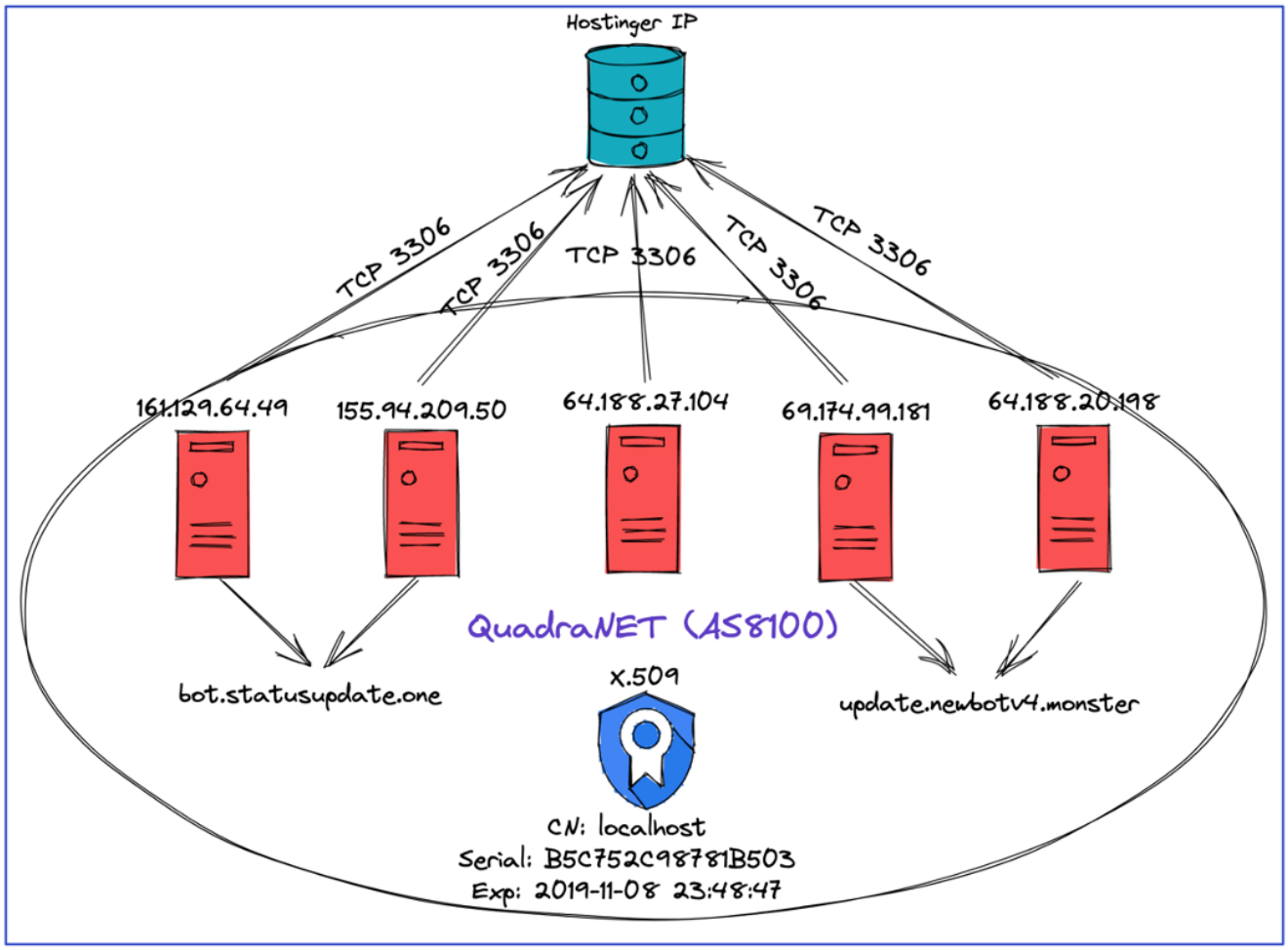
An Analysis of Infrastructure linked to the Hagga Threat Actor

team-cymru.com/blog/2022/07/12/an-analysis-of-infrastructure-linked-to-the-hagga-threat-actor

Kyle Krejci View all posts by Kyle Krejci July 12, 2022



Summary

As this research reveals, mapping out adversary infrastructure has distinct advantages that enable a proactive response to future threats. A well resourced team with access to the right tools can monitor changes to adversary infrastructure in real time, discoveries can become strategic advantages when fully exploited. This blog is geared towards the practitioner threat hunters and threat researchers, anyone reading this with the bottomline in mind should take a look at our economic study here first.

