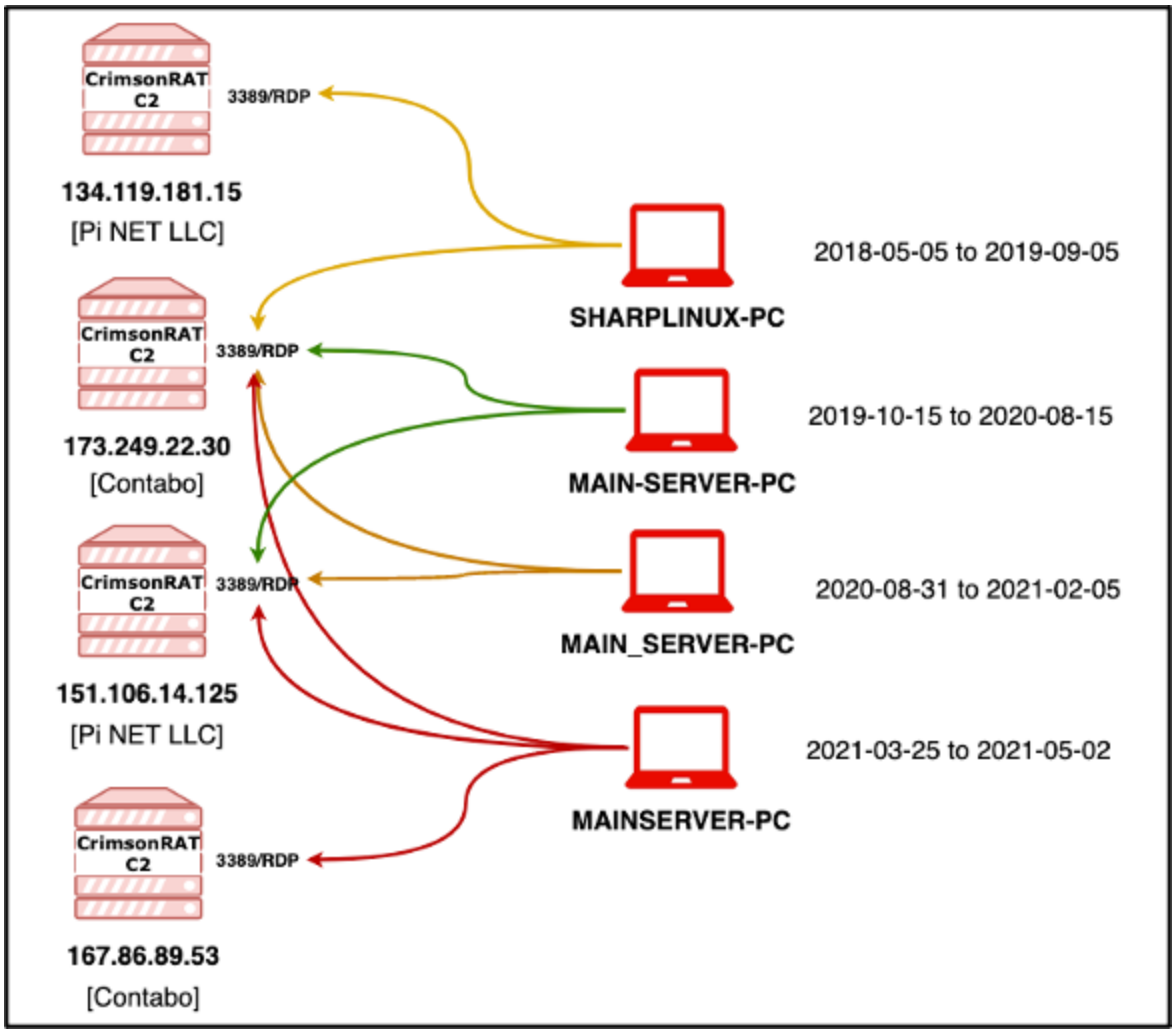
Transparent Tribe APT Infrastructure Mapping

team-cymru.com/blog/2021/07/02/transparent-tribe-apt-infrastructure-mapping-2/

S2 Research Team View all posts by S2 Research Team July 2, 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.

This is the second blog of a two-part series on Transparent Tribe's CrimsonRAT infrastructure. You may read the first article here:

Part 1: A High-Level Study of CrimsonRAT Infrastructure October 2020 – March 2021

We have been tracking CrimsonRAT, Transparent Tribe's most ubiquitous remote access tool, over several months. This blog will present a deeper dive into the methods we use to identify CrimsonRAT infrastructure and observations on specific artefacts which have allowed us to attribute this infrastructure dating back multiple years.

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

- CrimsonRAT infrastructure is largely hosted on infrastructure leased by Pi NET LLC, a Vietnamese VPS reseller.
- An RDP certificate serves as a key indicator for CrimsonRAT and has been observed on 17 C2 servers in total.
- A methodology for tracing CrimsonRAT C2 servers was devised based on network traffic patterns and the scanning of beacon ports.
- CrimsonRAT C2 servers provide a standardized response when an initial TCP connection is established.
- Potential crossover login activity has been observed, linking multiple C2 servers together, as well as providing a link to AhMyth AndroidRAT.

