2020-12-30 07:28:02 UTC = 12:58:02 Local IST
- 2021-02-04 07:53:52 UTC = 13:23:52 Local IST
- 2021-02-23 03:51:31 UTC = 09:21:31 Local IST
- 2021-03-04 12:10:54 UTC = 17:40:54 Local IST
- 2021-03-06 04:15:27 UTC = 09:45:27 Local IST
- 2021-03-14 09:59:47 UTC = 15:29:47 Local IST

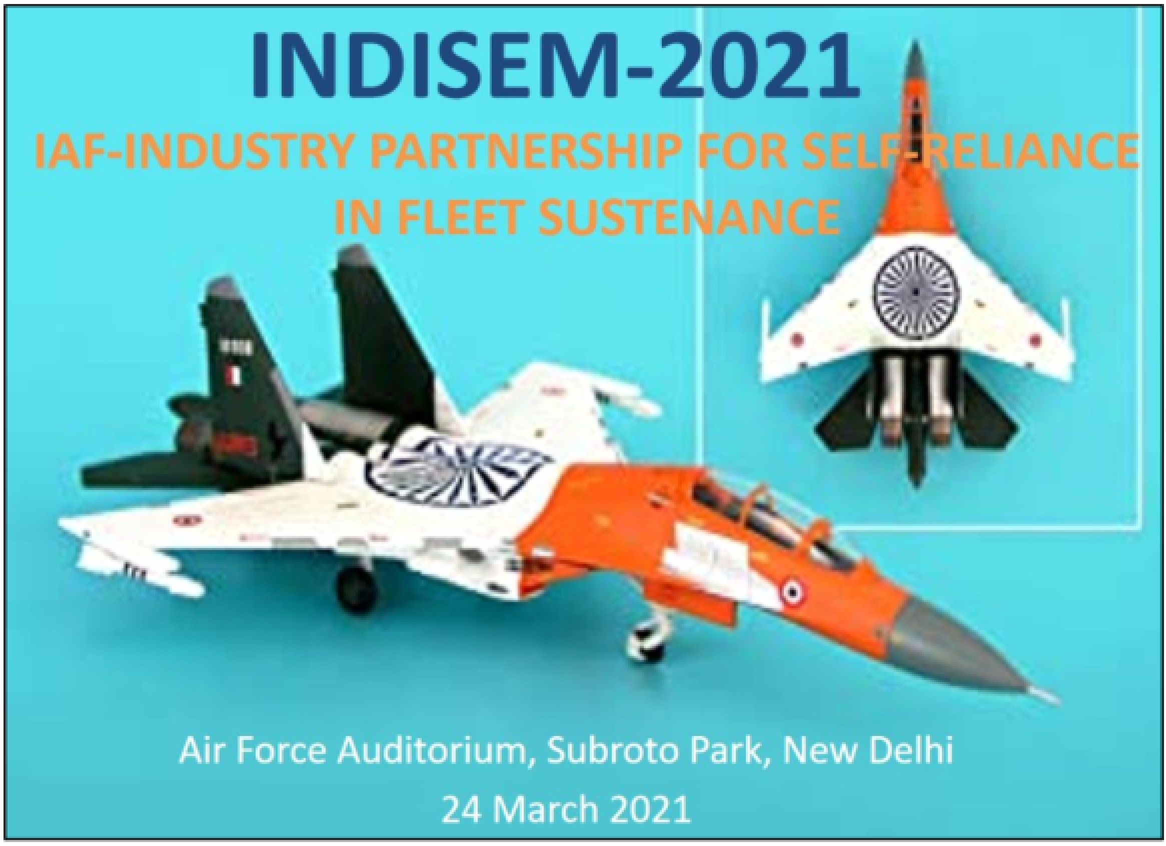
These findings are caveated by the limitations of our coverage, i.e., these findings are accurate based on the traffic we have observed – other compromises may have taken place outside of these hours.

Victimology

A recent Transparent Tribe campaign, targeting the Indian Air Force (IAF), was used to provide an example of victimology.

On 24 March 2021, a Transparent Tribe lure document (Figure 4) was disclosed on Twitter, comprising a PowerPoint presentation for an IAF/industry collaborative event – ‘INDISEM-2021’.

