VB2020 localhost

30 September - 2 October, 2020 / vblocalhost.com

PANDAMIC: EMISSARY PANDAS IN THE MIDDLE EAST

James Shank & Jacomo Piccolini

Team Cymru, USA

james@cymru.com
jacomo@cymru.com

"A scout should learn as much as possible about enemy psychology, habits, organization, and tactics." – USMC 'Scouting and Patrolling' MCTP 3-01A

ABSTRACT

Network forensics is a well-developed discipline within the infosec industry. But what happens when you apply that tradecraft to global network visibility?

For more than a year, we concentrated our efforts on tracking the infamous APT27 group of actors. What we found is compelling! Much like pandas leaving paw prints in the snow and other clear signs of their presence that trained observers are able to spot, the Emissary Panda actors leave many traces behind that analysts can use to watch their movements.

For a while, APT27 (a.k.a. Emissary Panda, TG-3390, BRONZE UNION, Iron Tiger, LuckyMouse) has been busy conducting operations targeting the Middle East. These threat actors have exhibited some operational security awareness, which minimizes certain analysis possibilities. Despite their attempts to hide, we found evidence showing communications with victims in the energy, health care, technology, education, travel and government sectors.

These threat actors leave fingerprints and trails that we have been able to uncover through network forensics. Our global Internet traffic analysis shows an extensive and well-designed infrastructure that has evolved over time. In this paper, we will reveal the group's fingerprints and highlight an impressive infrastructure. We have uncovered exfiltration paths, control infrastructure, and what appears to be a migration from one hosting provider to another.

In an unexpected and unusual announcement in December 2019, the Iranian government tweeted publicly claiming they had 'foiled' an attack by 'the well-known APT27' – but is this really the case? This paper will add to the story by showing the before, during and after impacts on the APT27 infrastructure around the time of the Iranian public statement.

In summary, we will reveal intimate knowledge of enemy infrastructure and behaviours, allowing practitioners to achieve cyber field awareness. We present network infrastructure mapping that may reveal the APT27 actor's battle plans. We will describe the scouting and detection methods we used to determine this infrastructure, as well as some defensive techniques network operators can employ to defeat these attacks.

Pandas are not native to the Middle East, and despite their best efforts to hide their espionage campaign and exfiltration activities, we have been able to track their tell-tale trails as they sneak through the corners of the Internet.

AECERT'S JUNE 2019 REPORT

Securing the Internet as a whole takes a collaborative effort. Both public and private sector researchers contribute greatly to the shared understanding of the threats we all face from APT actors and others. Like others, we use these reports, bulletins and publications to help build our knowledge and understanding of these threats.

We regularly monitor reports from many different sources to help us to stay on top of online threats. Like all major threat actor campaigns, APT27 has been on our radar for a long time. We often find reports that can be enriched to create a more complete picture of actor activity, through an analysis of the entire cyber field and Internet-scale visibility. These reports become a useful seed from which we can map out actor infrastructure beyond first hops, improve surveillance of actor activity, and add context that increases situational awareness. In many instances, *Team Cymru* is able to see more, know more, and understand more of the activity than the original report reveals. This story covers one such occasion.

On 13 June 2019, aeCERT, the Computer Emergency Response Team of the United Arab Emirates, published a bulletin titled 'Advanced Notification of Cyber Threats against Family of Malware Giving Remote Access to Computers' [1]. This report warned of an active and ongoing malware campaign and provided a list of several indicators of compromise. It also gave sound advice regarding ways to mitigate the impact and defend networks against this campaign activity.

The network indicators from the aeCERT report are reproduced in Table 1, augmented to include the originating network for each address.

aeCERT's report noted the use of HyperBro, a remote access trojan (RAT) that has previously been identified by other cybersecurity organizations [2]. HyperBro remains resident in memory and is loaded through side-loading the DLL [1]. These communication methods support RAT-like functions and VPN-like capabilities over encrypted channels. According to aeCERT's report, the inside tunnel addresses were non-routable IPs, suggesting that the attackers were using tunnels to reach their victims.

The aeCERT report identifies a new variant within the HyperBro family called HyperSSL. This tool is said to side-load an encrypted payload that is then decrypted and executed in memory [1]. It uses PolarSSL (now called mbed TLS [3]), which aeCERT observed operating over port 443 [1]. aeCERT's report also identified TCP port 4550 as the port used by HyperSSL to connect to the control servers.

We also note that some other reports have overlapping indicators with HyperBro and HyperSSL, calling it by another name. A presentation by *FireEye*'s *Mandiant* names a tool 'FOCUSFJORD', and we noted that the registry key signatures (the appending of '-ll37389743nxshkhjhgee') overlaps with HyperSSL signatures [4, 6].

IP address	Network AS and name
10.69.0.176 192.168.4.26 192.168.1.237	Unrouted RFC1918
202.179.0.142 202.179.5.161	AS 9934 - MICOM-MN-AS Mongolia Telecom, MN
138.68.133.211 104.248.169.149 134.209.88.107 138.68.154.133 139.59.67.212 139.59.82.32 142.93.219.48 142.93.233.195 159.89.168.83 178.128.202.249 206.189.123.156 209.97.171.8	AS 14061 - DIGITALOCEAN-ASN, US
203.91.119.4	AS 24559 - GMOBILE-MN G-Mobile Corporation, MN
103.224.80.86	AS 55933 - CLOUDIE-AS-AP Cloudie Limited, HK
185.220.59.120	AS 197328 - INETLTD, TR

Table 1: aeCERT's reported IP addresses with originating AS added.

A BRIEF NOTE

We do not wish to further victimize the targets of APT actors or other threat actor groups. Within this paper, we do not mention any victims by name or by identifying resource. All IoCs contained within this paper are believed to be owned and used solely by the threat actors during the time period identified. We show IoCs inline during discussions of the timeline where relevant. The infrastructure is very dynamic and many of the IoCs mentioned throughout are no longer active. An overview of recent IoCs is available in the IoCs section at the end of this paper.

As with all reports of reconnaissance of actor infrastructure, this paper is based fully on the data *Team Cymru* holds and can access. This paper reflects a comprehensive portrayal of what is known, but as with all data, it is subject to observation bias that may underrepresent the totality of the APT27 actor infrastructure and activity. We would welcome the chance to compare our notes with the APT27 actor's internal notes, but we are unlikely to get the chance to do so. We believe that this paper reflects the most informed available understanding of the APT27 infrastructure and overall activity outside of APT27's own data.

THE SUMMER OF 2019

Starting from the aeCERT report's indicators, how does one achieve the state of cyber field awareness – that deep understanding of enemy operations that enables a tactical defence to stop the threat today and tomorrow?

Team Cymru's roots are in the deep technical knowledge of how the Internet works, applied to interpreting network metadata through the lens of threat intelligence practice. Today, we still gather and collect many different types of indicators that allow us to see what others cannot and do not.

Taking the indicators from aeCERT's report and comparing them against our data holdings, we see network communications and other indicators that allow us to map out the infrastructure of the APT27 actor group. We also found an X.509 certificate being served by some of the hosts, which is shown in Table 2. It is convenient that the naming suggests a possible use for the certificate.

Common name	domain.com
O	VPN
Subject	CN=domain.com, O=VPN
NotAfter	2028-12-30 01:55:37
NotBefore	2019-01-02 01:55:37
SHA1	6B:10:79:40:80:A1:55:3A:08:76:76:09:5D:05:4F:16:08:94:A2:4B
Issuer	CN=VPN CA, O=Work

Table 2: First X.509 certificate observed.

To enrich our understanding of the actor infrastructure, we performed our initial analysis based on network metadata. Table 3 shows the original aeCERT report indicators that were still active at the time of our analysis and the new associated systems found within *Team Cymru* network data.

aeCERT IoCs [1]	Hosts talking to aeCERT IoCs
104.248.169.149	223.12.171.71
134.209.88.107	223.12.172.63
138.68.154.133	223.12.224.122
139.59.67.212	223.12.224.20
139.59.82.32	47.244.134.234
142.93.219.48	47.244.159.87
159.89.168.83	47.244.161.239
178.128.202.249	47.244.227.84
206.189.123.156	47.244.29.164
209.97.171.8	47.244.57.48
	47.52.211.201
	47.52.226.143
	47.52.39.161
	47.89.31.25
	47.91.206.33

Table 3: aeCERT IoCs with additional associated hosts.