Eggs in One Basket (Pi NET LLC)

When reviewing CrimsonRAT C2 infrastructure an RDP certificate (with a Common Name value of **WIN-P9NRMH5G6M8**) continued to appear. Our certificate data showed this Common Name appearing across many of the previously identified 'preferred' providers (see Part 1) used by Transparent Tribe. After reviewing rWhois records for IP addresses hosting this certificate it became apparent that many, if not all these hosts, were being subleased to **Pi NET LLC**.

A list of all 17 CrimsonRAT C2 servers hosting the Common Name WIN-P9NRMH5G6M8 certificate is provided at the end of this blog.

Expanding this search using Shodan's data holdings, we were able to bolster our theory (the association of the certificate with **Pi NET LLC**) as only a relatively small number of hosts (240) were identified, the majority of which were either assigned directly to, or subleased to **Pi NET LLC**.

Unfortunately, not all providers document the details of subleasing in Whois records, so we were not able to tie ALL the IP addresses identified to a single entity (Pi NET).

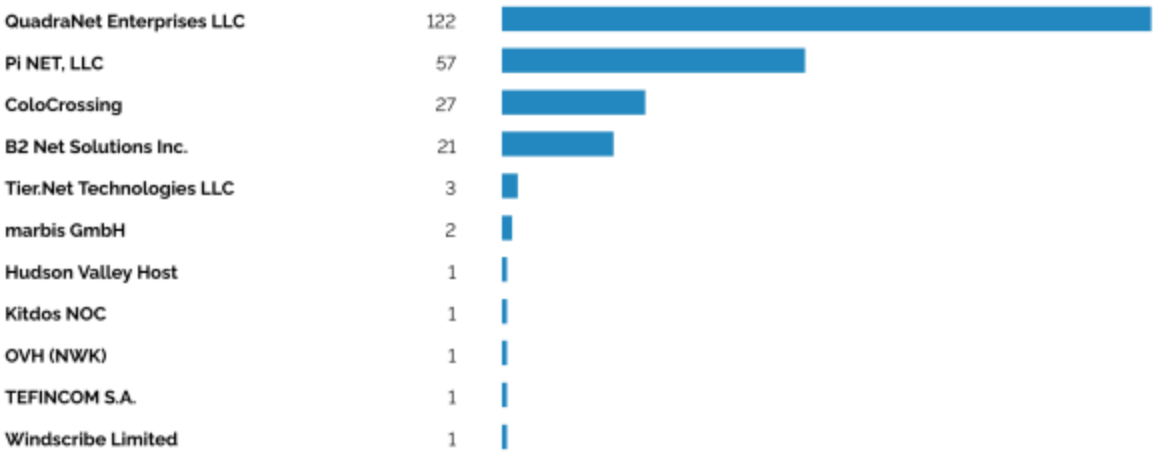


Figure 1:

Shodan 240 hosts found with Common Name WIN-P9NRMH5G6M8

More recently we have also observed a different certificate in use on **Pi NET LLC** hosts, with a Common Name of **WIN-L6BUPB5SQBC**. This certificate is associated with CrimsonRAT C2s **134.119.181.15, 181.215.47.169** and **134.119.181.142** and moving forward could be an alternative indicator of Transparent Tribe activity.

Reviewing Whois information for all CrimsonRAT C2 servers we have identified to date, we found that roughly three-quarters (75%) were associated in some way with **Pi NET LLC**.

Therefore, we assess with moderate confidence that Transparent Tribe is hosting a large proportion of (known) CrimsonRAT infrastructure through this single VPS provider, i.e., whilst CrimsonRAT servers are overtly hosted with several different providers, it is likely that this infrastructure is managed and sold by the small reseller **Pi NET LLC.**

Pi NET LLC (pivps[.]com) is a VPS reseller based out of northern Vietnam, which provides very affordable Windows and Linux hosts accepting payment in various cryptocurrencies alongside conventional methods.

Team Cymru attempted to contact the reseller about this activity but received a canned response on how to submit an abuse complaint. Using the provided instructions we filed an abuse complaint on 17 CrimsonRAT C2s.

Pi NET LLC's known IP ranges are shared via our public GitHub

Sweep & Scan

In Part 1 of this research, we discussed how CrimsonRAT C2 servers communicated with **ip-api[.]com** when new victims beaconed in, providing us with an indicator to look for in our network traffic data when reviewing activity surrounding potential C2 servers. The presence of connections to **ip-api[.]com** therefore providing increased confidence that a particular IP address was associated with CrimsonRAT activity.

The combination of knowing that a large proportion of C2 servers are hosted on **Pi NET** leased IP ranges and that the C2 servers communicate with **ip-api[.]com** has allowed us to develop a 'sweep and scan' technique over time, providing a process for identifying CrimsonRAT C2 servers in the absence of publicly disclosed malware samples.

CrimsonRAT uses a custom C2 protocol where the first five bytes are the size of the rest of the data. Figure 3 is an example of the response to the initial TCP connection to a port where the CrimsonRAT server is listening.

