Emotet Redux

blog.lumen.com/emotet-redux/

March 8, 2022

What Global Network Visibility Reveals about the Resurgence of One of the World's Most Notorious Botnets

Executive Summary

Since its reemergence on Nov. 14, 2021, Black Lotus Labs has once again been tracking Emotet, one of the world's most prolific malware distribution families which previously infected more than 1.6M devices and caused hundreds of millions of dollars in damage across critical infrastructure, healthcare, government organizations and enterprises around the world. Using our global visibility, we have determined that while Emotet has not yet attained the same scale it once had, the botnet is showing a strong resurgence with a total of approximately 130,000 unique bots spread across 179 countries since November 2021. This growing pool of bots presents a looming threat to organizations around the world; Emotet bots serve to not only propagate the malware by spamming targets through legitimate mail servers using stolen credentials, but they also serve as footholds for lateral movement in coveted networks and could be promoted to act as proxy C2s.

Introduction

Emotet is widely considered one of the world's most dangerous global malware families due to its role in gaining initial access to infected machines and then selling that access to other cybercriminals, such as ransomware operators. When we first reported on Emotet a few years ago, we focused on its unique tiering structure and how the complex architecture both enabled resiliency against individual C2 disruptions and provided a successful malware distribution framework to rent out as a service to other actors and ransomware operators. We explored how network telemetry revealed that some infected Windows devices or bots were promoted via a UPnP module to serve as proxy C2s, forwarding communications from newly infected devices to threat actor-controlled infrastructure. We used Lumen's global backbone visibility to plot out the distinct clusters of C2s known as Epochs 1 and 2, and we determined that only the Bot C2s were communicating with other malware families such as TrickBot, IcedID, Qakbot, Dridex and others. At the time, we identified, on average, 40,000 unique Emotet bots daily and tracked more than 300 unique Emotet C2s in a given month.

After a brief hiatus in summer of 2019, Emotet came back full swing with a new set of bots and C2s added to its arsenal (Epoch 3). After an active couple of years, Emotet was taken offline by law enforcement in January 2021, only to resurface late last year with some initial help from TrickBot.

Since that time, the infosec community has been closely monitoring its return, with numerous organizations reporting new functions and changes in the infection methodology. It is evident from early reporting and substantial recent spamming activity that Emotet's return warrants attention. But how mature is the new version of Emotet? Does it rival its predecessor? Black Lotus Labs' analysis reveals that while Emotet's C2 infrastructure was reestablished in November, the aggregation of bots really didn't begin in earnest until January. And while the current daily unique bot count is smaller than that of Emotet in its heyday, the number is steadily increasing. The scale of the new bot infrastructure coincides with some notable differences in the tiering structure and geographic distribution this time around.

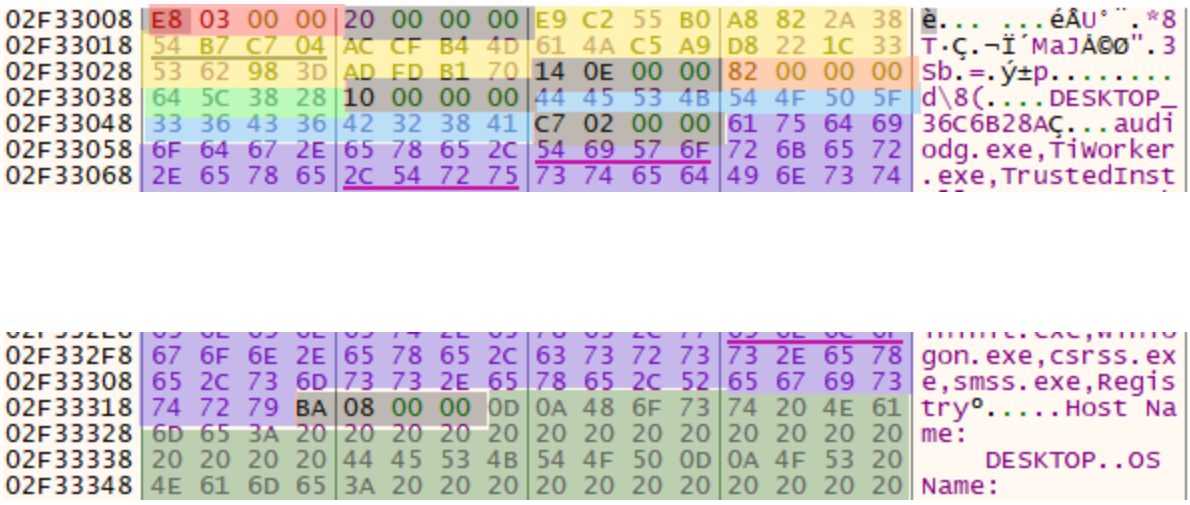
Technical Details

New Functions

As other threat intel intelligence teams have noted, the new Emotet exhibits a few notable changes in how it functions, including, the algorithm it uses to encrypt network traffic and the separation of the process list into its own module.