Combining all of our initial indicators after the first set of pivots from further analysis of network communications allowed us to create a map showing a far more extensive infrastructure than the aeCERT paper detailed.

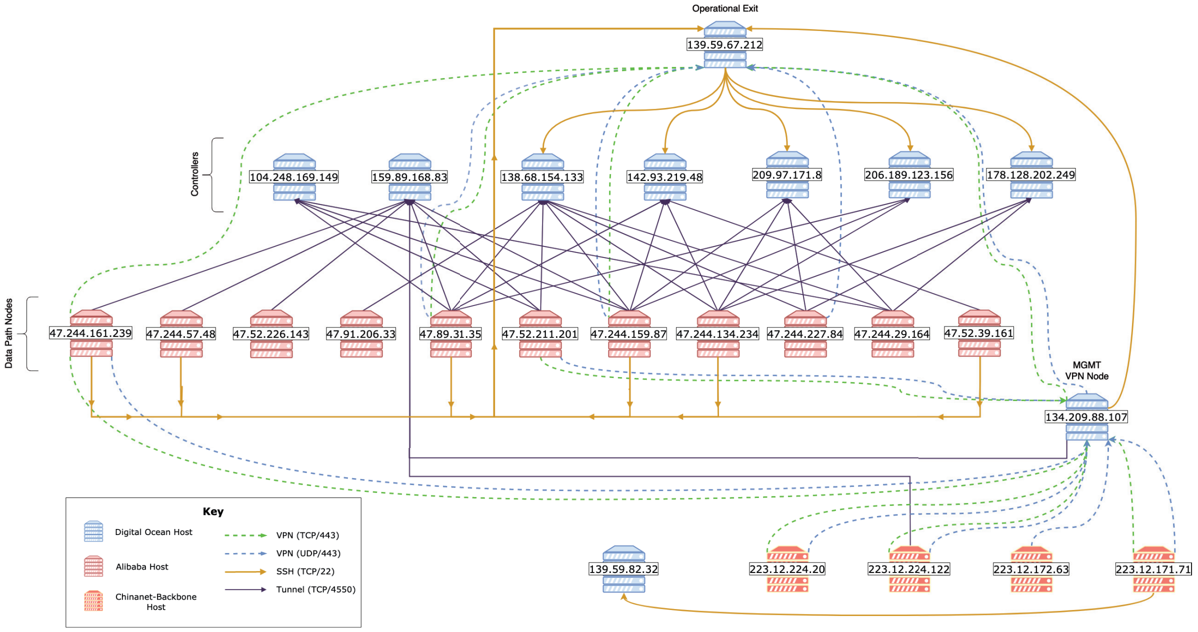


Figure 1: Observed actor infrastructure up to August 2019.

Mapping out the enemy positions is a vital part of military scouting. In the digital space, understanding the infrastructure used by malicious actors is essential to systematic defence and getting ahead of the next round of attacks. To help with the understanding the systems discussed from this point forward, it will be helpful to define a few terms.

Malware communication	Victim connections by HyperBro and variants to controllers, connecting over TCP/443.
Management (MGMT) VPN node	Listen for connections, expose observed X.509 certificates, part of the tunnelling infrastructure, over TCP/443 and UDP/443.
Data path node	Connect to controllers, believed to be used to collect exfiltrated data, part of the tunnelling infrastructure.
Operational node	Systems used for forward activity such as reconnaissance, exploiting targets, and configuring infrastructure.

Table 4: Definition of terms used.

We can see that, during the summer of 2019, the actors established a network topology with multiple paths between nodes. Starting closest to the actors, we see connections from *Chinanet Backbone* or *Alibaba* establishing tunnels to the management VPN nodes at *DigitalOcean*. From these, they create tunnels to operational nodes, which they use to SSH into the malware controllers. These malware controllers receive victim communications, but also establish tunnels to what we believe to be data exfiltration nodes. This configuration is complex and we believe it is intended to hide the attackers' origins from their victims, while also providing redundancy and fault tolerance.

The fact that the actors have set up and are operating this level of infrastructure gives an indication of their sophistication and the value of these attacks for APT27. We believe the actors use distinct paths for management purposes and data exfiltration. The management VPN path is used to connect to operational nodes. These operational nodes are used for configuring and maintaining infrastructure, reconnaissance of targets, and exploiting targets. The data exfiltration tunnel path is used for carrying traffic from malware controllers back towards the actors. The use of distinct paths for different purposes is part of the group's operational security awareness.

We noted the significance of 139.59.67.212 to the actor infrastructure. This host, an operational node, showed what we believe to be VPN connections inbound from higher order infrastructure and SSH sessions outbound to command-and-control servers. We also see indicators consistent with target reconnaissance (HTTP/HTTPS) outbound from this host. The first X.509 certificate we observed was live on this host from April 2019 to June 2019. Based on the network activity of this host, it seems that this system is used by the actors for management and forward compromise activity.

The actors used 134.209.88.107 during this phase as a management VPN node for receiving and creating VPN connections. We see inbound UDP and TCP port 443 traffic coming to this host, as well as some outbound UDP and TCP 443 connections from this host to both *DigitalOcean* and *Alibaba* hosts. This host also hosted the first X.509 certificate observed from April 2019 to July 2019. This is the main host we observe *Chinanet Backbone* hosts connecting to at the time, but we also see some connectivity between *Chinanet Backbone* and 159.89.168.83.

We see a wide variety of targets within this initial data analysis, showing victim malware communications connecting back to the controllers via TCP port 443. These indicators of successful execution of the malware on many different victim networks is present throughout our monitoring. We include basic victim demographics at the end of this report, keeping with our policy of protecting victims from further victimology.

LITTLE IS STATIC BETWEEN SUMMER AND FALL

As with the changing of the leaves from vibrant green to hues of red, orange and yellow, so too do the resources used by threat actors change. Sometimes these changes have predictable frequency or signals that reveal details of their preferences or operational security. Starting around September 2019, we observe several changes in the operational hosts, the providers used, and some of the patterns of network communication.

These changes all took place well after the publication of the aeCERT notice. It was not clear to us at this time what prompted the significant changes to the actor infrastructure and communications patterns. Prior to this, we had not observed a similar change in infrastructure.

Most notably, we observe significant changes in active hosts and network fingerprints. Many of the former *DigitalOcean* hosts were no longer active. We noted a significant reduction in TCP port 4550 traffic. We see the actors moving fully to using port 55781 for network communications, having previously used port 4550. We also note a significant change, seeing the actors introduce a second X.509 certificate into their infrastructure, shown in Table 5.

Common name	domain.com
O	VPN
Subject	CN=domain.com, O=VPN
NotAfter	2029-08-23 01:53:45
NotBefore	2019-08-26 01:53:45
SHA1	43:CD:54:4A:01:8F:29:56:A3:3E:D6:55:1E:ED:85:DC:26:05:9D:62
Issuer	CN=VPN CA, O=Work

Table 5: Second X.509 certificate observed.

Our data shows this certificate in use by nine hosts during September 2019. These hosts, along with the initial observation dates, are shown below.

IP address	**ASN**	**First seen**
47.56.102.6	Alibaba, HK	2019-09
47.75.124.161	Alibaba, HK	2019-09
47.90.97.10	Alibaba, HK	2019-09
47.254.233.126	Alibaba, MY	2019-09
47.244.146.7	Alibaba, HK	2019-09
139.162.98.149	Linode, LLC, JP	2019-09
47.56.183.184	Alibaba, HK	2019-10
47.52.39.167	Alibaba, HK	2019-10
47.56.176.33	Alibaba, HK	2019-10

Table 5: Host addresses observed serving second X.509 certificate.

This new X.509 certificate uses an identical Subject (CN=domain.com, O=VPN) and Issuer (CN=VPN CA, O=Work) to those used by the previous certificate. This certificate is observed on hosts at a hosting provider (*Alibaba*) already known to be a favourite of this threat actor, which increases our confidence that this is the same threat actor group.

