Behind the scenes of the Emotet iInfrastructure

hello.global.ntt/en-us/insights/blog/behind-the-scenes-of-the-emotet-infrastructure

Security division of NTT Ltd.

Reliance Securities

Reliance Securities implemented smart contact center technologies to put their customers at the heart of their operations, reducing their response times. They have also pinpointed which platform their customers prefer to communicate through.

Reliance Securities

Reliance Securities implemented smart contact center technologies to put their customers at the heart of their operations, reducing their response times. They have also pinpointed which platform their customers prefer to communicate through.

ASHRAE

ASHRAE’s new headquarters creates a blueprint for the intelligent building

ASHRAE

ASHRAE’s new headquarters creates a blueprint for the intelligent building

Emotet is a threat known to use large amounts of command and control servers (C2s) in parallel in order to ensure uptime and bypass blocking.
This first layer of C2s, also called Tier 1 C2s, will in part forward their received traffic to Tier 2 servers. This relationship has previously been observed by Centurylink[1].

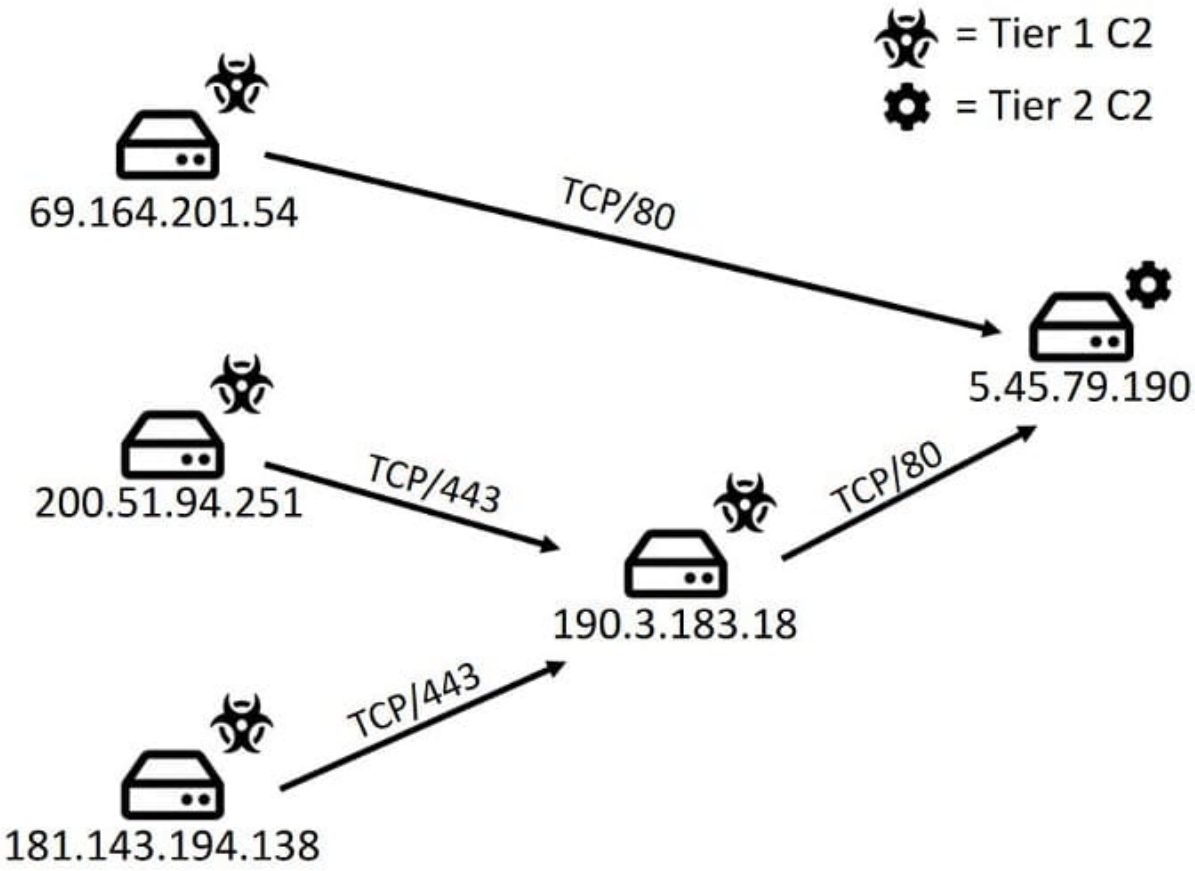
NTT Ltd. Threat Detection decided to explore the malware infrastructure of Emotet deeper, with multiple goals in mind:

