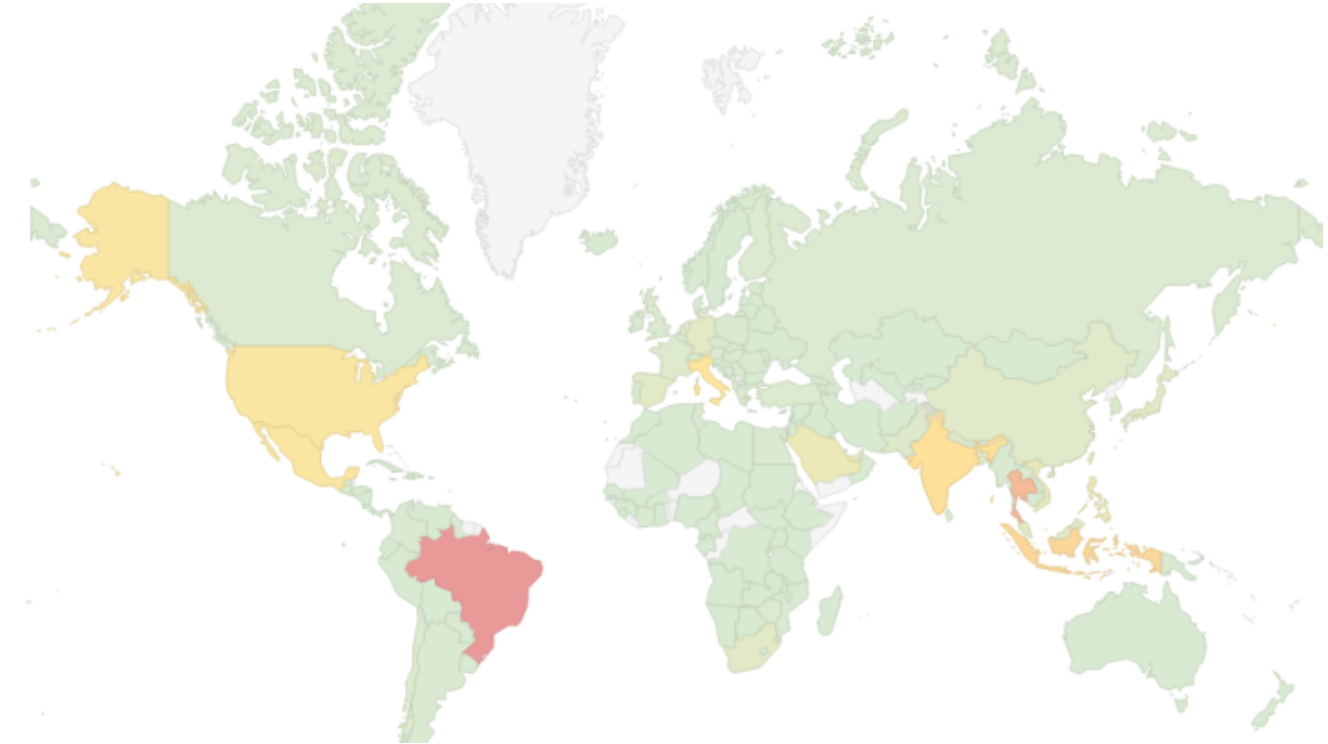


Emotet Botnet Rises Again

 bitsight.com/blog/emotet-botnet-rises-again

May 24, 2022 Share Facebook Twitter LinkedIn



Written by João Batista & Pedro Umbelino

If you work in cybersecurity, you've probably heard of the Emotet botnet. Once considered the world's largest malware botnet more than one year ago, Emotet was composed of hundreds of command and control servers and almost two million victims. Emotet was so large that it took a joint effort between law enforcement agencies and authorities from Netherlands, Germany, the United States, the United Kingdom, France, Lithuania, Canada, and Ukraine to allow investigators to take control of the botnet's servers, disrupt the malware's operation, and arrest two operators.

Unfortunately, law enforcement was not able to deliver a fatal blow to Emotet. In November 2021, a new version of Emotet emerged. How did this happen? What is the botnet doing today? And how can organizations avoid becoming victims?

Emotet - Hard to Kill

First discovered as a banking trojan in 2014, Emotet malware evolved into the go-to solution for cybercriminals over the years. One of the main reasons for Emotet's popularity is its functionality. Emotet is a self-propagating and "modular loader" malware, which means that while it is running on an infected system, botnet operators can send different modules that are capable of executing different jobs.