The network behaviours of the hosts using this certificate show similarities to the hosts already established as part of the APT27 infrastructure. Several of the hosts showing the new X.509 certificate are seen making UDP port 443 connections to a management VPN node we see hosting the old X.509 certificate: 68.183.94.205.

Taking into consideration everything we know at this point, we are able to create a view of the APT27 infrastructure in September 2019, which is shown in Figure 2.

A SHIFT TOWARDS LINODE

By September 2019, we noted that the actors were using *Linode* hosts for more of their infrastructure. While we had observed hosts within *Linode* being used by the actors before, in September there was a drastic change towards *Linode*. Given the introduction of substantial *Linode* infrastructure, we theorized at this point that the actors may have been shifting from preferring *DigitalOcean* to preferring *Linode*. We later see them using both *Linode* and *DigitalOcean*, changing our understanding of this initial move from a change in preference to a diversification of their cloud posture.

LATE FALL 2019

With time, the patterns become more concrete and observations gain more confidence. Previously, we had noted TCP port 4550 traffic dropping to zero. TCP port 4550 activity was not observed throughout this reporting period (nor up to the time of writing this paper), and TCP port 55781 activity continued. The second X.509 certificate (see Table 5) was seen on more

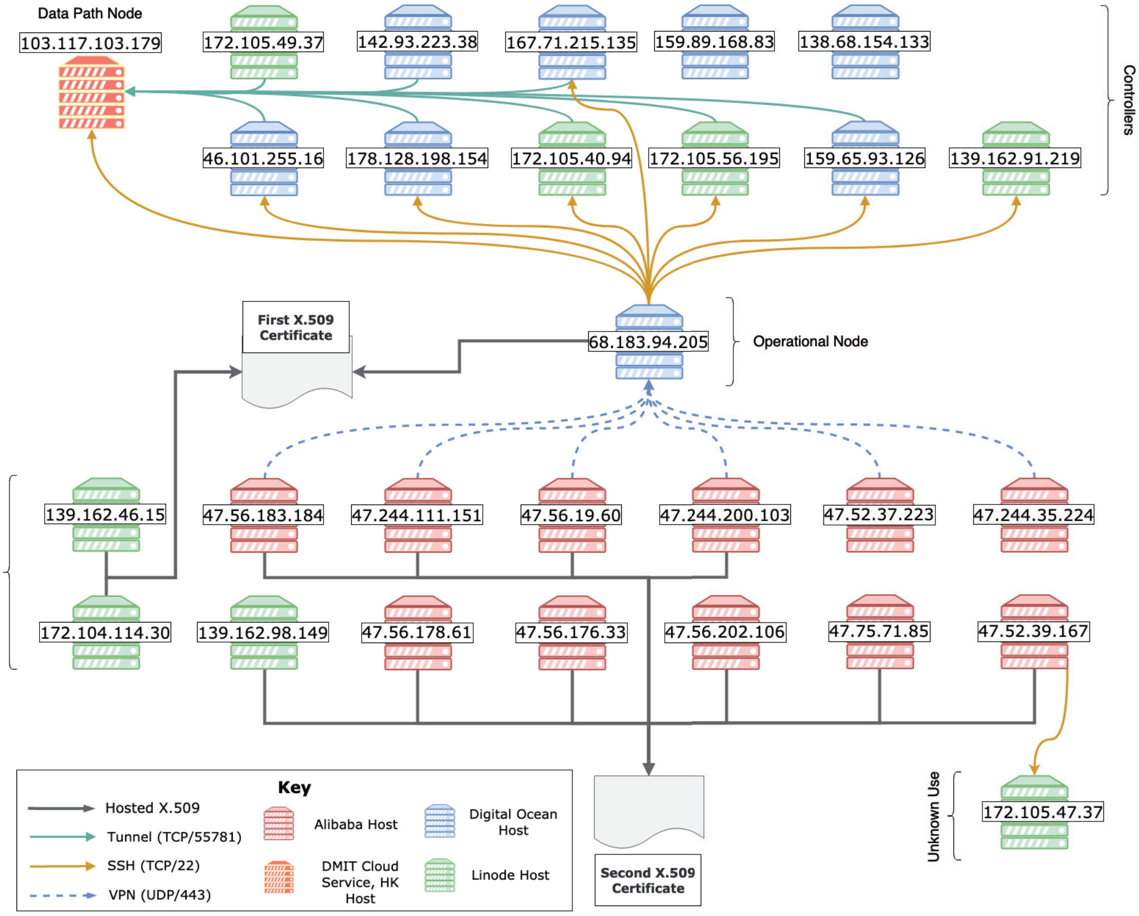


Figure 2: Observed actor infrastructure from September 2019.

hosts. We saw ten in total, four of which overlapped with hosts observed in previous periods, but we also noted that five previously observed hosts were no longer serving the second X.509 certificate. Only three previously observed hosts were seen using the first X.509 certificate (see Table 2). These certificate changes are shown in Table 6, reflecting the observations current as of November 2019.

IP address	ASN	X.509	First Seen	Last Seen
68.183.94.205	Digital Ocean, LLC, US	First	2019-07	2019-11
172.104.114.30	Linode, LLC, US	First	2019-07	2019-11
139.162.46.15	Linode, LLC, US	First	2019-08	2019-11
139.162.98.149	Linode, LLC, JP	Second	2019-09	2019-11
47.56.19.60	Alibaba, HK	Second	2019-10	2019-11
47.75.71.85	Alibaba, HK	Second	2019-10	2019-11
47.244.200.103	Alibaba, HK	Second	2019-10	2019-11
47.244.111.151	Alibaba, HK	Second	2019-10	2019-11
47.52.116.124	Alibaba, HK	Second	2019-11	2019-11
47.91.222.81	Alibaba, HK	Second	2019-11	2019-11
47.75.13.135	Alibaba, HK	Second	2019-11	2019-11
47.91.221.5	Alibaba, HK	Second	2019-11	2019-11

Table 6: X.509 certificates observable in November 2019.

Using the overlaps of tracking all the indicators we have thus far established on these actors, we are able to update our understanding of their network topology.

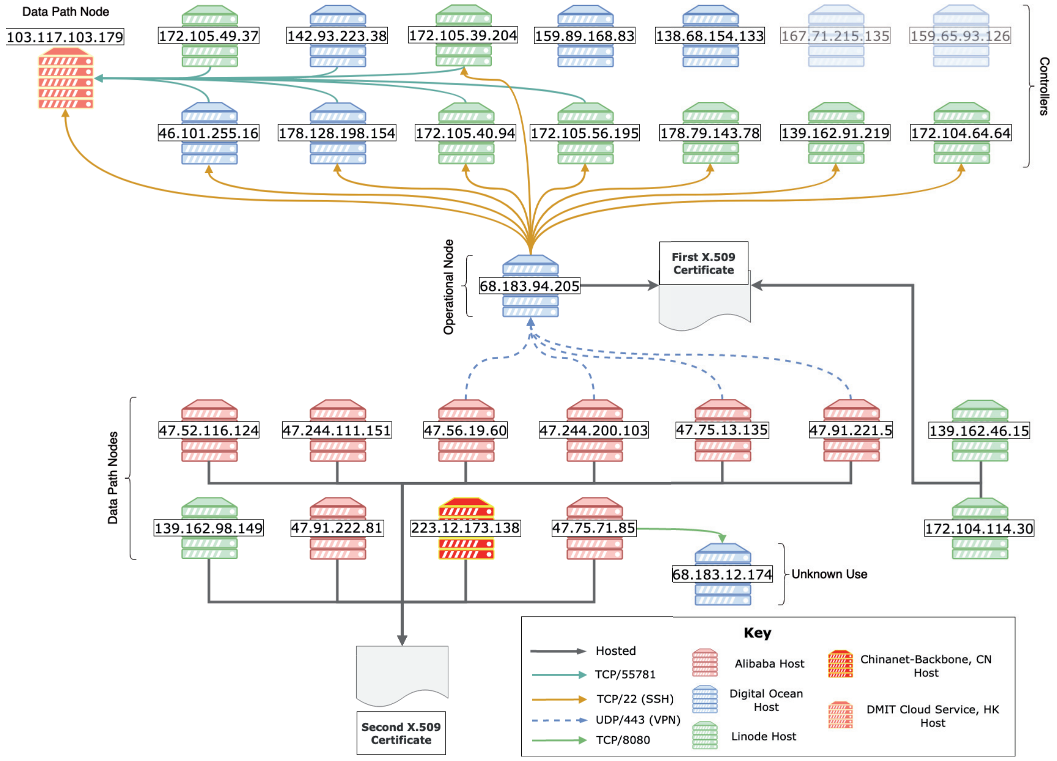


Figure 3: Observed actor infrastructure November 2019.