While the previous version of Emotet used the RSA encryption scheme with a single key to encrypt and validate network traffic, the new version employs elliptic curve cryptography (ECC), with a public key to perform the encryption and a separate algorithm to perform data validation.

In the prior version of Emotet, the list of running process on the infected computer was sent to the C2 along with the initial beacon. In the new version, a process list module is sent to the infected machine after it first checks in with the C2. Initially, the new process module would only send the list of running processes. However, the operators recently added functionality to gather additional information about the infected host, demonstrating the ongoing evolution of Emotet's code.



Red	Command
Gray	Size of next field
Yellow	SHA256
Orange	Module ID
Light Green	Module job number
Blue	Bot ID
Purple	Process list
Dark green	System information

Figure 1: Excerpts from Emotet communication from bot to Tier 1 C2 showing header, process list and system information

Global Distribution of C2s

While Black Lotus Labs tracked more than 300 unique Emotet C2s in May of 2019, the number of unique C2s in the roughly four months since the resurgence is roughly 200. As Figure 2 reflects, when Emotet came back online in November 2021, it did so with a smaller, but relatively consistent pool of Tier 1 C2s. Over the last few months, the C2 pool has continued to grow to an average of 77 unique Tier 1 C2s per day from late February through March 4.

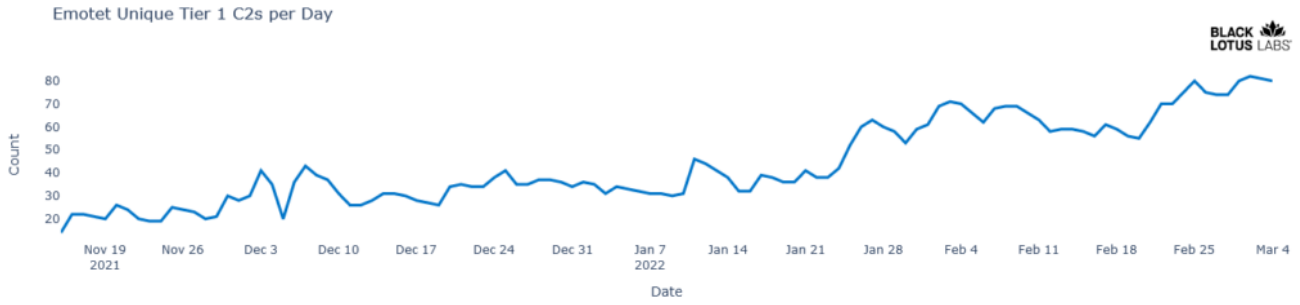


Figure 2: Daily active unique Emotet Tier 1 C2s November 2021 – March 4, 2022

The global distribution of Tier 1 Emotet C2s today, depicted in Figure 3, has some similarities with our earlier reporting on Emotet's prior Tier 1 C2 infrastructure: Emotet C2s are once again predominently located in the United States and Germany. The rest of the list of top 10 countries by volume of C2s includes (in order of prevalence): France, Brazil, Thailand, Singapore, Indonesia, Canda, United Kingdom and India. The average number of days an Emotet Tier 1 C2 is active currently stands at 29 since the resurgence. However, as the botnet once again becomes more established, that figure may change; the average active days of an Emotet C2 in 2019 was 38.