- ensure our long-term detection capabilities for Emotet traffic in our customer environments
- explore the underlying Emotet infrastructure and track the setup and longevity of the Tier 2 servers
- collaborate with CERTs and notify ISPs of malicious activity

We own and operates one of the world's largest tier-1 IP backbones, giving insight into a significant portion of the global internet traffic. We’re also consistently ranked among the top five network providers in the world. In the fall of 2018, our security division added botnet infrastructure detection capabilities to our Managed Security Services (MSS) Threat Detection services. This unique capability was use during this project in order to explore and monitor the Emotet network infrastructure.

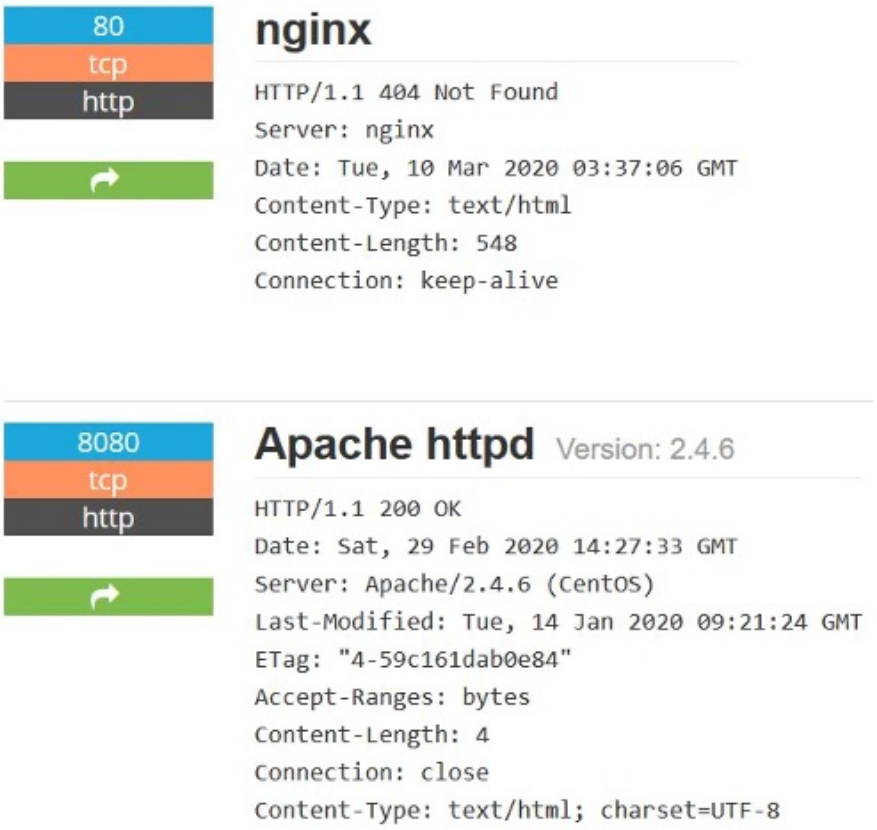
Starting the journey

The assumptions of behaviour of the Tier 1 C2s were reduced to the expectation that they forward their traffic towards a Tier 2 C2. We initially monitored Tier 1 C2 traffic en masse. We extracted Tier 1 C2 lists from Emotet samples and applied these IOCs in our netflow monitoring in NTT Ltd.’s global internet infrastructure, where one potential Tier 2 C2 was found:



The Emotet botnet is divided into separate Epochs, Epoch 1, 2 and 3, which all have their own separate Tier 1 C2 infrastructure [2]. The Tier 1 C2s in the picture above belong to Epoch 2.