AN ACTIVE DECEMBER 2019

December 2019 introduced some changes into the ongoing relationship between the threat actors and one of their victims. There was also a significant increase in activity in terms of infrastructure changes. Using the techniques we've been applying throughout this report, we are able to update our early December 2019 data points to create the following view of the infrastructure:

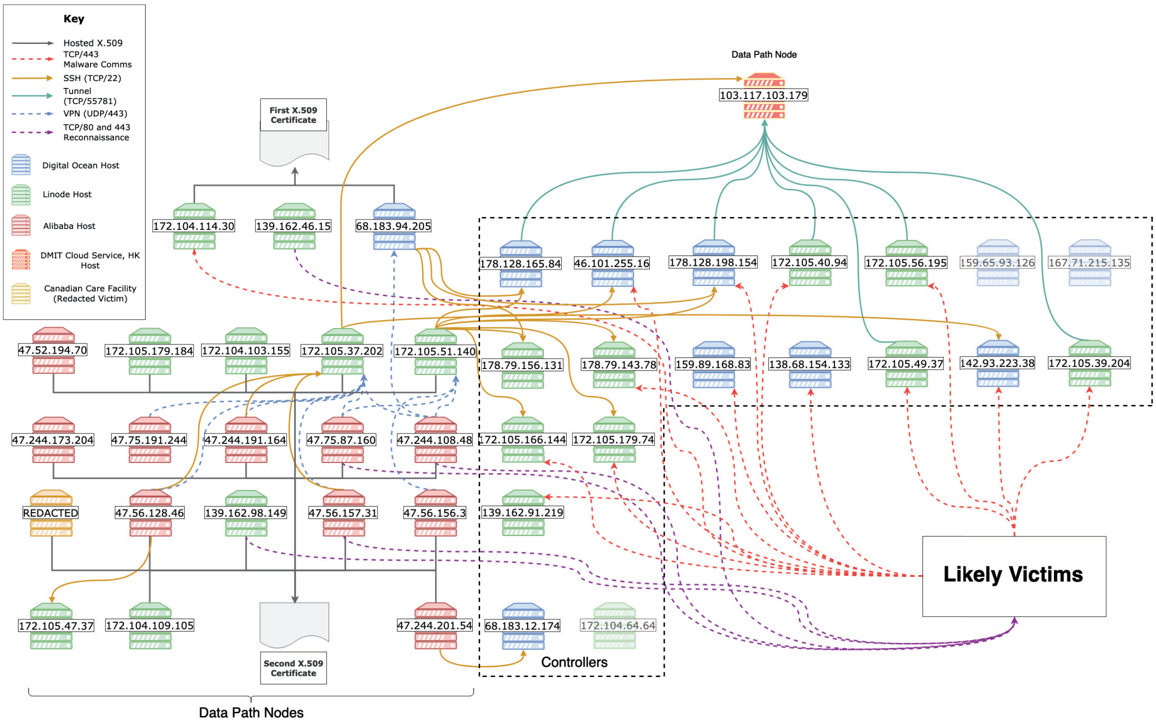


Figure 4: Observed actor infrastructure early December 2019.

At this point, we noted a pronounced shift in utility between *DigitalOcean* hosts and *Linode* hosts. In particular, *DigitalOcean* host 68.283.94.205, which was previously observed to be a significant operational node, diminished in use during this timeframe. We saw these functions shifting to *Linode* hosts 172.105.37.202 and 172.105.51.140. *Linode* appears to be the favoured hosting provider, along with *Alibaba*, in December 2019. This data is compatible with our previous speculation of a shift to *Linode* and away from *DigitalOcean*.

In early December 2019, we saw two hosts (both previously identified) serving the first X.509 certificate observed. For the second X.509 certificate observed we saw 16 hosts. This was the highest count to date for hosts configured to serve these X.509 certificates. We also saw a host at *Alibaba*, 47.56.156.3, serving the second X.509 certificate observed via TCP port 8443. Until this point, we had not seen either certificate hosted on ports other than 443.

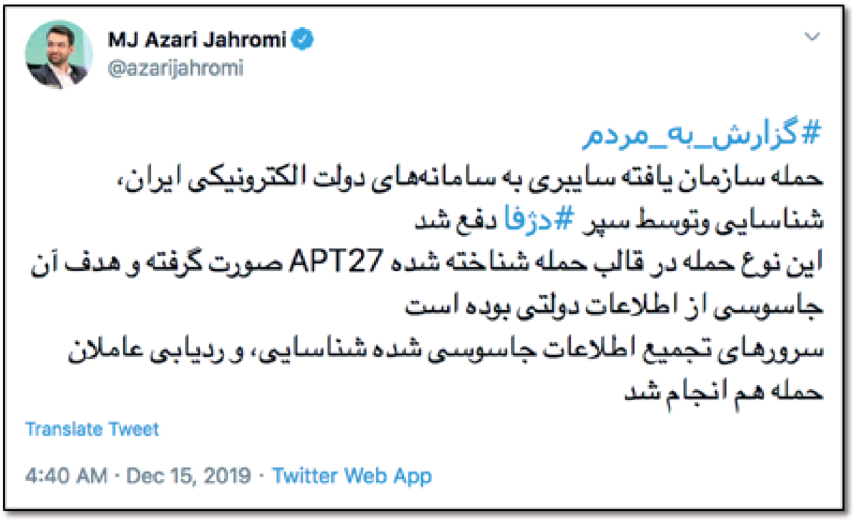
This timeframe reveals an oddity. A private Canadian long-term care facility or nursing home was introduced into the infrastructure, not as a victim but rather was used by the threat actors as a VPN node. This was the first time we observed the introduction of a non-hosting provider system into the infrastructure. We noted what appeared to be web browsing compatible with target reconnaissance from this host.

We believe this host was compromised, as our data shows the host to have been vulnerable. We are not certain why this host was incorporated into the infrastructure. One possibility is that the systems were provisioned by a different group within the APT27 actor hierarchy, and this system may have been put on the wrong list when handed to a team building out the next infrastructure. Alternatively, and more simply, it could have been added in an attempt to make their browsing stand out less for networks monitoring for user-like behaviours exhibited by data centre hosts.

AND NOW FOR SOMETHING COMPLETELY DIFFERENT

Twitter has become a preferred platform for political messaging and sees increasing use by politicians to express all forms of announcements, sentiments, and policy altering decisions. Most tweets do not influence or change the course of most APT group activity. But some do.

In Figure 5, we show a tweet from MJ Azari Jahromi (@azarijahromi), Iranian Minister of Communications and Technology. This tweet says that Iran has found 'Foreign spying malware on their government servers,' that the Ministry attributes to the 'well-known APT27'. This tweet was posted on 15 December 2019.



MJ Azari Jahromi
@azarijahromi

#گزارش_به_مردم
حمله سازمان یافته سایبری به سامانه‌های دولت الکترونیکی ایران،
شناسایی وتوسط سپر #دژفا دفع شد
این نوع حمله در قالب حمله شناخته شده APT27 صورت گرفته و هدف آن
جاسوسی از اطلاعات دولتی بوده است
سرورهای تجمیع اطلاعات جاسوسی شده شناسایی، و ردیابی عاملان
حمله هم انجام شد

Translate Tweet

4:40 AM · Dec 15, 2019 · Twitter Web App

Figure 5: Tweet by Iranian Minister of Communications and Technology.

Sometimes, it is hard to know the impact of these sorts of announcements. But Internet-scale visibility allows us to analyse the changes in the actor infrastructure following this tweet.