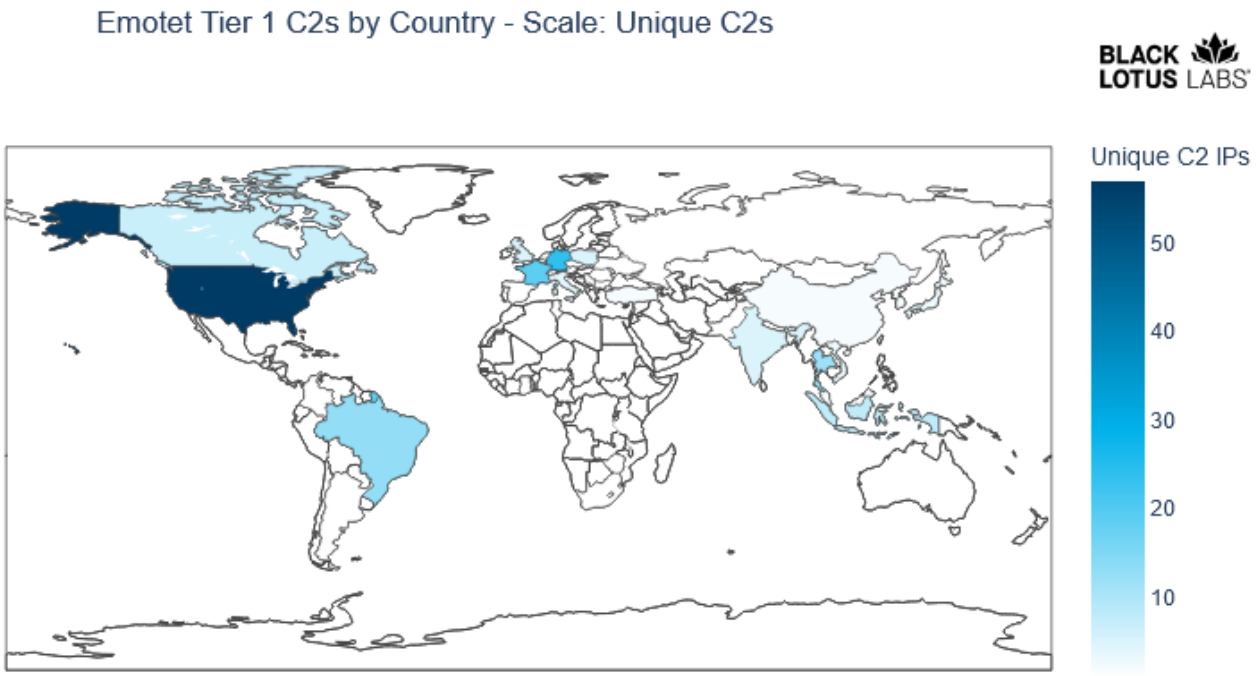


Figure 3: Emotet global Tier 1 C2 distribution as of March 4, 2022

Change in Tiering Model

One core difference in the architecture of Emotet today is the apparent absence of Bot C2s. In the earlier version of Emotet, a subset of bots would receive a UPnP module that enabled an infected device to act as a C2 by opening a port on the user's router that would then allow

it to proxy traffic from Emotet bots to a higher-tier C2. These Bot C2s, which represented as much as 80% of the Emotet C2s we reported at the time, were the only C2s that appeared to communicate with other malware families.

However, to date, Black Lotus Labs has not observed new Emotet bots being infected with the UPnP module or exhibiting proxy communications with Tier 1 C2s. It remains to be seen whether the lack of Bot C2s is a permanent shift, or just an effect of Emotet's rebuilding phase that may yet include reestablishing Bot C2s in the future.

Global Distribution of Bots

While Emotet's new C2 infrastructure exhibited a steady base beginning in November, it took a few months before a sizable pool of bots was reestablished. Figure 4 illustrates the relative lack of Emotet bots until a notable uptick beginning in mid-January 2022. The weekly cadence of fluxuations in the number of new Emotet bots from January through the time of this report mimic those we saw for Emotet back in 2019.

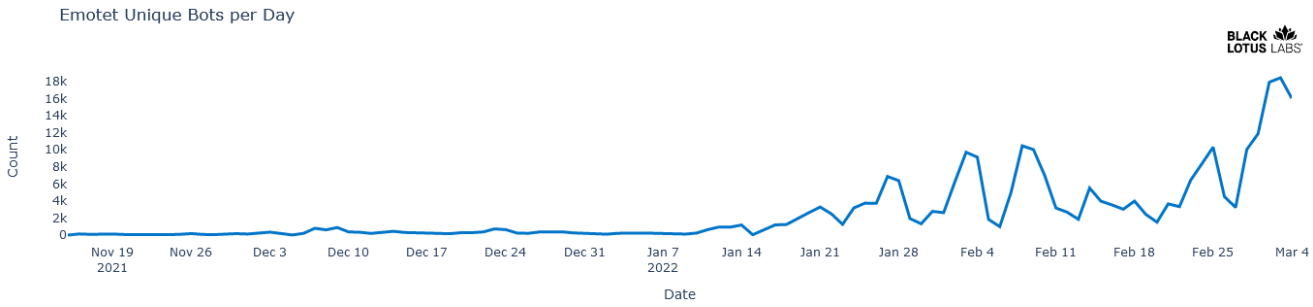


Figure 4: Daily active unique Emotet bots November 2021 – March 4, 2022

As depicted in Figure 5, Emotet bots today show a heavy distribution in Asia, namely Japan, India, Indonesia and Thailand. This is not surprising given the preponderance of vulnerable or outdated Windows hosts in the region. The remaining top 10 countries by volume of Emotet bots includes (in order): South Africa, Mexico, the United States, China, Brazil and Italy.