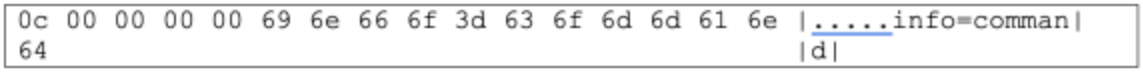


Figure 2: CrimsonRAT C2 response to initial TCP connection

This response provides us with a distinct signature for CrimsonRAT, made more distinct when scanning IP addresses assigned to **Pi NET LLC** that have communicated with **ip-api[.]com**, which allows us to identify currently active C2 servers.

This signature can be implemented in open-source scanning tools (such as Nmap). An example 'nmap-service-probes' file containing the signature for CrimsonRAT C2 servers is available on our public GitHub (Happy scanning!)

The threat reconnaissance methodology is therefore as follows:

1.) Monitor network traffic for all known IP ranges of **Pi NET LLC** to identify hosts connecting to 208.95.112.1:80 (**ip-api[.]com**).

2.) Review inbound connections to candidate C2 IPs looking for victims beaconing in from Indian or Afghanistani-assigned IP addresses (TCP port range 2991–17443).

3.) If potential victim connections are observed, scan the identified port to detect and confirm a CrimsonRAT C2 response.

4.) Step 2 can be skipped but would require a more exhaustive port sweep at Step 3.

When using the above methodology, many 'known' CrimsonRAT C2 servers were identified, however two further servers (**185.136.169.139** and **107.173.204.38**) were also identified, that to our knowledge, had not been publicly reported previously (and do not currently have a malware sample associated with them).

185.136.169.139

Open Port: 3389

C2 Port: 4561,14565,28443

Sample: No sample found

107.173.204.38

Open Port: 3389

C2 Port: 6576, 8586

Sample: No sample found

An analysis of C2 **185.136.169.139** shows victims beaconing in as recently as 01 June 2021, with targeting concentrated in Indian-administered Kashmir.

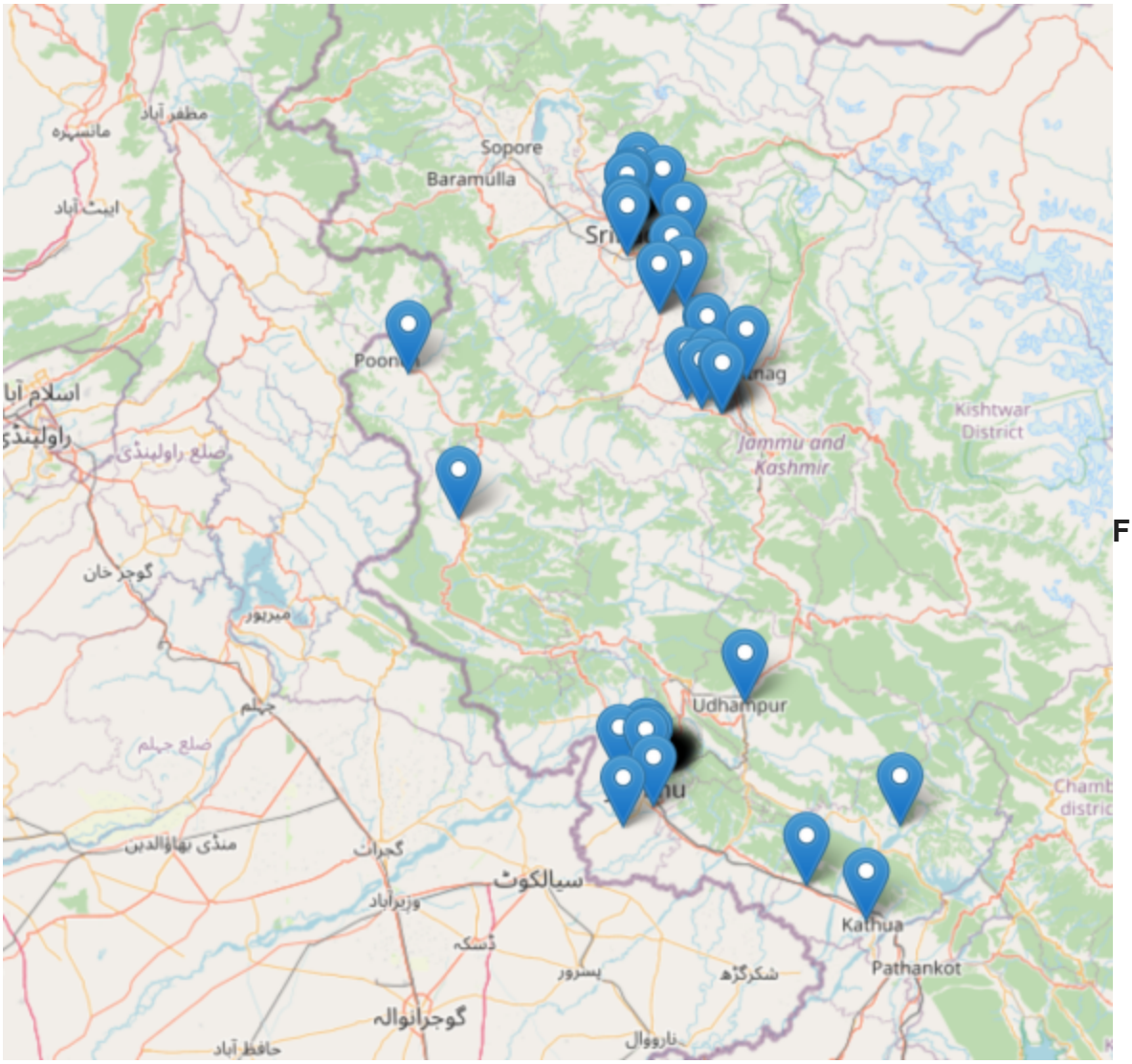


Figure 3: Victim clustering for C2 185.136.169.139

RDP Login Overlap (WeCanSeeYou)