Introduction

We began tracking the threat actor Hagga in late 2021 following the release of an analysis by Z-Lab (Yoroi Security's malware research team). Z-Lab were tracking a worldwide campaign to distribute the Agent Tesla information stealer through an elusive multi-stage infection process. In their analysis, they shared the IOCs for this campaign, including a single hardcoded IP address (69.174.99.181) and a common URL directory pattern for the identified C2 panels.

This blog will describe how we were able to pivot in threat telemetry, using these IOCs as seeds, to identify several other C2s used by this threat actor, ultimately leading us to a backend MySQL server.

Figure 1: C2 Panel IOCs

Key Observations

- Hagga infrastructure is hosted on dedicated leased infrastructure, largely on QuadraNet and Vietnam Posts and Telecommunications (VNPT).
  .
- An HTTPS certificate serves as a key indicator of Hagga C2 panels.

69.174.99.181 (QuadraNet, US)

Passive DNS data for 69.174.99.181 identified it hosting the domain (update.)newbotv4[.]monster from 01 November 2021 onwards. During the period 17 September – 17 December 2021, no further domains were hosted on this IP, indicating it was likely dedicated infrastructure (and not a compromised / shared host).

Reviewing certificate data for this IP address identified an expired self-signed SSL certificate with a CN value of localhost.

SHA1: B0:23:8C:54:7A:90:5B:FA:11:9C:4E:8B:AC:CA:EA:CF:36:49:1F:F6

Whilst examining threat telemetry for 69.174.99.181, it was noted that 97% of the observed data related to communications with a single Hostinger IP address on TCP/3306 (the default port for MySQL servers). This activity occurred between 14 October – 17 December; occurring during the same time window as the Agent Tesla campaign identified by Z-Lab.

Hostinger IP Address

Note: The Hostinger IP address is redacted throughout this report. As backend infrastructure, its identification would not provide any value to network defenders, and as explained below is likely also utilized for unconnected shared hosting purposes.

Passive DNS data identified this IP as a web hosting control panel server. This is supported by open ports data identifying 16 TCP ports that are associated with Hostinger cPanel services. Namely, ports 21, 25, 80, 110, 143, 443, 465, 587, 993, 995, 2080, 2083, 2086, 2087, and 3306.

Threat telemetry data for the Hostinger IP address identified inbound connections to TCP/3306 from numerous other IP addresses dating back to at least 17 September 2021. It was assessed that the IP was shared amongst other Hostinger clients, who were likely unconnected to malicious activities.