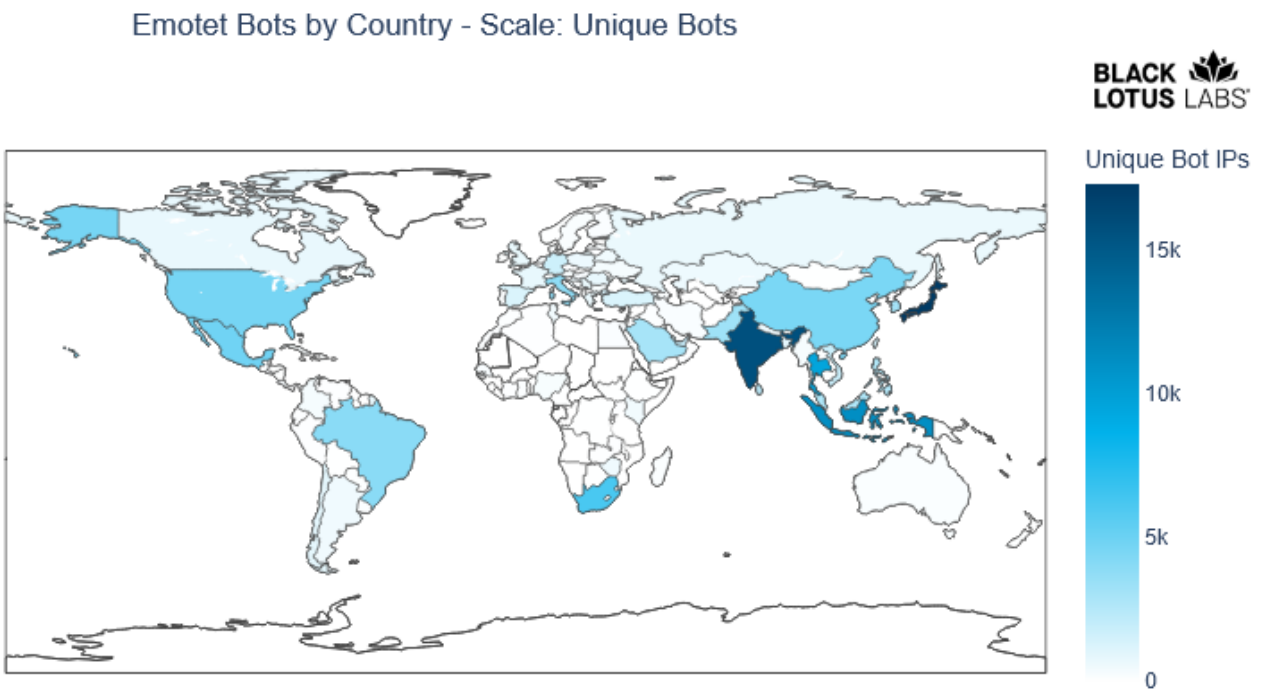


Figure 5: Emotet global bot distribution as of March 4, 2022

Conclusion

The growth and distribution of bots is an important indicator of Emotet's progress in restoring its once sprawling infrastructure. Each bot is a potential foothold to a coveted network and presents an opportunity to deploy Cobalt Strike or eventually be promoted to a Bot C2.

While other organizations can characterize the nature of the C2 nodes through analysis of the bot infection vector via malware samples, the Black Lotus Labs reputation system tracks both Emotet's C2 infrastructure and its bots. This intelligence feeds the Lumen security services portfolio to help protect customers from interacting with known or suspected malicious infrastructure.

Because Emotet is primarily spread through malicious email attachments and embedded URLs, we advise Lumen customers to bolster defenses against phishing as an initial access vector through full monitoring of network resources, ensuring proper patch management and conducting ongoing phishing and social engineering training for employees.

Our visibility showed a marked drop after March 4, with Emotet bots and Tier 1 C2s dropping down to 2,855 and 36, respectively. However, those numbers already appear to be climbing once again: we are currently tracking 6,435 bots and 62 Tier 1 C2s.

We would like to thank the many researchers who track and share information to help defend against the Emotet botnet. In particular, we are grateful to the tireless efforts of Joseph Roosen and the Cryptolaemus team, and Roman Hüssy of abuse.ch.

Black Lotus Labs took action to null-route some Emotet C2 infrastructure and will continue to collaborate with the community to detect and disrupt Emotet. We encourage other organizations to alert on these and similar indicators in their environments.

For additional IoCs associated with this campaign, please visit our GitHub page.

If you would like to collaborate on similar research, please contact us on Twitter @BlackLotusLabs.

This information is provided “as is” without any warranty or condition of any kind, either express or implied. Use of this information is at the end user’s own risk.