In Part 1 of this research, we discussed our hypothesis that Transparent Tribe operators likely managed their infrastructure via RDP, with TCP/3389 being observed open (and had a service running) on 83% of the servers we analyzed.

When reviewing screenshot data from the Shodan data holdings for C2 **173.249.2230**, we observed the user 'MAINSERVER-PC' visibly logged in at the time of the screenshot. Pivoting on this finding has subsequently allowed us to identify potential crossover activity dating back to May 2018.

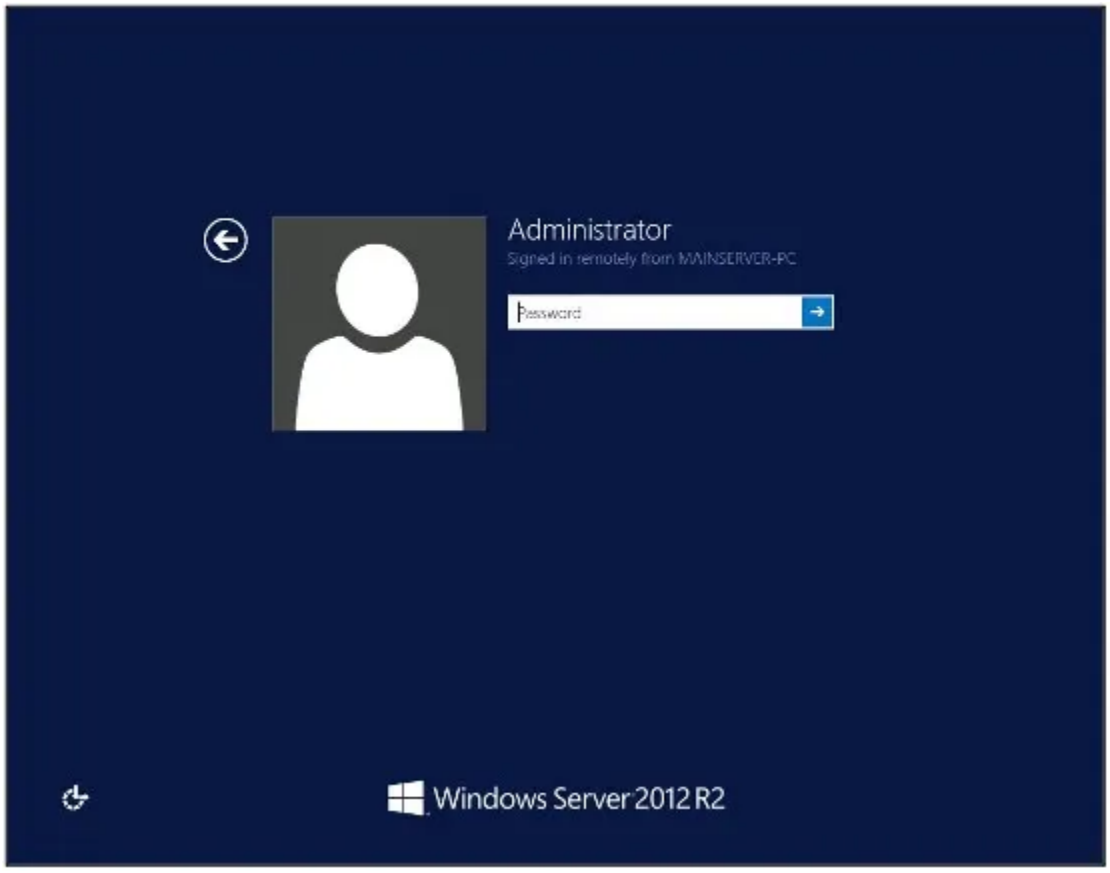


Figure 4: Shodan screenshot MAINSERVER-PC login

Caveat: this could be legitimate VPS administrator panel traffic or successful bruteforce attempts on RDP. Since we were unable to speak with the provider we cannot confirm.

Reviewing the screenshot history of C2 **173.249.22.30** in Shodan showed the following activity timeline with logged in Machine Name and Date(s) Observed.