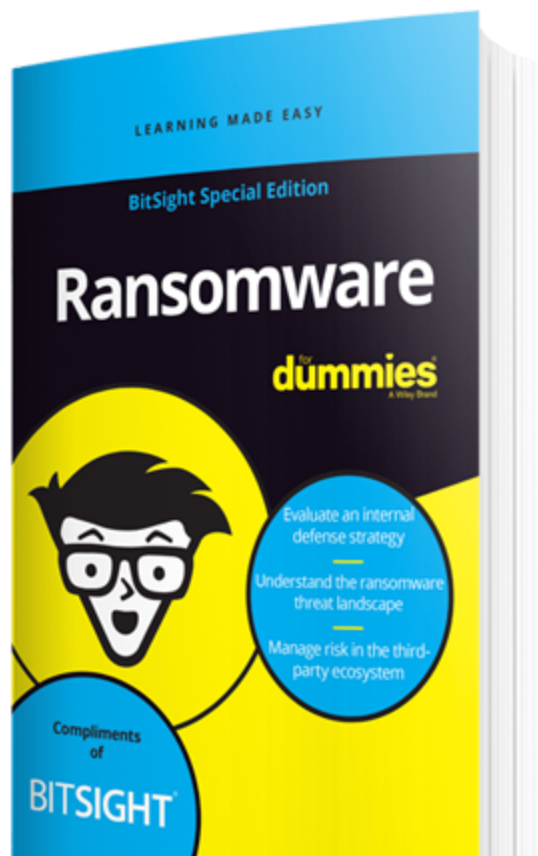
The Emotet infrastructure essentially acted as a primary door opener for computer systems on a global scale. It was then rented by cyber criminals to install their own malware: info stealers, ransomware, banking trojans, and other types of malware. In many respects, Emotet worked like a SaaS solution, only in this case, it was MaaS (malware-as-a-service).

Observing millions of infected machines, law enforcement tried to move against Emotet. In January 2021, law enforcement shut down Emotet and seized the infrastructure behind it. After gaining control of the infrastructure, on April 25, 2021, law enforcement effectively killed the botnets by issuing a final update to remove the remaining infections. But before the takedown, a partnership between Emotet operators and the Trickbot group allowed Trickbot operators to leverage the Emotet infrastructure to distribute Trickbot, a banking trojan. On November 14, 2021, Trickbot command and control servers began issuing tasks to their infected machines, instructing them to download a new Emotet version.

Emotet began spreading rapidly once again. The malware that law enforcement hoped to kill was back in business.

BitSight Exclusive: Ransomware for Dummies

Bring your strategic defense to the next level



BitSight Exclusive: Ransomware for Dummies

Bring your strategic defense to the next level

Ransomware attacks globally nearly doubled in 2021. BitSight's Ransomware for Dummies book reveals indicators of potential attacks, and how to minimize costly damage when successful ransomware targets you.

[Download eBook](#)


[Button Arrow](#)

Emotet Infection Chain

Emotet spreads itself via email phishing campaigns, using the infected computers to send the malicious emails. The emails can have multiple formats, such as simple emails without any context or replies to stolen email threads. Typically, the emails can carry either an attached Excel/Word document, a password-protected zip file, or a link to download the document. More recently, on April 22, our team spotted Emotet using LNK files instead of the usual Excel files, showing that the threat actors are trying to improve their tactics to increase their infection success rate.

Below is an example of a hijacked email thread with an attached Excel XLS file:



 **mike@** [REDACTED]
RE: 2021 South Carolina Builder Journal
To: confirmations@ [REDACTED]

Mike Thrasher

[mike@](#) [REDACTED]

Dear Mr. Thrasher,

Please see the following attachment regarding participation in the 2021 South Carolina Builder Journal.

Please feel free to contact me if you have any questions or comments. Thank you.