Within just two days of this tweet, by the end of 17 December 2019, we see substantial changes. 103.117.103.179 played a significant role in the actor infrastructure between September 2019 and December 2019 as a data exfiltration node, receiving TCP port 55781 connections from multiple controllers. It appears to be inactive after 17 December 2019. We do not see another host taking over the role of this host. It is possible that this infrastructure was retired in direct response to MJ Azari Jahromi (@azarijahromi)'s tweet.

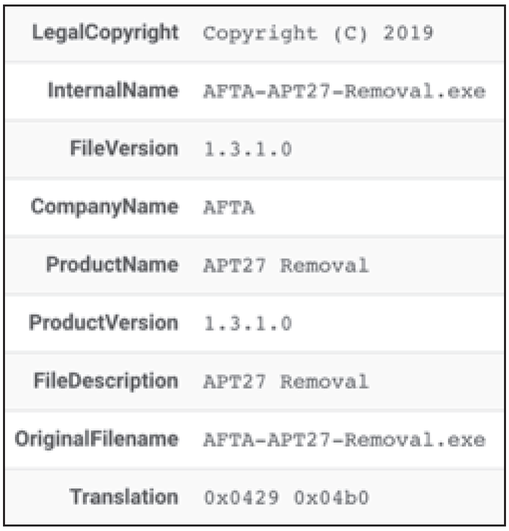
After 17 December 2019, we see a very significant reduction in TCP port 443 traffic to Iranian-based victims. Notably, several controllers no longer communicate with Iranian-based victims. We observe a general reduction in management activity. Reductions Iranian-based victim communications held through January 2020, with no data showing APT27 activity with Iranian government resources. Prior to this time, Iranian government resources were a significant target for these threat actors.

AND SOMETHING ELSE COMPLETELY DIFFERENT

Cyber field awareness involves full-scale awareness, understanding both attacker activity and resources as well as defender activity and resources. As we noted previously, we see what we believe to be a significant change in network activity around the same time as the tweet confirming some compromise of Iranian infrastructure. But was this reduction due to the threat actors changing their patterns of behaviour or due to the defenders developing better detection or remediation techniques?

HyperBro, as discussed here in more detail from the aeCERT report [1] and the LuckyMouse paper [2], is the malware component of the actor infrastructure. The pattern of compromise is to use several different means to gain access to systems [5, 6], followed by the installation of HyperBro (and/or the HyperSSL variant). These tools have known fingerprints, one of which is to create a mutex name by appending the string 'Defender' to the current account name on the *Windows* machine executing HyperBro, for example 'JoeDefender' [6].

In searching through our malware holdings to find HyperBro variant samples, we found a sample using the 'Defender' style name for a mutex that did not match other characteristics of HyperBro variants (SHA1: f7979ded11e695448c24a7a8efc1ea2649f9196c). It turns out that this sample is not a variant of HyperBro, and in fact shows authorship attribution to AFTA, the Iranian Cyber Security Agency.



LegalCopyright	Copyright (C) 2019
InternalName	AFTA-APT27-Removal.exe
FileVersion	1.3.1.0
CompanyName	AFTA
ProductName	APT27 Removal
ProductVersion	1.3.1.0
FileDescription	APT27 Removal
OriginalFilename	AFTA-APT27-Removal.exe
Translation	0x0429 0x04b0

Figure 6: Version information of f7979ded11e695448c24a7a8efc1ea2649f9196c.

When sandboxing this application, we captured the start-up image which showed two logos side by side (see Figure 6). We discovered that the logos are that of *BitBaan*, an Iranian cybersecurity company (on the left), and the AFTA logo (on the right).

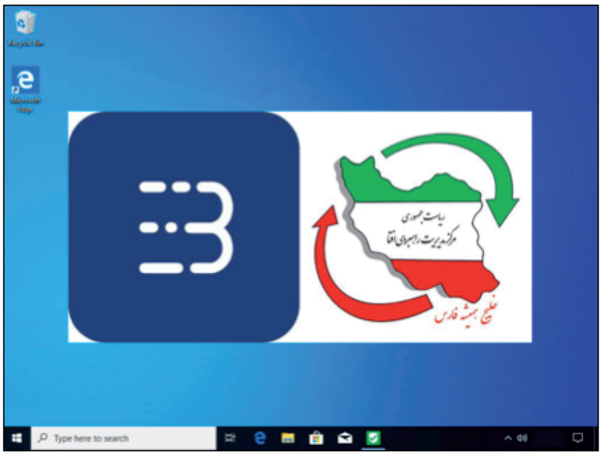
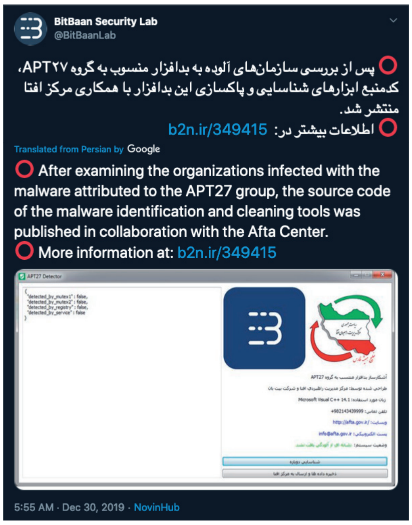


Figure 7: Cleaning tool sandbox screenshot, showing the BitBaan (left) and AFTA (right) logos.

On researching this further, and looking into *BitBaan*, we noted that they describe themselves as the first Iranian startup focused on malware analysis. We also found a tweet [7], shown in Figure 8, where they talk about the creation of this tool (and show the side-by-side logo from the sandbox execution).



BitBaan Security Lab
@BitBaanLab

⭕ پس از بررسی سازمان‌های آلوده به بدافزار منسوب به گروه APT۲۷،
کدمنبع ابزارهای شناسایی و پاکسازی این بدافزار با همکاری مرکز افتا
منتشر شد.
⭕ اطلاعات بیشتر در: b2n.ir/349415

Translated from Persian by Google

⭕ After examining the organizations infected with the malware attributed to the APT27 group, the source code of the malware identification and cleaning tools was published in collaboration with the Afta Center.
⭕ More information at: b2n.ir/349415

```
{
 "detected_by_mutex1" : false,
 "detected_by_mutex2" : false,
 "detected_by_registry" : false,
 "detected_by_service" : false
}
```

آشکارساز بدافزار منتسب به گروه APT27
طراحی شده توسط: مرکز مدیریت راهبردی افتا و شرکت بیت بان
زبان مورد استفاده: Microsoft Visual C++ 14.1
تلفن تماس: +982143439999
وبسایت: http://afta.gov.ir/
پست الکترونیکی: info@afta.gov.ir
وضعیت سیستم: نشانه ای از آلودگی یافت نشد

5:55 AM · Dec 30, 2019 · NovinHub

Figure 8: BitBaan tweet with Google Translation to English (https://twitter.com/BitBaanLab/status/1211601603519754240).

Our analysis shows this tool bundled with another application and instructions. The instructions discuss putting this tool on a network share, likely to facilitate cleaning up larger networks of compromised computers. Analysing the tool itself, we note that it searches for infections via registry keys, running processes, and mutexes known to be associated with a likely variant of HyperBro. It then removes the infection by cleaning the registry key, removing the configured service, killing the svchost.exe process running the side-loaded DLL, and removing the files from the disk. The second application analyses logs and creates summary information for review by incident responders or administrators.

Most automation takes place because a reasonably large number of repetitions of the same activity need to be performed. We believe the existence of these automated removal tools, in conjunction with *BitBaan* and AFTA, indicates a significant number of compromises of Iranian infrastructure by the APT27 actors. This assessment is supported by our forensic analysis of network data. The complete analysis of this removal tool is available in *Team Cymru*'s blog [8].

A NEW YEAR OF APT27 (JANUARY AND FEBRUARY 2020)

The coming of the new year brings with it a change in infrastructure and targeting for the APT27 actors. The decrease in overall activity seen starting after the Iranian tweet continued through February 2020. Some older infrastructure was torn down, and with it, the use of the first X.509 certificate observed ceased. We have yet to see this first X.509 certificate in use again.

We have been tracking victim connections since our first set of observations on APT27. Following the reduction in actor infrastructure and activity, the victim connections become more easily depicted in the infrastructure maps. We include victim connections in a highly summarized form to avoid further victimization of the actor's targets.

