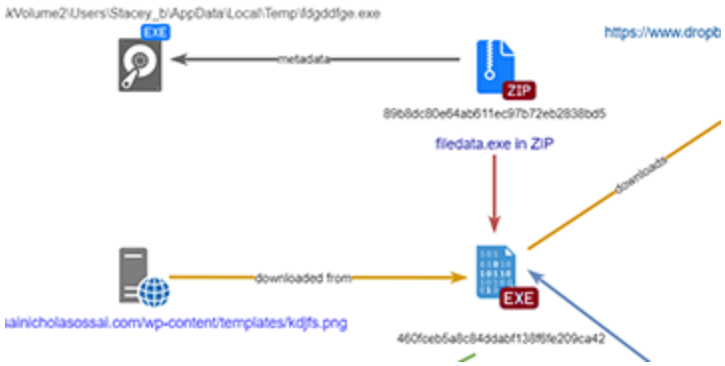
Inside Look at Emotet's Global Victims and Malspam Qakbot Payloads

blog.kryptoslogic.com/malware/2018/08/01/emotet.html



Authored by: Kryptos Logic Vantage Team on Wednesday, August 1, 2018
Tags: emotet

The Emotet botnet reputation precedes it; historically aggressive and malicious, today it has evolved and incorporated a number of advancements to create a more resilient botnet delivery system, nearly immune from takedown. Recently, US CERT reported that Emotet incidents (and its subsequent payload droppers) are affecting state, local, tribal, and territorial (SLTT) governments at up to 1 million dollars per incident.

We have captured a global view of many of the active infections within the latest Emotet botnet. At the time of this writing, we believe this to be the only publicly available coverage of actively infected Emotet peers.

In an earlier post, we announced Telltale and provided the WannaCry data set for organizations to determine if they are still affected by residual ransomware risks. Today, we will further enrich this data set by adding Emotet data promoted from the Vantage Breach Intelligence Service to our free version of the offering, Telltale. Organizations looking to reduce their risk exposure to Emotet and or WannaCry should consider signing up for either of these breach notification offerings.

The remainder of this post will:

- Provide a high level view of the Emotet botnet distribution and some of its metrics;
- Examine the latest botnet trends and deep dive into a recent Qbot sample.

Emotet by the Numbers

Most telemetry available today on Emotet has been likely sourced from vendor-specific AV or spam infection attempts (e.g. blocked infections). However, to be clear, the following visibility is sourced from the Emotet peers which are actively infected and participating in the botnet,

that is, those which have not been blocked.

Overall we can compute a partial view of at least one of the botnets:

- 70,000+ unique IPs identified
- 4000+ unique ASNs communicated
- 5000+ unique organizations and telecoms affected
- 170 countries affected

It would be fair to estimate the botnet is at any given point between 50,000 to 150,000 infected nodes. Looking at the aggregate of the information we can see how that breaks down by country.

Total Hits by count.

While the science of evaluating the total infection hits for any given malware strain is out of scope for this post, what we can interpret from our source data and the traffic patterns against any particular IP address is that many organizations infected by Emotet have more than one infection, which was likely triggered by a pivoting component like EternalBlue (you know the same EternalBlue from NotPetya and WannaCry). We have observed several organizations (hospitals, research centers, etc) exhibit signs of dangerously high levels of Emotet infection volume. Clearly, the United States and South Korea have tells of high frequency activity from some certain organizations which increase its numbers. While this is certainly concerning, it is more prudent to examine the unique IP addresses graph below to get a different perspective not skewed by some of the noise of certain infected organizations.

Top 12 countries seen by Unique IP.

Again we see a high number of United States coverage in the Unique IPs visualization. A special note should be given to India in that India typically has a high DHCP churn, resulting in higher than normal level of unique IPs for any given period.

Finally we can observe a full global map distribution which shows us no real surprises other than Emotet is widespread.

A global map of Emotet's reach, distributed by Source IP.