The objective of this event was to purportedly identify organizations in India’s commercial sectors capable of undertaking maintenance contracts for the IAF fleet.



INDISEM-2021

IAF-INDUSTRY PARTNERSHIP FOR SELF-RELIANCE IN FLEET SUSTENANCE

Air Force Auditorium, Subroto Park, New Delhi

24 March 2021

Figure 3: Lure Document Positioning an Indian Air Force Conference

The venue for the event is listed as the Air Force Auditorium in Subroto Park, New Delhi. Open-source research identifies Subroto Park as the location of numerous IAF buildings, including the ‘Air Force School’ (Figure 4).

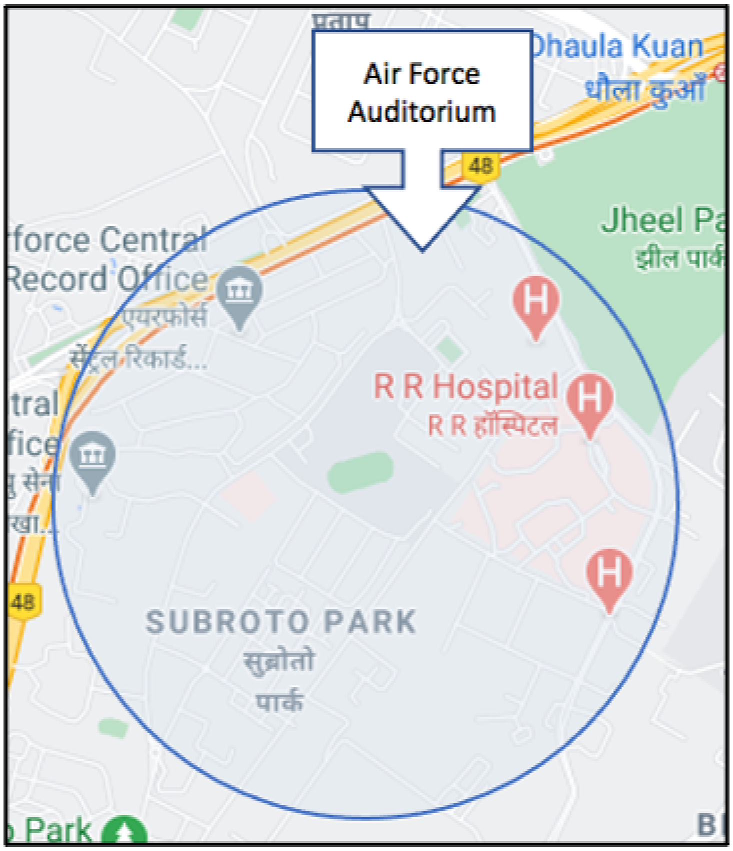


Figure 4: Subroto Park and the Indian Air Force Buildings

Network traffic data for the C2 **185.136.169.155** used in this campaign was reviewed and victim IP addresses connecting to the beacon ports (6128, 8761, 11214, 15882, 17443), were plotted on a map using geolocation information.

This process revealed two clusters of victims in close proximity to Subroto Park (Figure 5).