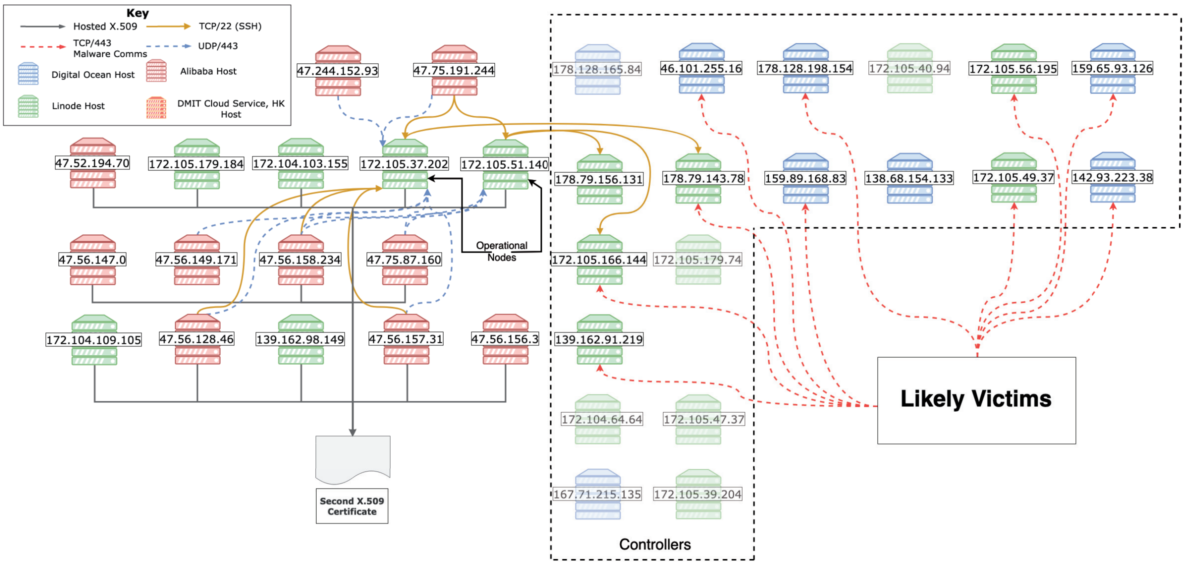


Figure 9: Observed actor infrastructure January 2020.

The February infrastructure map shows a continuation of the trend of reduced activity following the MJ Azari Jahromi (@azarijahromi) tweet (Figure 4). We do see some expansion of the total number of target countries starting in February, which may indicate a strategic decision to switch to alternate targets after being ousted by Iran. In February, the traffic to Iran (and most other targets) is more compatible with reconnaissance efforts than exploitation and data exfiltration.

The actors continue to use 172.105.51.140 and 172.105.37.202 to manage their infrastructure. We continue to observe a shift away from *DigitalOcean* as a preferred hosting platform and continue to observe provisioning of new resources at *Alibaba* and *Linode*. We see two new probable controllers (139.162.221.60 and 178.79.177.69) introduced during February, which may indicate positioning for a future return of activity.

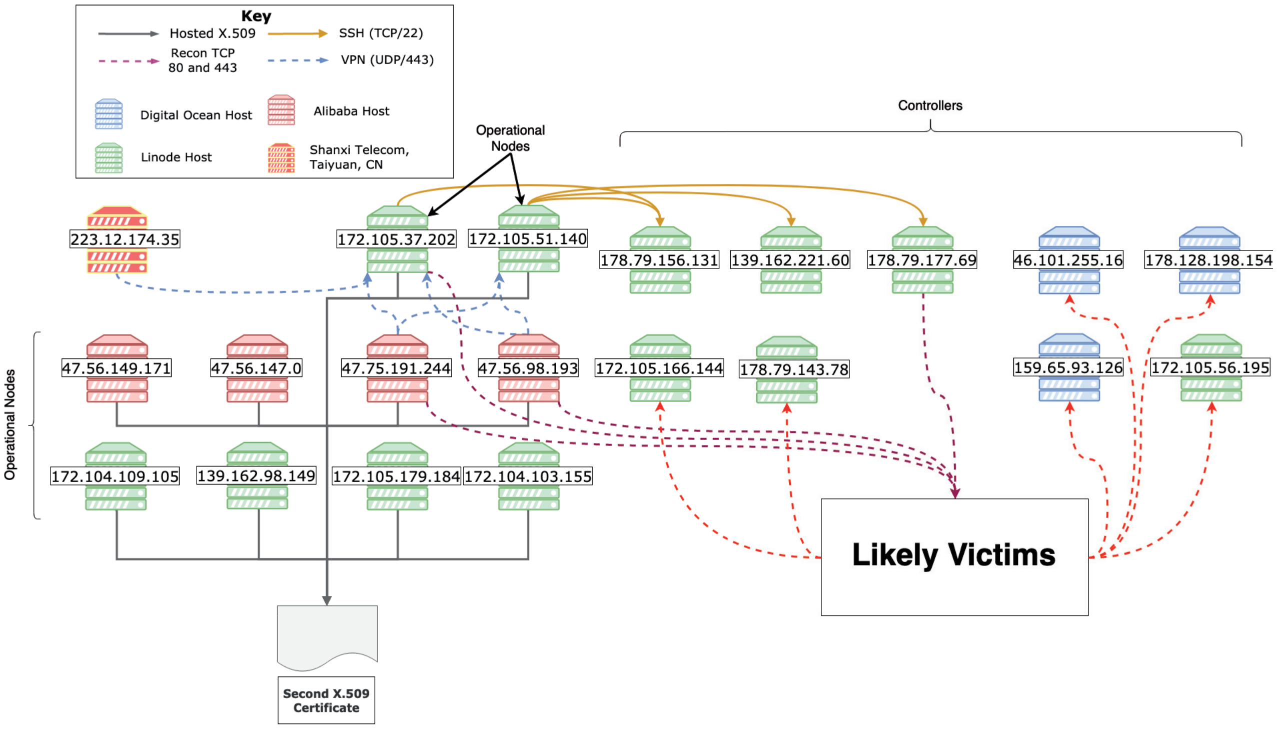


Figure 10: Observed actor infrastructure in February 2020.

A NEW SPRING

When tracking threats, and trying to obtain a state of cyber field awareness, spotting trends and changes in activity levels and patterns is essential to understanding the enemy. For the first couple months in 2020, it appears that the APT27 actors were tactically retreating, withdrawing from a very aggressive position and engaging mostly in scouting new targets. However, this retreat changes in March.

In March 2020, the APT27 actors were busy again. We see the introduction of seven new hosts serving the second X.509 certificate observed, with only three of the current hosts being observed prior to March hosting this certificate. These hosts were mostly at *Linode* (four), but now we see *DigitalOcean* hosts being provisioned again (two) and a new hosting provider introduced (*GCORE*). We observed the actors using *GCORE* resources that GeoIP data places within Russia.

We see a marked increase in the size of the active infrastructure starting in March 2020 that reverses the trend following the MJ Azari Jahromi tweet. Along with this increase, we also see a shift away from using 172.105.51.140 and 172.105.37.202 for management activities. The actors have also begun targeting Saudi Arabia to a much greater degree than previously observed. The shift to Saudi Arabia as a target began in February, but the sustained shift and traffic levels through March makes it clear that this shift is a prominent focus for the actors. We see SSH sessions from 66.175.218.50 and from 47.56.254.96 in March and through April, indicating that these systems may be taking over the role previously occupied by 172.105.51.140 and 172.105.37.205. We will continue to monitor these hosts over the subsequent months. Figure 11 shows the observed actor infrastructure during March 2020.

THE RETURN TO PERSIA

April 2020 shows the continued use of 66.175.218.50 and 47.56.254.96 for management activity, both of which are observed SSH'ing into two hosts each. No new controllers are found during this period, but we do see a continued focus on Saudi Arabia. This month, we see 15 distinct hosts across four providers serving the second X.509 certificate observed.