"**MAINSERVER-PC**" 2021-04-20, 2021-03-25

"**MAIN_SERVER-PC**" 2021-02-14, 2021-02-12, 2021-01-04, 2020-12-31, 2020-12-11, 2020-11-23, 2020-11-16, 2020-09-22, 2020-09-14

"**MAIN-SERVER-PC**" 2020-08-15, 2020-07-13, 2020-06-30, 2020-06-19, 2020-06-12, 2020-06-04, 2020-05-28, 2020-05-04, 2020-03-21, 2020-03-05, 2020-03-01, 2020-02-27, 2020-02-01, 2020-01-28, 2019-12-31, 2019-12-27, 2019-12-26, 2019-10-22, 2019-10-15

"**SHARPLINUX-PC**" 2019-09-05, 2019-08-25, 2019-08-21, 2019-08-02, 2019-07-21, 2019-04-12, 2019-01-24, 2018-11-25, 2018-05-05

Based on these possible indicators of successful login activity, a review was undertaken to capture this data for all known CrimsonRAT C2 hosts.

In addition to C2 **173.249.22.30**, a pattern of crossover login activity emerged for the following C2 servers: **134.119.181.15**, **151.106.14.125** and **167.86.89.53**, between May 2018 and May 2021.

This activity highlighted the odd nature of the renaming of “MAINSERVER” to various similar schemas, with the oldest login events showing “SHARPLINUX-PC”.

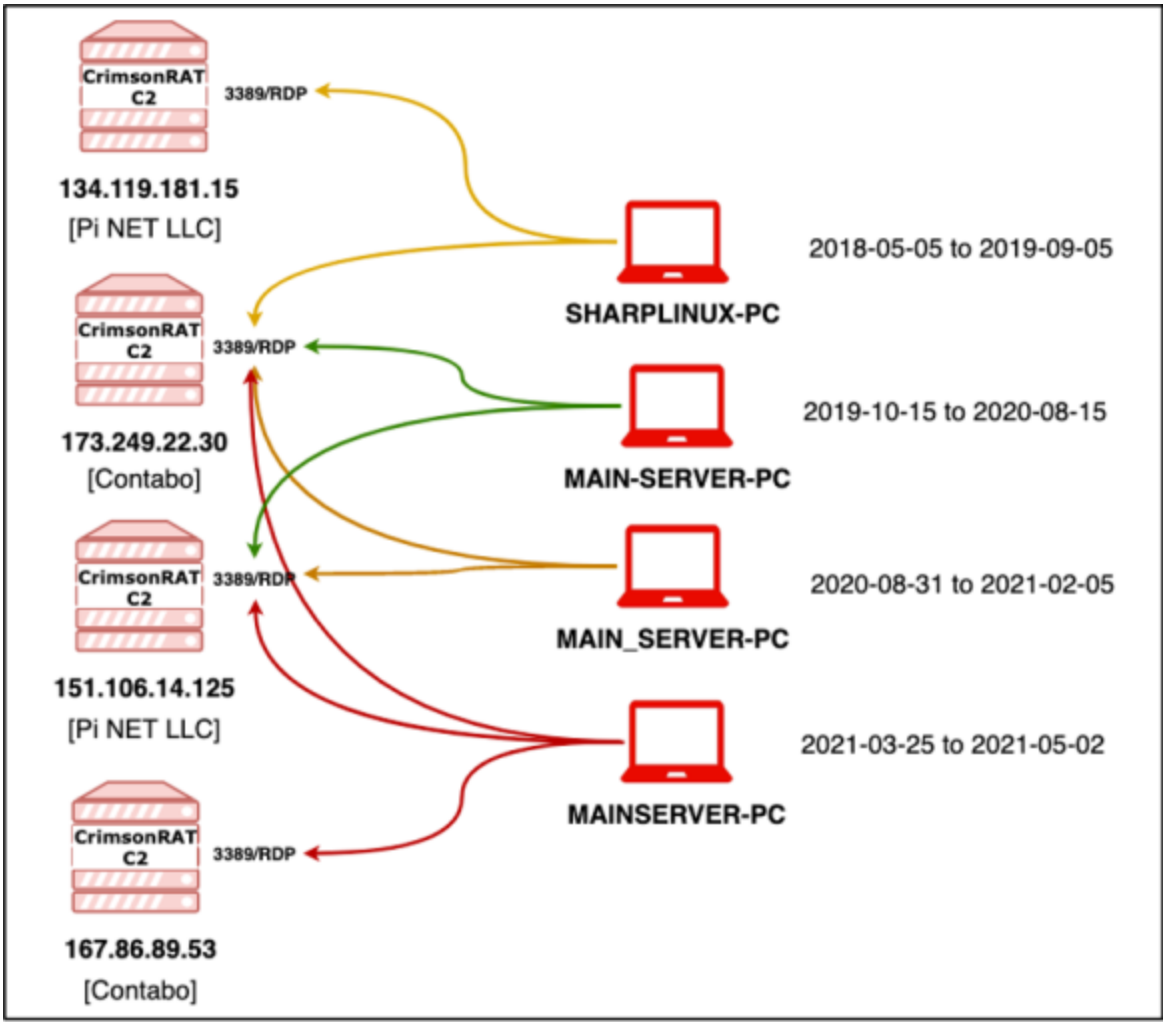


Figure 5: Overlapping RDP login events and timeline

As we were still skeptical of the link between these logins and Transparent Tribe, we decided to map timestamps related to known CrimsonRAT malware samples (associated with the IP addresses in question) to the timestamps observed in Figure 7.