Malspam Payload Show Signs of Evolving Botnet Trends

While Qakbot is just one of many things that can be dropped we learn very quickly why the Emotet network introduces a significant level of risk to organizations. The latest Emotet design utilizes a new blueprint in the evolution of modern malware and botnets. Because Emotet's Command and Control (C&C) systems work through a complex decentralized network of infected hosts and proxy peers, it could prove a difficult take down task for law enforcement considering there are few single points of failure and would require multiple levels of cooperation in near perfect harmony.

Traditional botnets heavily depended on Peer-to-Peer for C2 communication and fallback, this allowed researchers to peak into the activity of the botnet and observe victim machines, newer/more resilient botnets seem to be moving away from this approach. Another way researchers observed victim machines was to reverse engineer the domain generation algorithm and register their own "sinkholes". As botnets move away from DGA this becomes unfeasible. Emotet and other botnets such as TrickBot pose a unique challenge to researchers and companies in the field.

However, our research demonstrates that it is not impossible to gain insight into these evolved botnets. IPs tend to be harder to blacklist than domain C2s so the traditional "IOC" approach is becoming less and less effective, On the other hand, you have various payloads all with their own techniques. So while a good Predict, Prevent, and Detect agent like Tactics (or perhaps EDRs) can help, it still requires analysts to steer.

Consequently, this also makes it difficult to block and track for most organizations, as IP addresses are constantly shifting and changing. This makes detecting the traffic a bit of a long term whack-a-mole game.

Ironically, Emotet drops a variety of payloads (like Qakbot) which are in fact separate botnets. Looking at a quite recent Malspam campaign we picked up a interesting Qakbot which in itself is another botnet sharing many of the same design resilience as Emotet, e.g., proxy peers and no DGA.

Qakbot graph.

A thorough review of Qakbot, ranging from protocol version 10 to 12, was written up by Intel Security in Virus Bulletin. Current Qakbot samples (version 322.368) are at version 15 of the protocol and behave similarly to version 12, with some exceptions:

- DGA mechanism appears to be completely gone
- The 1024-bit RSA key used for encrypting keys and verifying signatures was removed, with only the same 2048-bit key remaining
- There are 31 possible C&C commands, upwards from the 25 described before

We found signs of Qakbot disabling HTTP2 in Firefox by modifying the profile.js configuration file, where we used to see banking malware disabling SPDY. HTTP2 is the successor to SPDY so disabling these leaves only HTTP1, which is much easier to intercept. Typically this is done so that the malware can hook a specific function in the browser: in the case of Firefox they normally hook `nspr4!PR.Read`.

Like Emotet, Qakbot contains signs of a UPnP library, removal of the DGA function, and reliance on decentralized peers through a proxy. To this end we see a malware which has

- Banking web injects;
- Its own botnet communication system outside of Emotet;
- Stolen certificates and heavy use of Powershell and other defense evasion techniques.

Conclusion

Emotet introduces significant challenges to the cybersecurity threat landscape which are very concerning. In the past, botnets which may have been too large or introduced significant risks could be taken down. If they were not taken down, at minimum defenders could coordinate on specific protocols and IP addresses or certain security controls to counteract the effectiveness and potential exposure of the botnet. However the resiliency introduced in the latest trends of botnets such as Emotet, Dridex, and Qakbot suggest that takedowns will be far more difficult, or infeasible and consequently operators will have quite a bit of difficulty counteracting against a perpetual high frequency whack-a-mole IP address blacklisting game.

The reality is that as Emotet continues to grow, it will increase public and private risk exposure to digital attacks which can be leveraged by staging attacks on top of these difficult to stop botnets. Whether it is a ransomware, a critical infrastructure attack, or the next EternalBlue, there is not much that can currently slow these attacks down in most organizational threat models. These types of new resilient botnets are a paradigm shift for attackers and have shown us the dangers of attack platforms which can undermine and circumvent security controls at scale.

We're pleased to be able to share the breach intelligence data we have gathered for free via our Victim Notification service Telltale. You can sign-up and check for any observed activity coming from your network for free. In the future we'll be adding more and more malware families to Telltale.

IOCs:

A list of binaries signed by the above detailed malicious code signing certificate are available here, a list of webinject URLs are available here and finally a list of webinject paths are available here.