Sincerely,

Michael McIntire
Ad Sales Director

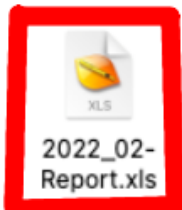


Figure 1. Hijacked email thread (observed by BitSight)

When opened, the attached Excel file asks the user to enable the macros:

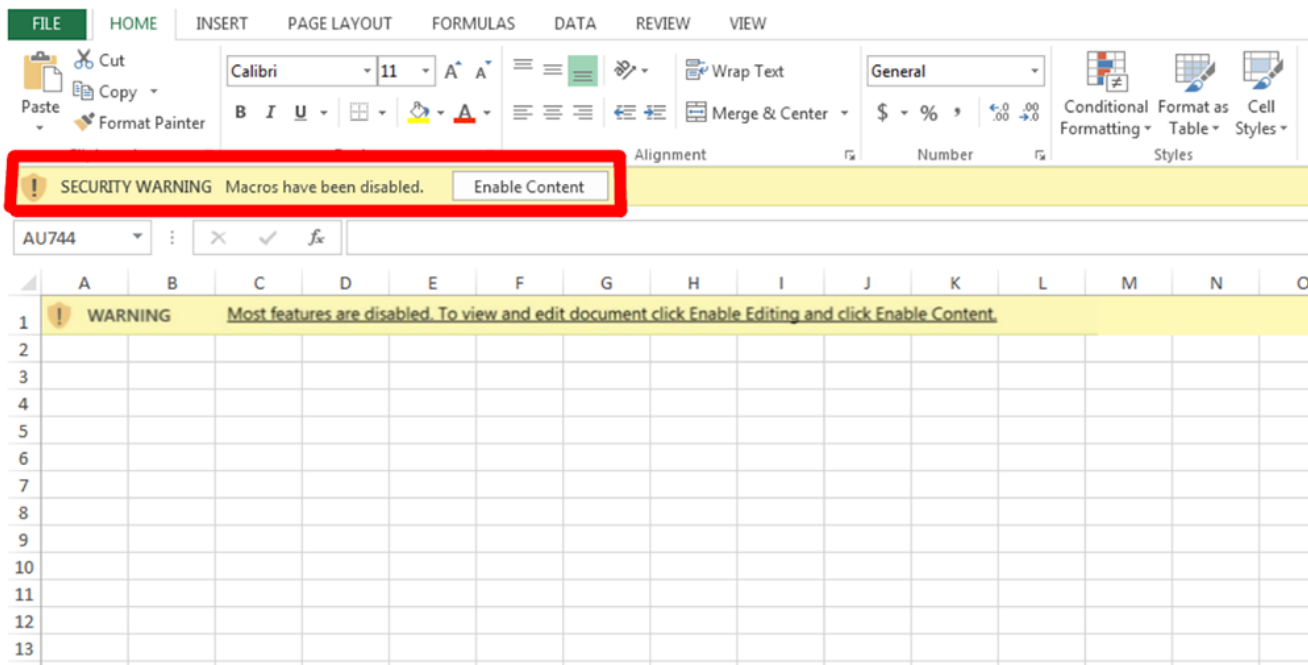


Figure 2. Emotet XLS file (observed by BitSight)

Once the user clicks “Enable Content,” Excel runs a macro that will try to download and execute the Emotet payload. Below, we can see what a complete process tree looks like when the macros are enabled:

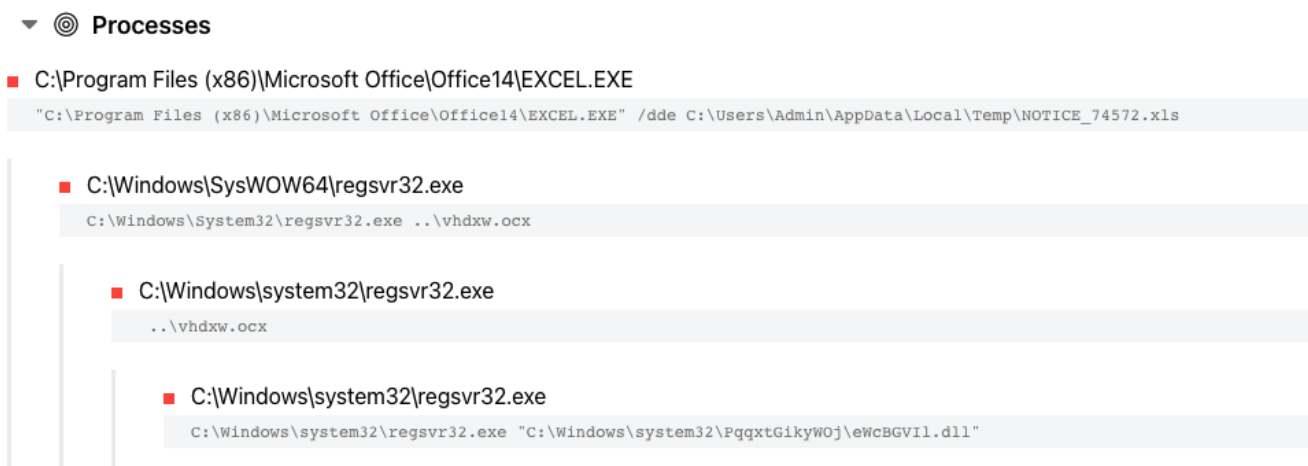


Figure 3. Emotet infection process tree (<https://tria.ge/220517-g92l5sgac3/>)

As seen above, the process tree ends with Emotet being launched via regsvr32.exe.