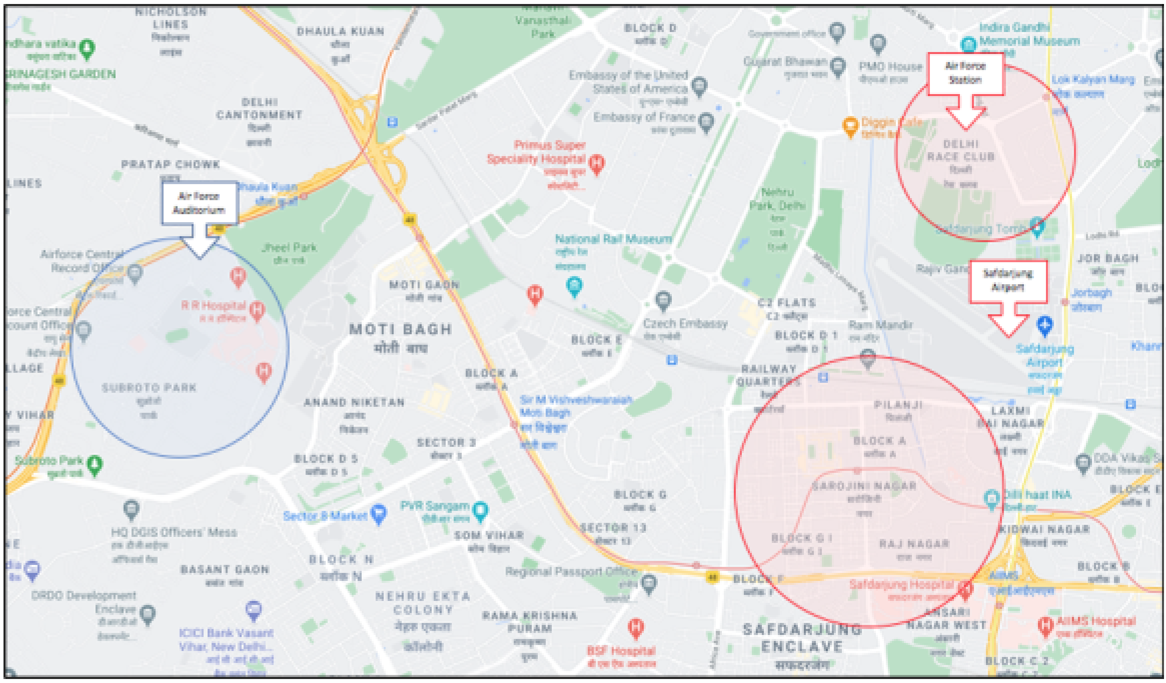


Figure 5: Subroto Park (blue) in Relation to Victim Clusters (red)

The victim cluster to the North centered around another area containing a number of IAF buildings, including an Air Force Station. The Southern cluster centered around the residential area of Sarojini Nagar. Between the two clusters sits Safdarjung Airport, a site which houses a number of Government Administrative buildings, including the Airports Authority of India and the Directorate General of Civil Aviation. The airfield itself is still operational and is used for the transfer of high-value individuals to Indira Ghandi International Airport when they travel out of the country – the Presidential estate is located just to the North of the Air Force Station marked in Figure 4.

The available coverage of this particular campaign shows the likely targeting of individuals within Indian Government or IAF locations, as well as a nearby residential area which could feasibly house some of these individuals.

Technical Appendix

***Beacon Ports consist of observed network traffic to known C2's and may not be representative of entire CrimsonRAT configuration.

IP Address	Whois	Open Ports	Beacon Ports
134.119.181.15	Pi Net, LLC, VN	3389	8861, 8561, 6818
151.106.14.125	Pi Net, LLC, VN	3389	6818, 14618, 8722, 16418, 3468
151.106.19.220	Pi Net, LLC, VN	3389	2682
172.245.247.112	ColoCrossing	3389	3878, 5648, 8666, 11824, 14624
172.245.87.12	ColoCrossing	3389	4586, 6276, 8443, 12447, 18856
173.212.192.229	Contabo	3389	3364, 16564, 8264
173.249.22.30	Contabo	3389	4228, 16582, 10864
173.249.14.104	Contabo	3389	6630, 9808, 3312
173.249.42.113	Contabo	3389	8148
185.136.169.155	Pi Net, LLC, VN	3389	8761, 11214, 6128, 15882, 17443
185.174.102.105	DeltaHost	80	2991, 5991, 54131
198.12.90.116	ColoCrossing	3389	3691, 6582, 4684
23.254.119.11	B2 Net Solutions	3389	3163, 6614, 4828, 5661
23.254.119.118	ColoCrossing		11214
209.127.16.126	B2 Net Solutions	3389	4768

45.32.151.155	Vultr	21, 80, 3389	6126, 11427, 12835
45.77.246.69	Vultr	3389	16185
5.189.134.216	Contabo		5156
64.188.12.126	QuadraNet	3389	9666, 12824, 6658, 49747
64.188.25.143	QuadraNet	3389	4586
64.188.25.206	QuadraNet		4125, 6522, 16621, 11422
66.154.113.38	QuadraNet	3389	3878, 8666
89.249.65.206	M247	3389	4816