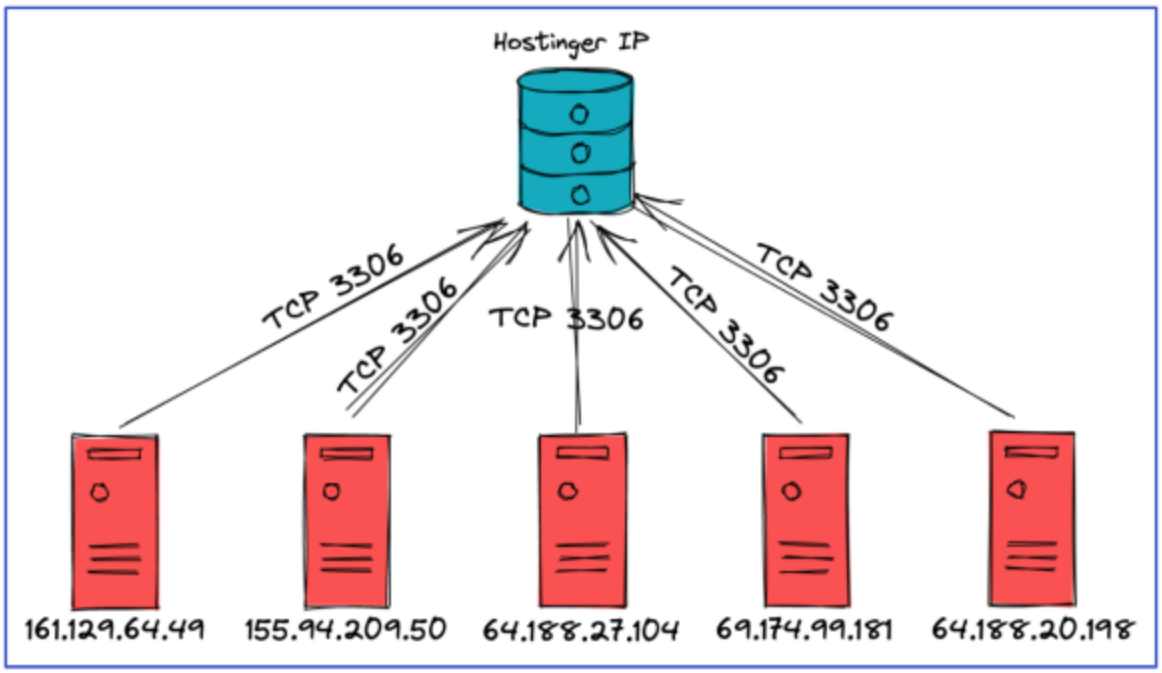


Figure 2: Hostinger MySQL Clients

Hostinger MySQL Clients

Considering the likelihood that the Hostinger IP was used in shared hosting, we needed to include additional constraints to limit our scope to data of relevance to the initial (and potentially other) C2s.

We identified several HTTP requests to the original C2 IP address, with several 'webpanel' paths using a common naming convention. These paths aligned with the Z-LAB C2 indicators.

Destination	URL
69.174.99.181:80	http://69.174.99.181/webpanel-reza/mawa/7f6328c1fd5ef5628c19.php
69.174.99.181:80	http://update.newbotv4.monster/webpanel-reza/bootstrap/dist/js/
69.174.99.181:80	http://update.newbotv4.monster/webpanel-reza/plugins/bower_components/jquery-steps-master/
69.174.99.181:80	http://69.174.99.181/webpanel-muti/mawa/647df66098e0036b38ea.php
69.174.99.181:80	http://69.174.99.181/webpanel-muti/mawa/
69.174.99.181:80	http://69.174.99.181/webpanel-roth/files/
69.174.99.181:80	http://69.174.99.181/webpanel-charles/files/

Table 1: 69.174.99.181 URL Requests

In addition, we also identified requests to one of the other Hostinger MySQL clients that matched one of the 'webpanel-' patterns:

Destination	URL
155.94.209.50:80	http://bot.statusupdate.one/webpanel-charles/
155.94.209.50:80	http://bot.statusupdate.one/webpanel-charles/login.php
155.94.209.50:80	http://bot.statusupdate.one/webpanel-charles/bootstrap/dist/css/bootstrap.min.css
155.94.209.50:80	http://bot.statusupdate.one/webpanel-charles/plugins/sweetalert/dist/sweetalert.css
155.94.209.50:80	http://bot.statusupdate.one/webpanel-charles/bootstrap/dist/js/bootstrap.min.js

Table 2: 155.94.209.50 URL Requests

Interestingly, one of the 155.94.209.50 URL requests was for a 'login.php' page. When navigating to that URL we were taken to a login page containing a "Mana Tools" logo.