If the compromised user has administrator privileges, Emotet sets up persistence by creating a Windows service that will run automatically. If the user has regular permissions, a new key gets added under the Windows registry key "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run".

Once installed, Emotet starts polling tasks from the command and control servers. These tasks can instruct the bot to either execute an Emotet module or a third-party malware.

Typically, we see Emotet trying to steal information (email client passwords, email contacts, email threads, and saved browser credentials) and turn the victim's computer into a spam bot capable of sending emails using the stolen credentials.

In some cases, we see Emotet trying to install third-party malware, which means that the botnet operators will provide access to other threat actors that operate a different type of malware. Since the re-emergence of Emotet, we have seen Emotet delivering malware such as CobaltStrike, Qbot, and SystemBC.

Emotet Infections on the Rise

Since March 2022, BitSight has observed Emotet targeting more than 3 million unique email addresses with spam.

Total targets

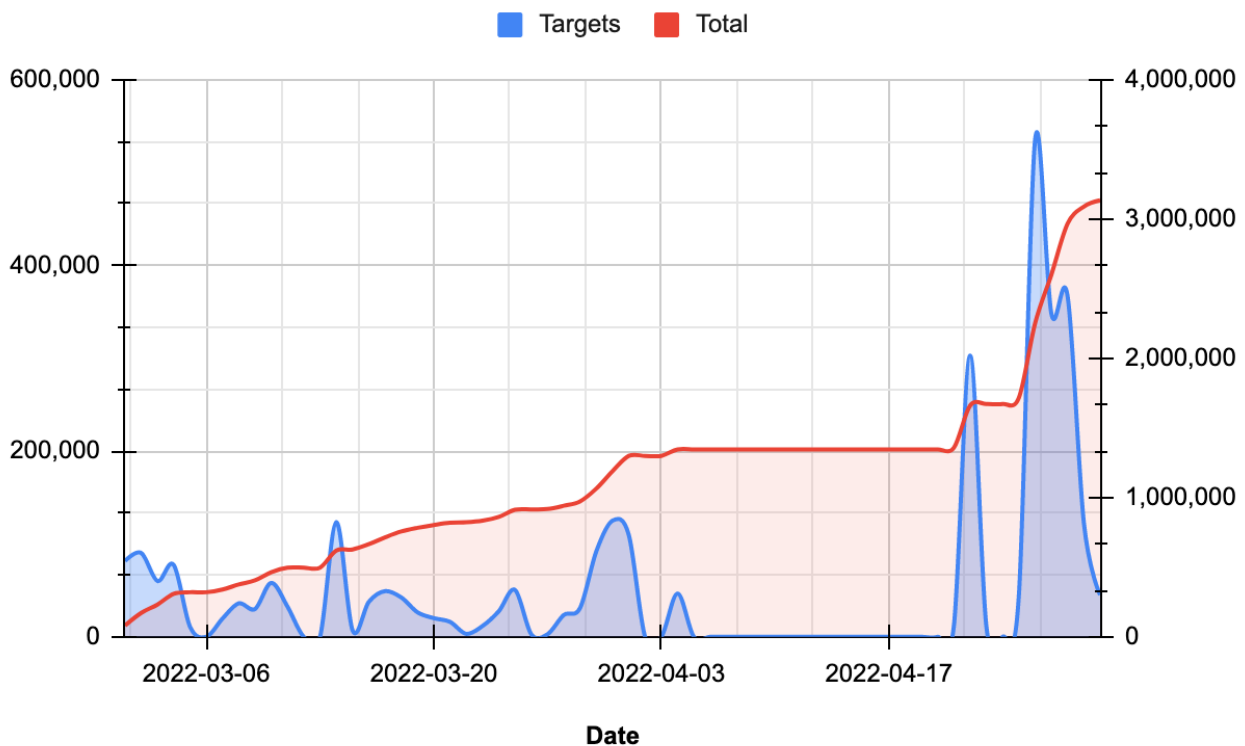


Figure 4. Total targets (observed by BitSight)

One thing that is interesting to note about Emotet is that there are occasionally time periods where no emails are sent at all. This is typical of Emotet's behavior, and usually comes when the operators are working on an update to the malware. Time periods of no activity are

typically followed by periods of heightened activity when a new wave of spam emails is being sent.