The results of which are as follows:

134.119.181.15 – 940667b9051600cbfb471ebc70cda43b

Submitted 2019-03-23 & Compiled 2019-01-08

173.249.22.30 – babc1b62dd7c823f8536476aef874a3d

Submitted 2019-06-18 & Compiled 2018-07-30

151.106.14.125 – 7a1f111520e5e74ba09e7f4beac6a84a

Submitted 2020-09-17 & Compiled 2020-06-20

167.86.89.53 – 4bda3f8d0cb36b33244afdb071a20860

Submitted 2021-04-27 & Compiled 2021-04-20

As can be seen, the compilation and submission timestamps fall within the ranges detailed in Figure 7, it can therefore be stated that Transparent Tribe were interacting with these C2 servers at the time the logins were observed.

As an additional measure to increase our confidence in these findings and to rule out the usernames being indicative of default management activity undertaken by **Pi NET LLC**. A VPS was purchased from **Pi NET LLC,** interactions with which confirmed that these usernames were defined by the customer/end user – i.e., potentially Transparent Tribe actors.

The usernames associated with these logins are therefore potential indicators of the group's activity.

Taking this analysis one step further, we were able to find crossover login activity that linked CrimsonRAT C2s (198.46.177.73, 192.99.241.4 and 66.154.113.38) with an AhMyth AndroidRAT C2 (212.8.240.221). In this case the usernames observed were 'WATER-PC' and 'YouCantSeeMe' (apparently WeCanSeeYou).

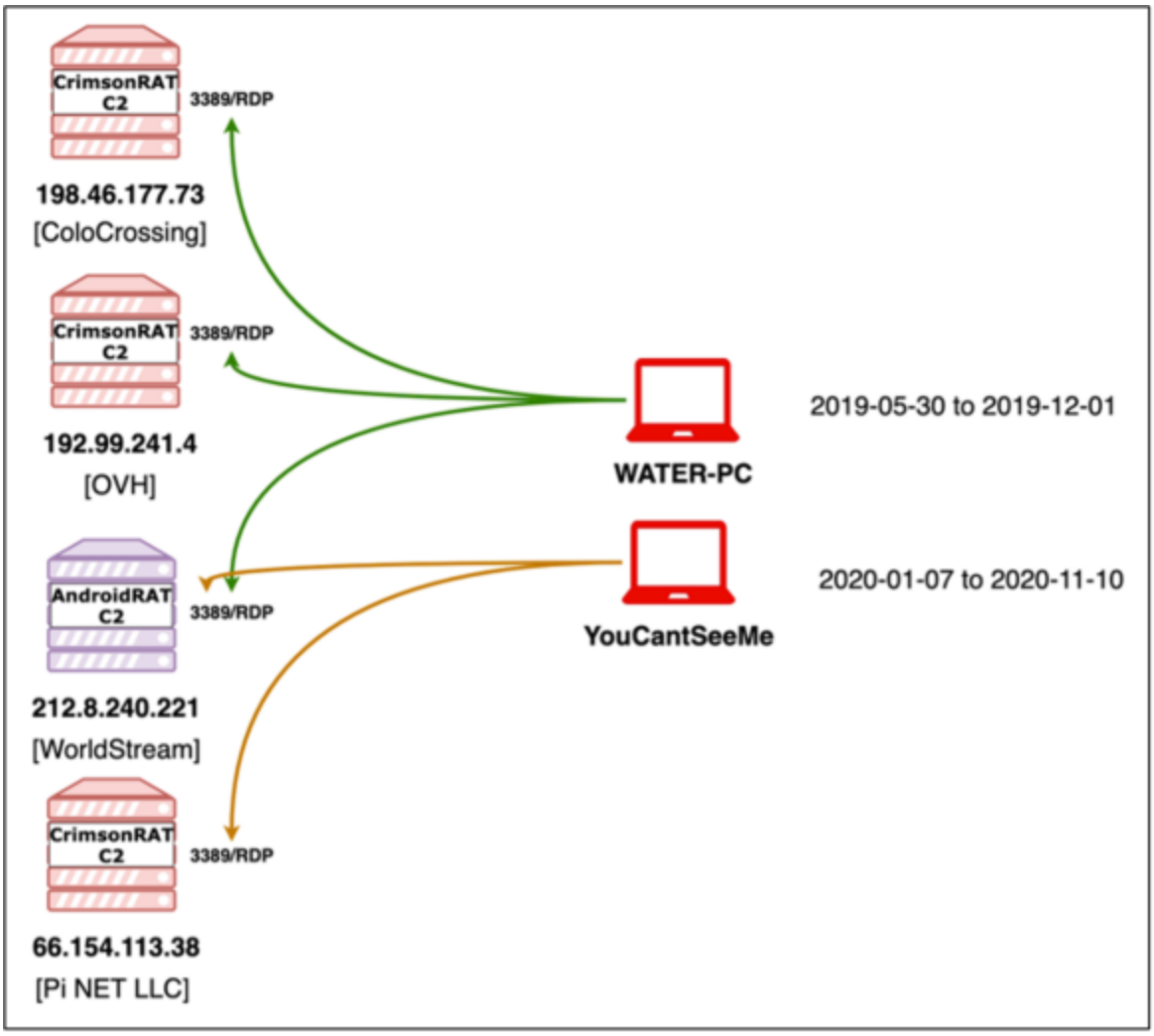


Figure 6: Overlapping RDP login events of AndroidRAT & CrimsonRAT

Conclusion

Transparent Tribe continue to pursue their intelligence collection objectives with CrimsonRAT targeted mainly at Indian entities. In this two-part blog series, we have highlighted some of the specific traits associated with CrimsonRAT infrastructure:

- The likely use of RDP / Port 3389 for management activities
- The prevalence of the Common Name WIN-P9NRMH5G6M8 certificate
- Concentration of activity in Pi NET LLC
- A discernible pattern in the response from the C2 server

Using the techniques that we have highlighted in this blog, it is possible to identify and track C2 servers without first observing associated malware samples, providing an opportunity to get a step ahead of the actors. By providing insight into these techniques, including the sharing of the Nmap script, we hope to provide the means for others to trace Transparent Tribe activities, to potentially limit their impact.

APPENDICES

CrimsonRAT – Common Name WIN-P9NRMH5G6M8

151.106.14.125

Pi NET LLC

WIN-P9NRMH5G6M8

172.245.247.112

ColoCrossing

WIN-P9NRMH5G6M8

107.173.204.38

ColoCrossing

WIN-P9NRMH5G6M8

64.188.12.126

QuadraNet [Pi NET LLC]

WIN-P9NRMH5G6M8

23.254.119.11

B2 Net Solutions [Pi NET LLC]

WIN-P9NRMH5G6M8

104.144.198.105

B2 Net Solutions [Pi NET LLC]

WIN-P9NRMH5G6M8

209.127.16.126

B2 Net Solutions [Pi NET LLC]

WIN-P9NRMH5G6M8

104.227.97.53

B2 Net Solutions [Pi NET LLC]

WIN-P9NRMH5G6M8

198.12.90.116

ColoCrossing

WIN-P9NRMH5G6M8

151.106.19.220

Pi NET LLC

WIN-P9NRMH5G6M8

185.136.169.155

Pi NET LLC

WIN-P9NRMH5G6M8

23.254.119.118

ColoCrossing

WIN-P9NRMH5G6M8

107.175.1.103

ColoCrossing

WIN-P9NRMH5G6M8

185.136.169.139

Pi NET LLC

WIN-P9NRMH5G6M8

167.160.166.177

QuadraNet [Pi NET LLC]

WIN-P9NRMH5G6M8

64.188.25.206

QuadraNet [Pi NET LLC]

WIN-P9NRMH5G6M8

66.154.113.38

QuadraNet [Pi NET LLC]

WIN-P9NRMH5G6M8

RDP Activity – CrimsonRAT C2's

Chain of custody for these C2 IPs cannot be definitively proven. As such there may be legitimate historical **Pi NET LLC** customers logging in for dates further back in time.

151.106.14.125

Pi NET LLC

Logged in from "MAINSERVER-PC" 2021-04-11, 2021-03-31, 2021-03-31, 2021-03-26

Logged in from "MAIN_SERVER-PC" 2021-02-05, 2021-01-07, 2020-11-25, 2020-09-19, 2020-09-10, 2020-08-31

Logged in from "MAIN-SERVER-PC" 2020-08-15, 2020-07-23, 2020-05-29, 2020-04-30

167.86.89.53

Contabo

Logged in from "MAINSERVER-PC" 2021-05-02, 2021-04-12,

Logged in from "ALPHA-PC" 2020-05-11, 2020-02-03, 2020-01-03

173.249.22.30

Contabo

Logged in from "MAINSERVER-PC" 2021-04-20, 2021-03-25

Logged in from "MAIN_SERVER-PC" 2021-02-14, 2021-02-12, 2021-01-04, 2020-12-31, 2020-12-11, 2020-11-23, 2020-11-16, 2020-09-22, 2020-09-14

Logged in from "MAIN-SERVER-PC" 2020-08-15, 2020-07-13, 2020-06-30, 2020-06-19, 2020-06-12, 2020-06-04, 2020-05-28, 2020-05-04, 2020-03-21, 2020-03-05, 2020-03-01, 2020-02-27, 2020-02-01, 2020-01-28, 2019-12-31, 2019-12-27, 2019-12-26, 2019-10-22, 2019-10-15

Logged in from "SHARPLINUX-PC" 2019-09-05, 2019-08-25, 2019-08-21, 2019-08-02, 2019-07-21, 2019-04-12, 2019-01-24, 2018-11-25, 2018-05-05

134.119.181.15

Pi NET LLC

Logged in from “SHARPLINUX-PC” 2019-01-25, 2018-12-14, 2018-11-23, 2018-11-03, 2018-10-15

66.154.113.38

QuadraNet

Logged in from “LINDSAY” 2021-04-06

Logged in from “YouCantSeeMe” 2020-11-10

Logged in from “DESKTOP-MRNHBAD” 2020-10-10

Logged in from “DESKTOP-AMQ4CQ0” 2020-02-18, 2020-02-09, 2020-01-29, 2020-01-26, 2020-01-23