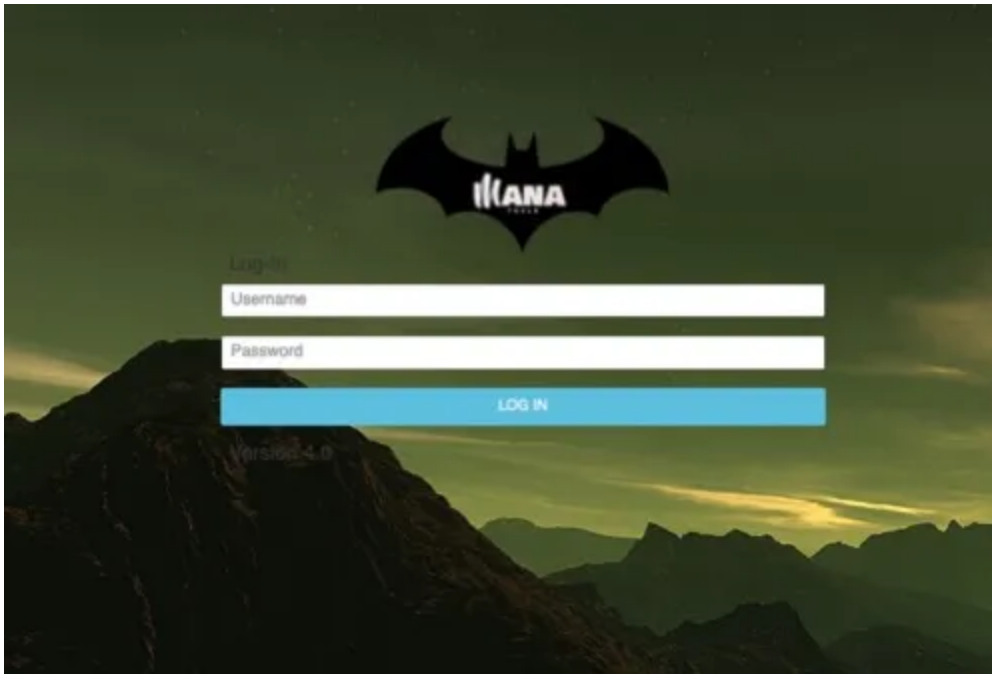


Figure 3: Mana Tools C2 Panel

Whilst we did not have evidence of a URL request to 69.174.99.181 for a 'login.php' page, when navigating to the URL http[:]//69.174.99.181/webpanel-reza/login[.]php we were taken to an identical page.

First reported in 2019 by Yoroi researchers, Mana Tools is a malware distribution and C2 panel that was created by the threat actor Hagga. It has been associated with several well-known malware variants, including RevengeRAT, AzoRult, Lokibot, Formbook, and Agent Tesla.

In addition to 155.94.209.50, we identified a further three MySQL clients hosting the same expired self-signed SSL certificate as 69.174.99.181.

According to reverse DNS and WHOIS information, all the identified IPs (based on URL and certificate data) are hosted on QuadraNet infrastructure.