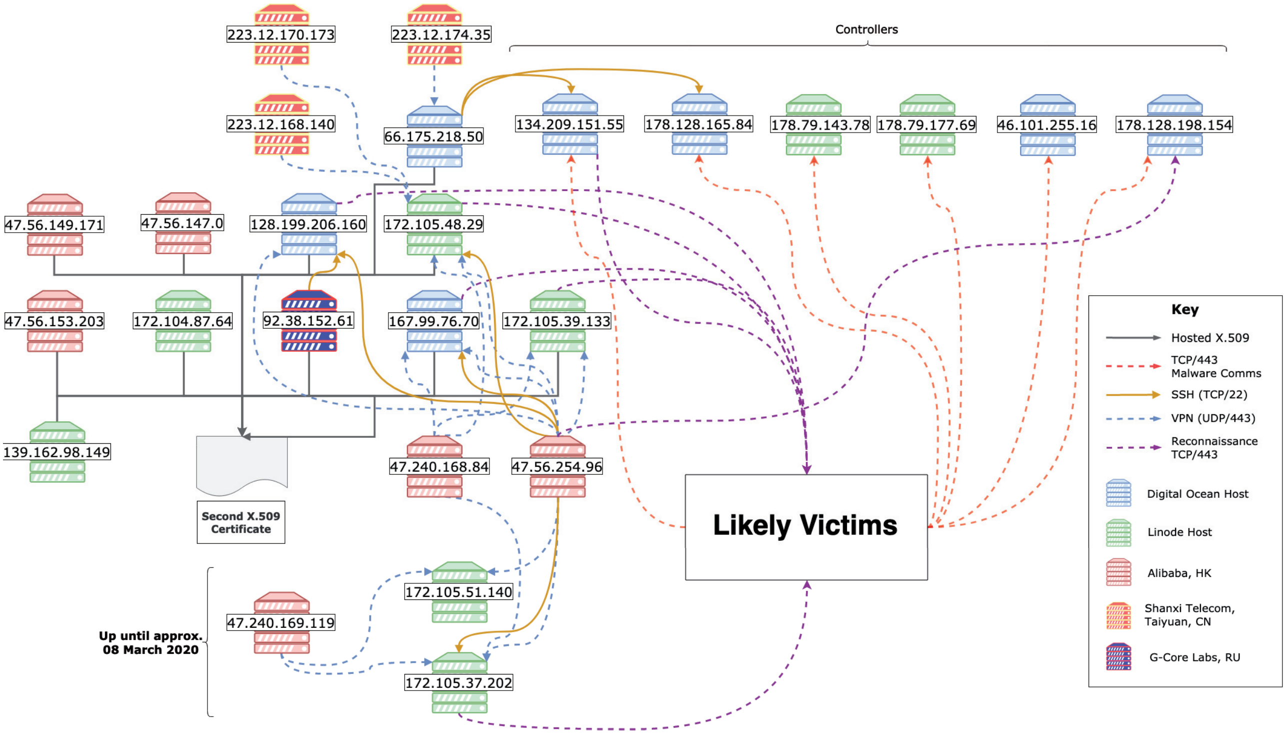


Figure 11: Observed actor infrastructure in March 2020.

In the cat-and-mouse (or kitten-and-panda) game actors and defenders dance the all-too-familiar back and forth motion of compromise and clean up. APT actors, though, show unique resolve in their focus on their targets. April shows them returning their attention to the targeting of Iranian government resources.

In addition to other connections, we see a couple of connections into TCP port 993 (IMAPS) on a government attributed host. While not conclusive, it is possible that these connections reveal that perhaps the kittens didn't beat the panda after all. Perhaps, like real pandas, they simply migrated down the mountains to the warmer valley during the winter months, waiting to return to their cool mountain homes just in time to beat the heat of summer.

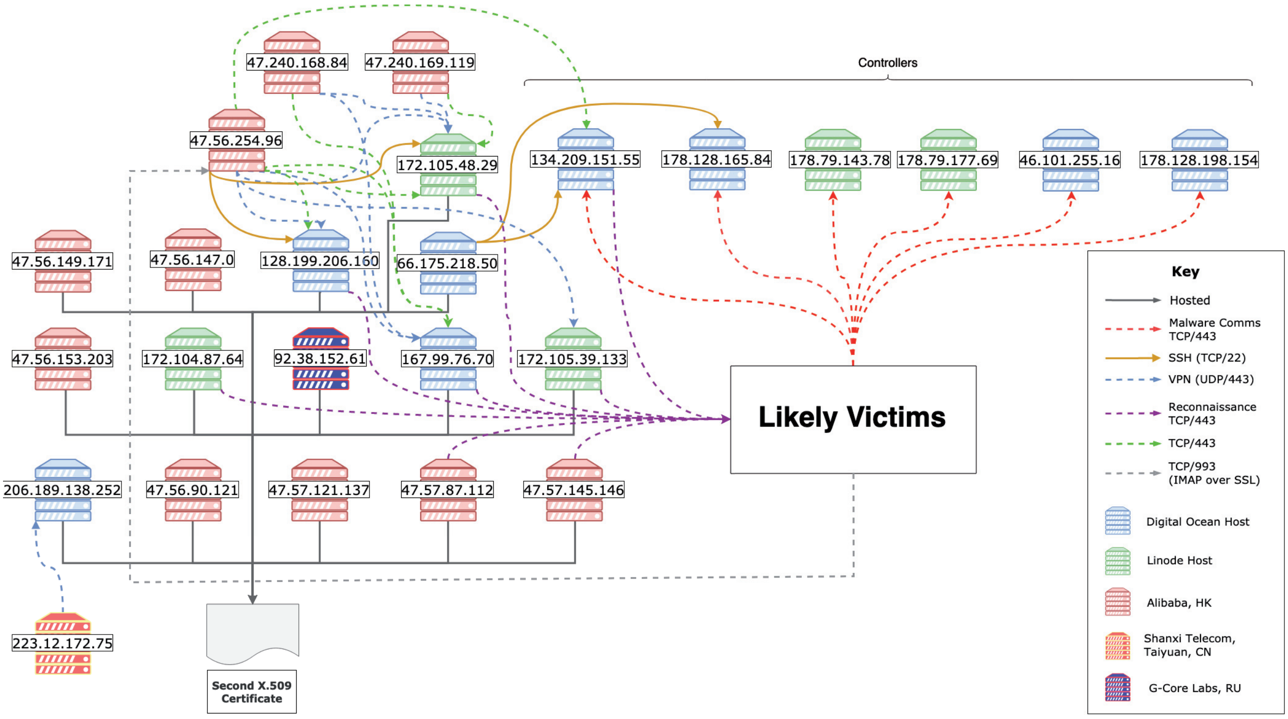


Figure 12: Observed actor infrastructure April 2020.

ABOUT THE VICTIMS

We do see many targets that we believe were compromised based on patterns of network connections (such as connections to controllers), data transfer, and longevity of the connections observable within available data. In some cases, though, we cannot establish with certainty that the targets were successfully compromised. We show a collective summary of victim demographics below where we have medium confidence the targets were successfully compromised.

Knowing who malicious actors target, what assets they focus on, and how they obtain access to their victims is equally critical to knowing the enemy and is a critical component of comprehensive cyber field awareness. In the case of APT27, we see victims within the following countries: Afghanistan, Bangladesh, Brazil, Bulgaria, Canada, Egypt, Greece, India, Iran, Iraq, Israel, Italy, Kazakhstan, Kenya, Kuwait, Kyrgyzstan, North Macedonia, Malaysia, Nepal, Oman, Pakistan, Palestine, Qatar, Russia, Saudi Arabia, Slovenia, South Africa, South Korea, Taiwan, Tajikistan, Turkey, United Arab Emirates, United Kingdom, United States, Uzbekistan, Vietnam, Zimbabwe, and some international organizations. Our data shows an unbalanced distribution of interest in these targets, with Iran being heavily favoured and Saudi Arabia a distant second.