A Shodan lookup of the services of the Tier 2 C2 shows the following setup of HTTP services:



At this point in the investigation we assumed that the above was the standard setup for all Tier 2 C2s and automated the analysis of outgoing traffic from Tier 1 C2s to find new Tier 2 C2s. We found new ones by selecting traffic where:

- the source IP is an Emotet Tier 1 C2
- the destination port is TCP/80 and is running a NGINX service, with the error message “HTTP 404 Not found”
- the destination IP is also running an Apache service which gives “HTTP 200 OK” status message over port TCP/8080

Observed backends

With our new workflow established we've observed 16 Tier 2 C2 servers with incoming Tier 1 C2 traffic of their respective associated Epoch:

- eight Tier 2 C2s belong to Epoch 1
- five Tier 2 C2s belong to Epoch 2
- three Tier 2 C2s belong to Epoch 3

With the following hosting providers used:

- seven using **Serverius Holding**
- five using **GloboTech**
- two using **Worldstream**
- one using **PnS Hostings**
- one using **RealHosters**

The graphs below show the timelines for when each Tier 2 C2 is receiving connections from Tier 1 C2s grouped by each Epoch. The Y-axis is the number of connecting Tier 1 C2s and the X-axis is the timeline. The coloured lines each represent a Tier 2 C2.

Epoch 1:

Comment:

Based on the synchronization in time when old Tier 2 C2s disappear and new Tier 2 C2s appears there are two separate Tier 2 C2 infrastructures for Epoch 1 in use at the same time: **37.252.15.50 -> 185.180.223.70 and 72.10.162.83 -> 72.10.162.84-> 72.10.162.85-> 72.10.162.86.**

Epoch 2:

Comment:

The new Tier 2 C2s appear at the same time or a little before the old one goes down. The overlap with two Tier 2 C2 active at the same time is noteworthy.

Epoch 3:

Comment:

The IP 134.119.194.179 has for a very long time been utilized as a Tier 2. The IP 37.252.14.29 has a low utilization of connecting Tier 1 C2s.

From the analysis above the following Tier 2 IPs were excluded due to their short time-span and low amount of connecting Tier 1 C2s indicating them to possibly be inactive:

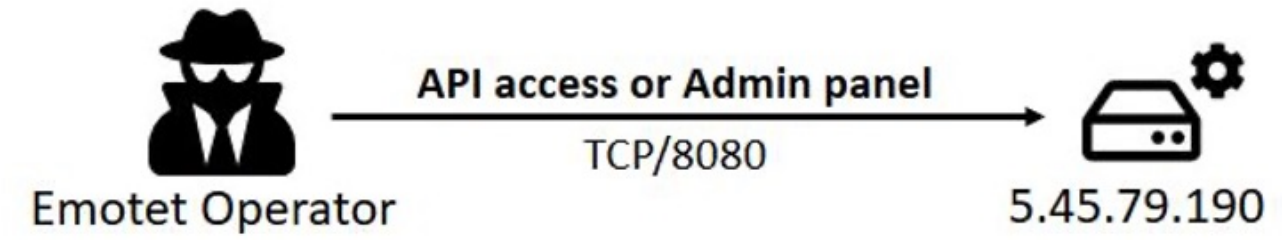
- 37.252.15.52
- 37.252.14.109
- 185.180.223.114

Theories on administration

Our analysts have three main theories on how the actor behind Emotet administers the Tier 2 C2 servers:

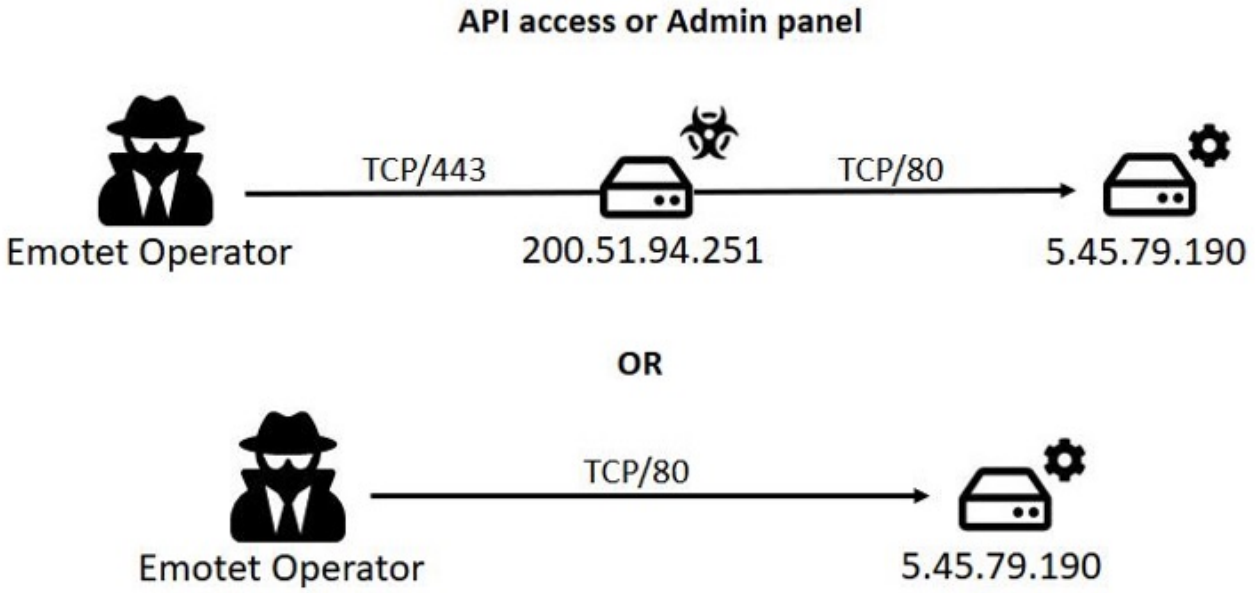
Theory 1 – Apache TCP/8080

An administration panel and/or API access exposed over Apache TCP/8080 which the actor connects to. No network traffic in the NTT Global internet infrastructure supporting this theory has been seen.



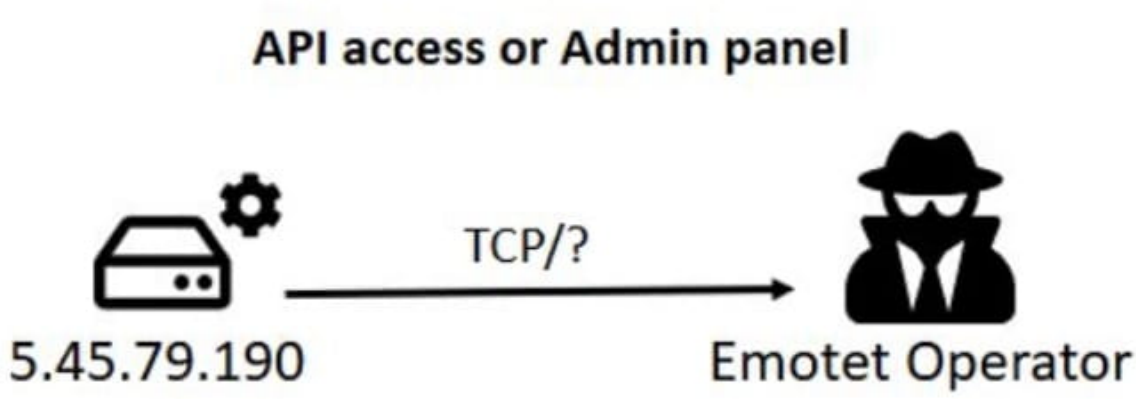
Theory 2 – NGINX TCP/80

The hosting of an administration panel and/or API access over the same port that they receive C2 traffic. This would make it easier for the actor to hide their tracks by possibly tunnelling their traffic through Tier 1 C2s towards Tier 2 C2s.



Theory 3 - A Tier 3 C2

Tier 2 C2s forwarding their traffic towards a central Tier3 C2 which has data for all three Epochs. No outgoing traffic from Tier 2 C2s inside of NTT Global internet infrastructure has been observed supporting this and it's seen as very unlikely.



Closing thought on theories

The overlaps observed in the Tier 2 C2 infrastructure with multiple Tier 2 C2s being active at the same time indicates an additional complexity. Based on netflow monitoring of our global internet infrastructure, theory 2 is found to be most likely, but forensics of Tier 2 C2s would be needed in order to confirm this theory.

Conclusion

NTT Ltd.’s Threat Detection has reliably been able to follow the changes in the use of Tier 2 servers in the Emotet network infrastructure. It’s noteworthy how one of the largest threat actors today can largely operate undisturbed with Tier 2 servers having uptime of multiple months. This research is of use when planning takedown actions, but also in understanding threat actors' operations and improving the detection capabilities that NTT Ltd. Threat Detection has in customer environments.

In the recently released 2020 Global Threat Intelligence Report, our researchers and thought leaders share statistics and trends from the previous year. A key theme in this year's report is 'Threat actors are innovating and evolving their tradecraft'. Read more about how automation, multi-stage-payloads and custom targeted malware are changing the threat landscape here.

References

[1] https://blog.centurylink.com/emotet-illuminated-mapping-a-tiered-botnet-using-global-network-forensics/

[2] https://isc.sans.edu/forums/diary/Emotet+epoch+1+infection+with+Trickbot+gtag+mor84/25752/