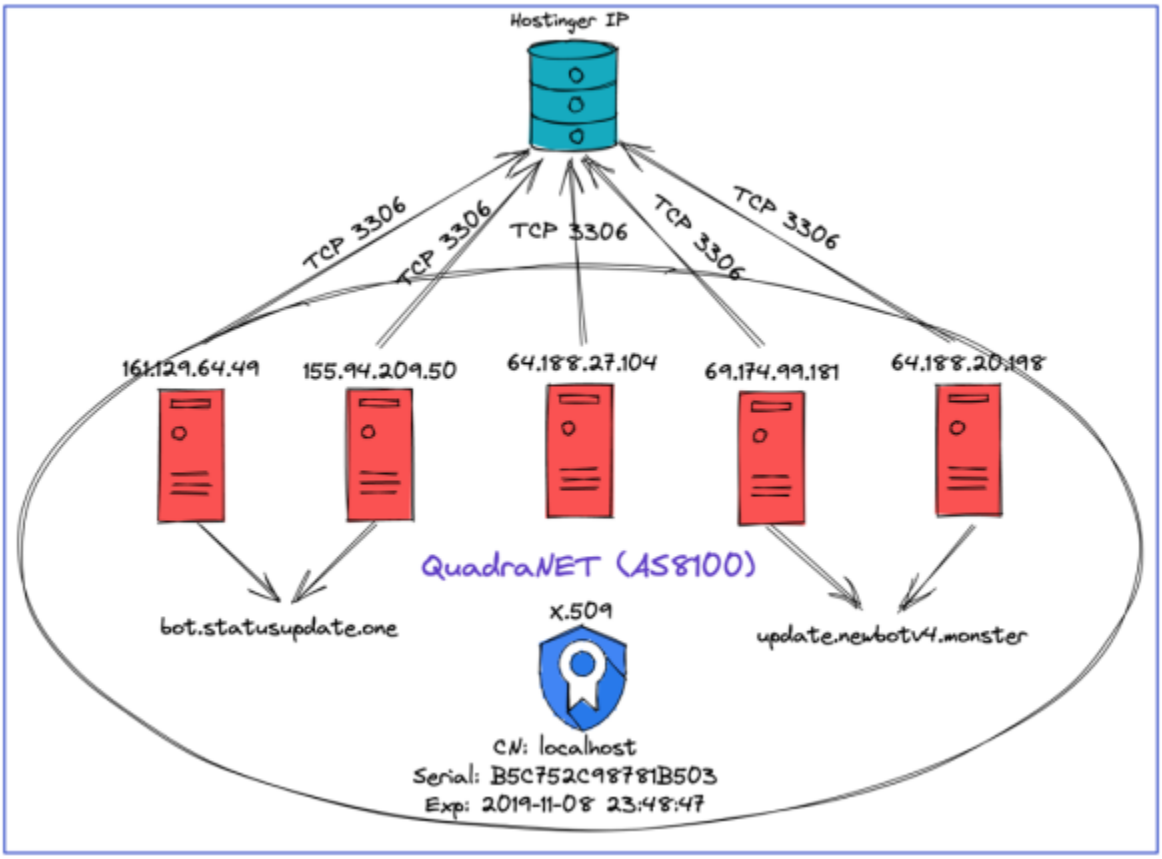


Figure 4: Hostinger MySQL Client Relation

Examining open ports data for each of the above IPs, it appears that they are run on MS-Windows based operating systems. In addition to having standard Windows ports open, TCP/445, TCP/3389, and TCP/445, they also returned WIN-NetBIOS Computer Names in the RDP response.

We also found commonalities amongst several of the Hostinger MySQL client IPs in Passive DNS data.

Domain bot.statusupdate[.]one (resolving to 161.129.64.49) was also observed in URL request data in connection with the Mana Tools C2 panel. 64.188.20.198 replaced the original C2 (69.174.99.181) as the hosting IP for domain update.newbotv2[.]monster.

Based on threat telemetry for communications with the Hostinger IP and timestamps for the Passive DNS resolutions, it appears that the threat actor “rebranded” the C2 domain from bot.statusupdate[.]one to newbotv4[.]monster around 13 October 2021.

The X.509 Certificate

It was identified that the certificate (Figure 3) with the serial B5C752C98781B503 was a default certificate included with OpenSSL as part of an XAMPP installation. XAMPP is a free, open-source distribution that packages OpenSSL, MariaDB, PHP, and Perl with an Apache web server. Its primary use is for developers, allowing them to deploy a web server on a local server to test web applications without the need for an internet connection.

Given that this certificate was installed on several systems hosting Mana Tools, it appeared that this threat actor was using XAMPP as the web server to host the Mana Tools C2 panel on Windows virtual servers.

Back to the Hostinger IP

Having identified the Hostinger IP as a common destination for MySQL traffic from several Hagga C2s, we needed to find more evidence to connect Hagga to the cPanel server. As stated earlier, given the possibility that the cPanel IP is shared amongst multiple Hostinger customers, this was difficult to achieve based on threat telemetry alone. To aid this process, we used insight derived from MalBeacon, in addition to further Passive DNS data.

Note: MalBeacon is a revolutionary system that can attribute malware campaigns to the threat actor themselves through proprietary pixel tracking technology. If you haven't heard of it before, I urge you to check it out.

MalBeacon data identified several actor IPs in the vicinity of Lahore, Pakistan, associated with the C2s 69.174.99.181 and 64.188.20.198.