Analysing the victims by industry sector gives us insight further insight into the threat actor behaviour. We see victims in the following sectors:

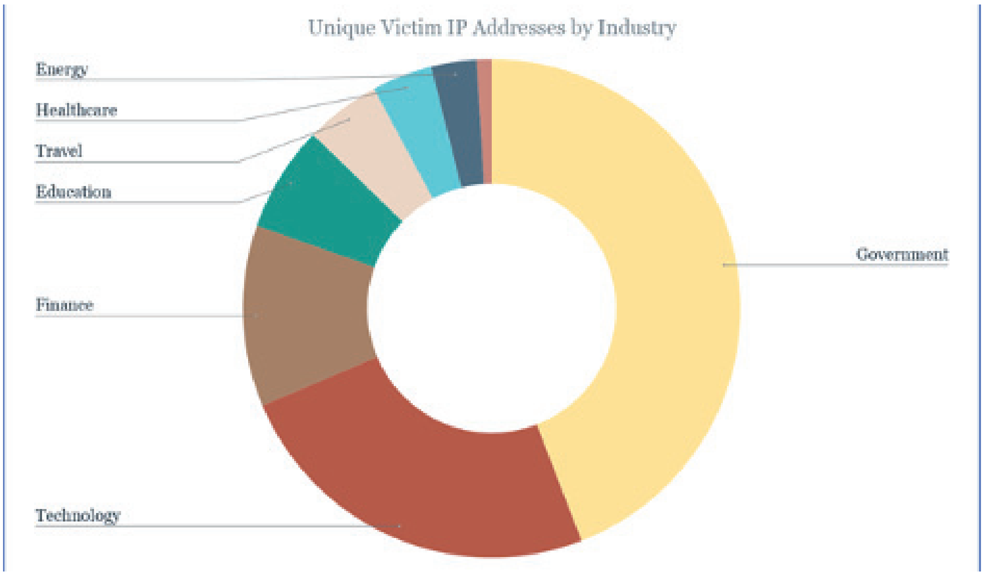


Figure 13: Unique victim IP addresses by industry.

Team Cymru does not wish to cause further victimization of those exploited by the APT27 actors. Therefore, as we previously mentioned, we will not be enumerating the list of victim organizations we have seen over the full observation period of these findings. The summary information is important, as victimology patterns are useful TTPs to indicate possible threat actor attribution and to increase the shared understandings of the targeting by APT27.

CONCLUSION

Julius Caesar famously said: 'Veni! Vidi! Vici!' – I came, I saw, I conquered.

Today, network defenders are fighting a well-equipped and capable array of enemies. Yet the old wit of Julius Caesar's simple three-word phrase is tied together by that one critical element that so many defenders forget: sight. The modern-day equivalent is cyber field awareness and those defenders who recognize the importance of knowing your enemy have a chance at success. After all, who knows what history may have been if Julius Caesar had left out the 'vidi'.

APT27 actors use a wide range of tools and infrastructure to enable their attacks, gaining access, persisting control, and exfiltration of data. We have shown a significant history of the last year of APT27 actor activity, which reflects an impressive infrastructure, a lot of successes in compromising targets, and several iterations of introducing and retiring assets.

The APT27 actors were successful in many ways. They were able to run a fairly complex infrastructure, allowing for tunnelled probing and reconnaissance. Many of their targets appear to have been successfully compromised, showing connections compatible with their malware reaching back to control servers. The tunnels show traffic in many cases, suggesting a possible exfiltration of data from their victim networks. They have a well-developed set of tools and skills, with an ability to support multiple ongoing attacks against many different countries as the same time. Yet they are not the only story here.

APT27 was successful at obtaining and maintaining access to Iranian resources for many months. The Iranians, to their credit, detected this and came up with what may have been a successful mitigation process applied to multiple distinct agencies to clean up these intrusions. This activity appears to have slowed down the attacks of the APT27 actors for many weeks against all potential targets. Persistence wins the day, however, and the APT27 actors appear to be increasing activity in the latest iterations of data.

The pandas seem to have bested the kittens in the summer and fall of 2019, but winter brought another story. The kittens detected the pandas and bested them in the winter. Spring brings more panda activity, showing a returned focus on the kittens, and time will tell how these two adversaries play together in the future.

Some suggest that APT actor groups are sufficiently advanced that organizations stand little to no chance of being able to defend themselves. The ongoing, persistent, mission-driven attention and focus of these threat actors make defence against these threat actor groups very difficult. Continuous attack focus requires continuous defence focus. Many organizations simply lack this ability to maintain a high level of attention to detail, and the right details, to successfully defend against APT actors.

Being aware of the global threat picture and obtaining that more complete cyber field awareness is more critical today than ever before. Actor groups are advanced, and they are persistent, but they are not invisible. Knowledge of the actor activity provides the necessary intelligence to tip the balance and give defenders a chance of defending against APT27 and all similarly positioned advanced threat actors.

REFERENCES

[1] Advanced Notification of Cyber Threats against Family of Malware Giving Remote Access to Computers. aeCERT. https://www.tra.gov.ae/assets/mTP39Tp6.pdf.aspx.

[2] Legezo, D. LuckyMouse hits national data center to organize country-level waterholing campaign. SecureList. June 2018. https://securelist.com/luckymouse-hits-national-data-center/86083.

[3] mbed TLS 1.3.10 released. https://tls.mbed.org/tech-updates/releases/mbedtls-1.3.10-released.

[4] Hall, T.; Clarke, M. Grab bag of attacker activity. https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1574947864.pdf.

[5] Pantazopoulos, N.; Henry, T. Emissary Panda – A potential new malicious tool. NCC Group. May 2018. https://www.nccgroup.com/uk/about-us/newsroom-and-events/blogs/2018/may/emissary-panda-a-potential-new-malicious-tool/.

[6] Falcone, R.; Lancaster, T. Emissary Panda Attacks Middle East Government SharePoint Servers. Palo Alto Networks. May 2019. https://unit42.paloaltonetworks.com/emissary-panda-attacks-middle-east-government-sharepoint-servers/.

[7] https://twitter.com/BitBaanLab/status/1211601603519754240.

[8] How the Iranian Cyber Security Agency Detects Emissary Panda Malware. Dragon News Blog. March 2020. https://blog.team-cymru.com/2020/03/25/how-the-iranian-cyber-security-agency-detects-emissary-panda-malware/.

INDICATORS OF COMPROMISE

X.509 certificates

Our name	SHA1
First X.509 certificate	6B:10:79:40:80:A1:55:3A:08:76:76:09:5D:05:4F:16:08:94:A2:4B
Second X.509 certificate	43:CD:54:4A:01:8F:29:56:A3:3E:D6:55:1E:ED:85:DC:26:05:9D:62

IP addresses

These addresses were active in April 2020.

IP address	ASN	Type	First seen	Last seen
47.56.147.0	Alibaba, HK	VPN node second X.509	2020-01	2020-04
47.56.149.171	Alibaba, HK	VPN node second X.509	2020-01	2020-04
128.199.206.160	DigitalOcean, US	VPN node second X.509	2020-03	2020-04
167.99.76.70	DigitalOcean, US	VPN node second X.509	2020-03	2020-04

IP address	ASN	Type	First seen	Last seen
172.104.87.64	Linode, US	VPN node second X.509	2020-03	2020-04
172.105.39.133	Linode, US	VPN node second X.509	2020-03	2020-04
172.105.48.29	Linode, US	VPN node second X.509	2020-03	2020-04
139.162.98.149	Linode, US	VPN node second X.509	2019-09	2020-03
47.56.153.203	Alibaba, HK	VPN node second X.509	2020-03	2020-04
66.175.218.50	Linode, US	VPN node second X.509	2020-03	2020-04
92.38.152.61	G-Core Labs, RU	VPN node second X.509	2020-03	2020-04
206.189.138.252	DigitalOcean, US	VPN node second X.509	2020-04	2020-04
47.56.90.121	Alibaba, HK	VPN node second X.509	2020-04	2020-04
47.57.121.137	Alibaba, HK	VPN node second X.509	2020-04	2020-04
47.57.145.146	Alibaba, HK	VPN node second X.509	2020-04	2020-04
47.57.87.112	Alibaba, HK	VPN node second X.509	2020-04	2020-04
178.128.165.84	DigitalOcean, US	Malware controller	2019-12	2020-04
134.209.151.55	DigitalOcean, US	Malware controller	2020-03	2020-04
47.56.254.96	Alibaba, HK	Operational node	2020-03	2020.04