Logged in from “LAPTOP-UUNKFB1F” 2019-11-23

185.136.169.155

Pi NET LLC

Logged in from “LAPTOP-9U6I2PN0” or “LAPTOP-9U612PN0” 2020-10-12

104.144.198.105

B2 Net Solutions

Logged in from “LAPTOP-816SBJ69” 2021-05-19

Logged in from “DESKTOP-H05P53Q” 2021-02-25, 2021-01-30

Logged in from “DESKTOP-HABU36A” 2021-01-02

Logged in from “MajorTROUBLE” 2019-09-09

107.175.1.103

ColoCrossing

Logged in from “FUKRY-PC” 2021-04-25, 2021-01-25, 2020-12-30, 2020-10-07, 2020-10-01

Logged in from “PAREET-PC” 2020-08-29, 2020-08-27,

Logged in from “DESKTOP-KOH33BE” 2020-07-12, 2020-07-01, 2020-06-16, 2020-05-13, 2020-05-11,

Logged in from “WINDOW-PC” 2020-04-30, 2019-12-23, 2019-11-25, 2019-11-14, 2019-10-21, 2019-10-05

Logged in from “HAIR-PC” 2019-08-04

167.160.166.177

QuadraNet

Logged in from “DESKTOP-G2BRQ9H” 2020-12-23

185.136.169.139

Pi NET LLC

Logged in from “DESKTOP-4PS2LQ2” 2020-6-17, 2020-06-09, 2020-06-03, 2020-06-02, 2020-04-10

Logged in from “SM-T590-8.1.0” 2019-11-02

Logged in from “SM-G975F-10”

104.227.97.53

B2 Net Solutions

Logged in from “DESKTOP-EOCT1H4” 2021-05-31, 2021-04-26

Logged in from “DESKTOP-HS0GBJK” 2020-09-23

Logged in from “LAPTOP-NM8GTNOV” 2019-10-08

198.12.90.116

ColoCrossing

Logged in from “MHA-L29” 2021-04-28, 2021-03-26 <—Possibly a Huawei Mate 9 phone

Logged in from “DESKTOP-45DG869” 2020-09-30, 2020-08-28, 2020-07-29

Logged in from “KHAN-PC” 2020-05-04

64.188.12.126

QuadraNet

Logged in from “Ghazi-PC” 2020-11-03, 2020-10-05, 2020-09-16

173.249.42.113

Contabo

Logged in from “JUPITER-PC” 2021-04-08, 2021-04-07, 2021-03-24, 2021-03-17, 2021-02-16, 2021-02-10, 2020-12-29, 2020-12-12, 2020-11-19, 2020-11-14

Logged in from “ALTIMETE-PC” 2019-06-04

64.188.25.206

QuadraNet

Logged in from “DESKTOP-QRE8VL3” 2020-07-23

173.212.192.229

[Contabo]

Logged in from “DESKTOP-0OORLDR” 2021-02-17

Logged in from “DESKTOP-QPCLT7A” 2020-07-29

Logged in from “CABLES-PC” 2020-04-01

Logged in from “DESKTOP-LJASOND” 2020-03-04

178.238.229.192

[Contabo]

Logged in from “FUKRY-PC” 2021-06-01, 2021-05-11, 2021-05-04, 2021-02-16, 2021-01-14, 2020-12-19, 2020-12-11, 2020-11-06, 2020-10-13, 2020-10-02

Logged in from “DESKTOP-SUVBKTE” 2021-05-23

Logged in from “PAREET-PC” 2020-09-18, 2020-09-17, 2020-09-08, 2020-08-05, 2020-07-21

Logged in from “DESKTOP-KOH33BE” 2020-06-08, 2020-05-31

Logged in from “WINDOW-PC” 2020-04-20, 2020-02-02, 2019-12-02, 2019-11-27, 2019-10-16, 2019-10-01

Logged in from “HAIR-PC” 2019-08-23, 2019-08-19, 2019-08-06, 2019-08-05, 2019-07-30

Logged in from “HP-PC” 2019-07-14

RDP Activity – Unique Machine Names Observed

The following list contains only unique machine names observed logging into CrimsonRAT C2 servers. There may be false positives due to the timeline and proof of ownership.

ALPHA-PC

ALTIMETE-PC

CABLES-PC

DESKTOP-0OORLDR

DESKTOP-45DG869

DESKTOP-4PS2LQ2

DESKTOP-AMQ4CQ0

DESKTOP-EOCT1H4

DESKTOP-G2BRQ9H

DESKTOP-HS0GBJK

DESKTOP-KOH33BE

DESKTOP-LJASOND

DESKTOP-MRNHBAD

DESKTOP-QPCLT7A

DESKTOP-QRE8VL3

FUKRY-PC

Ghazi-PC

HAIR-PC

JUPITER-PC

KHAN-PC

LAPTOP-816SBJ69

LAPTOP-9U6I2PN0

LAPTOP-NM8GTNOV

LAPTOP-UUNKFB1F

LINDSAY

MAIN-SERVER-PC

MAINSERVER-PC

MAIN_SERVER-PC

MHA-L29

Michaels-MBP-2

PAREET-PC

SHARPLINUX-PC

SM-G975F-10

WINDOW-PC

YouCantSeeMe