Timestamp	Actor IP	C2 Domain	Cookie ID
11/26/21 11:31	42.201.155.21	update.newbotv4.monster	bs5f8f8coj22sfdthf23nkmumj
11/26/21 11:32	42.201.155.21	69.174.99.181	bs5f8f8coj22sfdthf23nkmumj
11/26/21 11:34	42.201.155.21	69.174.99.181	NA
11/29/21 16:20	42.201.155.40	update.newbotv4.monster	bs5f8f8coj22sfdthf23nkmumj
12/1/21 15:31	42.201.155.40	update.newbotv4.monster	bs5f8f8coj22sfdthf23nkmumj
12/2/21 19:43	42.201.155.40	64.188.20.198	bs5f8f8coj22sfdthf23nkmumj
12/2/21 19:43	42.201.155.40	64.188.20.198	bs5f8f8coj22sfdthf23nkmumj
12/2/21 19:46	42.201.155.40	64.188.20.198	bs5f8f8coj22sfdthf23nkmumj

Table 3: Malbeacon data

Whilst examining threat telemetry data for the Hostinger IP, we found cPanel management traffic to TCP/2083 from the actor IP 42.201.155.21 on 26 November 2021 and from 42.201.155.40 between 02 December 2021 and 03 December 2021. This activity aligned with the dates the IPs were associated with the Hagga C2s.

We also identified resolutions in passive DNS data that connect the newbotv4.monster and statusupdate.one domains to Hostinger.

Name Queried	Response
statusupdate.one	109.106.251.97
cpcontacts.newbotv4.monster	109.106.251.97
webdisk.newbotv4.monster	109.106.251.97
cpanel.newbotv4.monster	109.106.251.97
cpcalendars.newbotv4.monster	109.106.251.97
webmail.newbotv4.monster	109.106.251.97
autodiscover.newbotv4.monster	109.106.251.97

Table 4: Hostinger PDNS Results

Whilst the response IP differed from the Hostinger IP address seen in the outbound TCP/3306 connections, it aligned with the processes of leasing a cPanel VPS with Hostinger.

When a user purchases their cPanel account through Hostinger, they are asked to add the domain that they are seeking to host on the account to start the service. Once that domain is added, Hostinger assigns several default hostnames to the domain that resolve to a second IP address, which differs from the cPanel management IP first provided. These default hostnames are what are detailed in Table 4.

The cPanel management IP can continue to be used for access to the web server control panel, or as an endpoint for a MySQL database.

Continued Observation of Hostinger IP

By continuously monitoring threat telemetry for the Hostinger IP and examining X.509 certificates and URL requests for new MySQL clients, we were able to identify additional related C2 infrastructure within hours or days of them being stood up.

- 103.151.122.110 (VNPT-AS-VN, VN)
- 72.11.157.208 (QuadraNet, US)
- 192.154.226.47 (Reprise Hosting, US)
- 64.188.21.227 (QuadraNet, US)
- 72.11.143.125 (QuadraNet, US)
- 72.11.143.47 (QuadraNet, US)
- 207.32.217.137 (1G Servers, US)
- 194.31.98.108 (PREFIXBROKER, NL)
- 103.133.105.61 (VNPT-AS-VN, VN)
- 78.138.105.142 VELIANET-FR-PINETLLC, FR)
- 103.153.77.98 (VNPT-AS-VN, VN)

Additionally, we were able to identify an upgrade to the Mana Tools C2 panel.

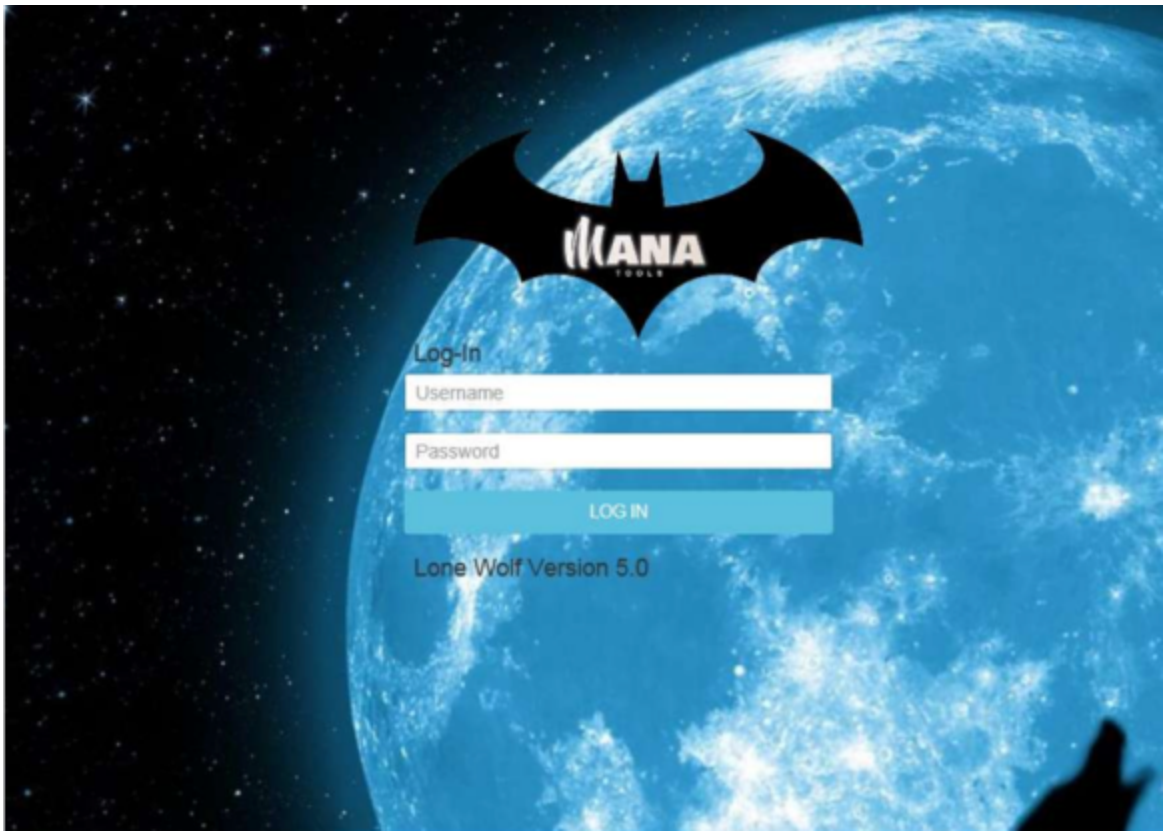


Figure 5: New Mana Tools C2 Panel

We revisited MalBeacon to examine beacon data for the newly discovered C2 domains and IP addresses to enumerate associated activity. We subsequently identified several ‘new’ adversary IPs in the vicinity of Lahore, Pakistan. These IPs were observed in

communications with the Hostinger IP during the same timeframe they were associated with the Hagga C2 panels.

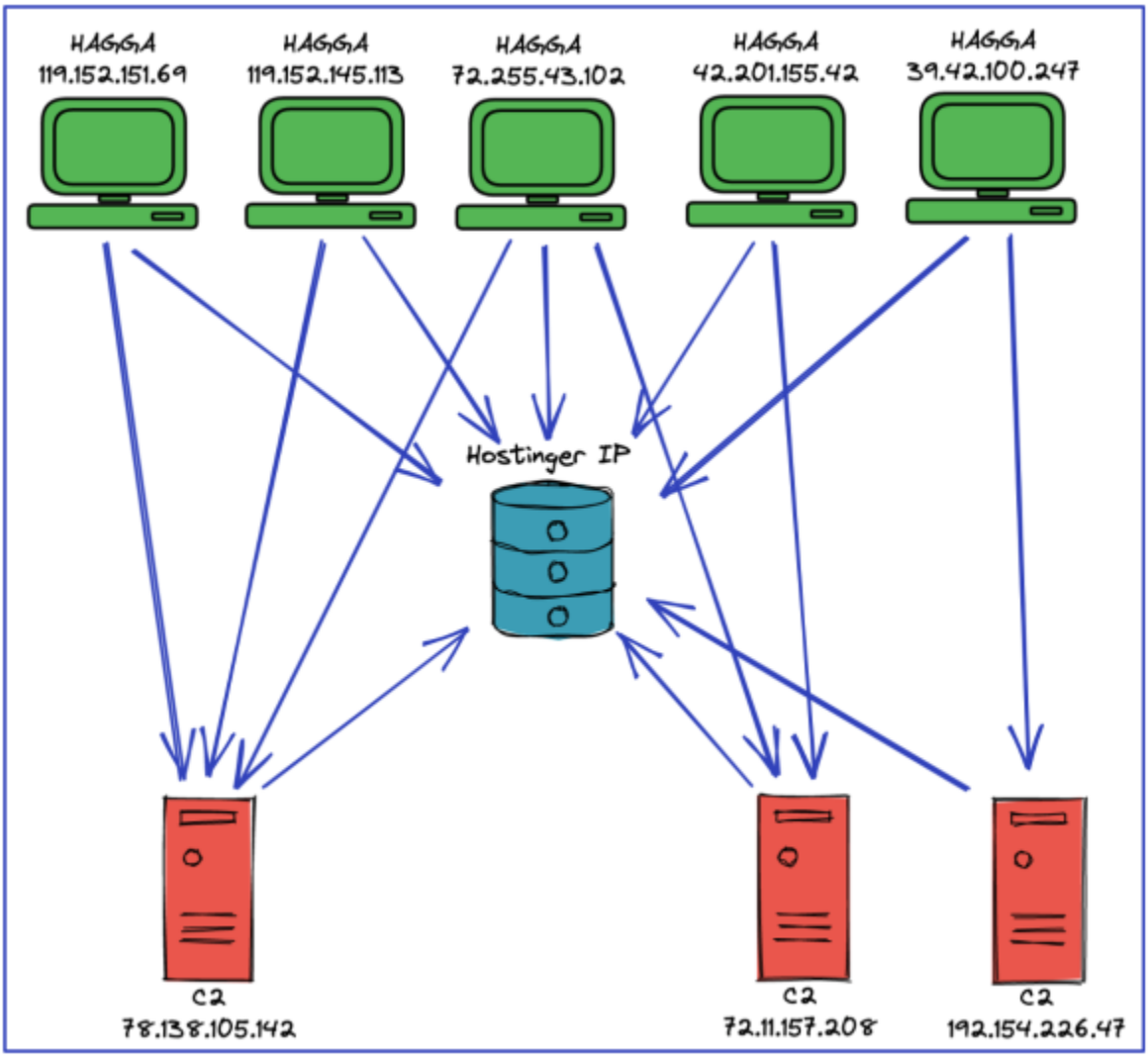


Figure 6: Hagga Activity

Conclusion

From the starting point of an IP address (69.174.99.181) associated with an Agent Tesla command and control server, it was possible to pivot and identify a backend server hosting a MySQL database operated by the threat actor Hagga. From this point a further pivot led us to the identification of additional C2s hosting the Mana Tools C2 panel along with a common certificate that can be used to increase confidence in attributing future infrastructure to this threat actor.

Indicators of Compromise

IP Addresses

- 103.151.122.110
- 72.11.157.208
- 192.154.226.47
- 64.188.21.227
- 72.11.143.125
- 72.11.143.47
- 207.32.217.137
- 194.31.98.108
- 103.133.105.61
- 78.138.105.142
- 103.153.77.98
- 69.174.99.181
- 161.129.64.49
- 155.94.209.50
- 64.188.27.104
- 64.188.20.198

Domains

- mobibagugu.duckdns.org
- mobibanewdan.duckdns.org
- mohbeebnew.duckdns.org
- mubbibun.duckdns.org
- cdec22.duckdns.org
- vncgoga.duckdns.org
- bakuzamokala.duckdns.org
- warnonmobina.duckdns.org
- abotherrdpajq.duckdns.org
- mobinomomuam.duckdns.org
- workflowstatus.live
- heavy-dutyindustry.shop
- microsoftiswear.duckdns.org
- update.newbotv4.monster
- newbotv4.monster
- bot.statusupdate.one