Effectiveness of Emotet in Collecting Credentials

Since March 2022, BitSight has observed more than 300,000 unique stolen email credentials, suggesting that Emotet is again becoming a significant malware threat.

Total stolen credentials

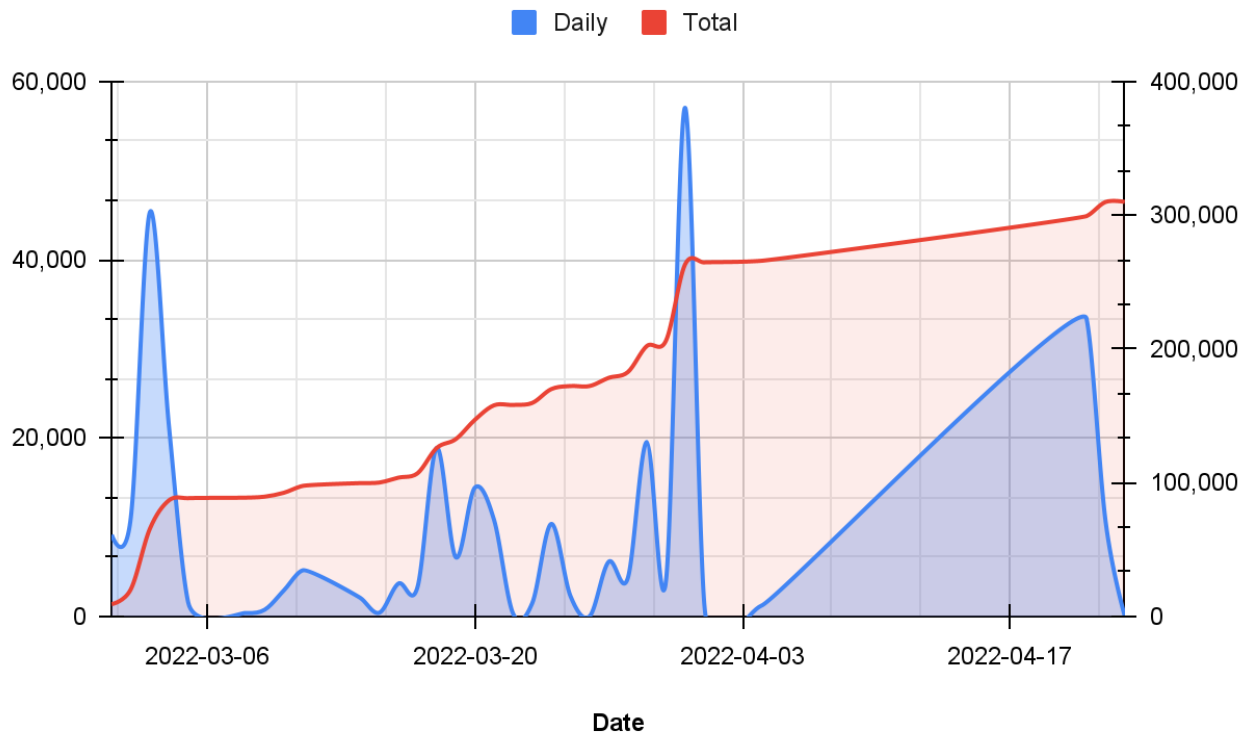


Figure 5. Total stolen credentials (observed by BitSight)

Japan and Italy in the Crosshairs

While BitSight observes a significant number of top-level domains being targeted, Japan stands out as one of the most targeted top-level domains. Our observations are consistent with [previous reports](#) from Japan's CERT, JPCC, describing the rise in Emotet infections affecting Japanese email addresses. Besides the interest in Japan, Emotet regularly targets Italy with malicious email campaigns.

Since the beginning of March, we have seen .COM, .IT (Italy), and .JP (Japan) as the three most targeted top-level domains within the spam targets. The remaining top-level domains that complete the top 10 list of most targeted TLDs are: .BR, .MX, .NET, .CA, .FR, .ID, and .DE.

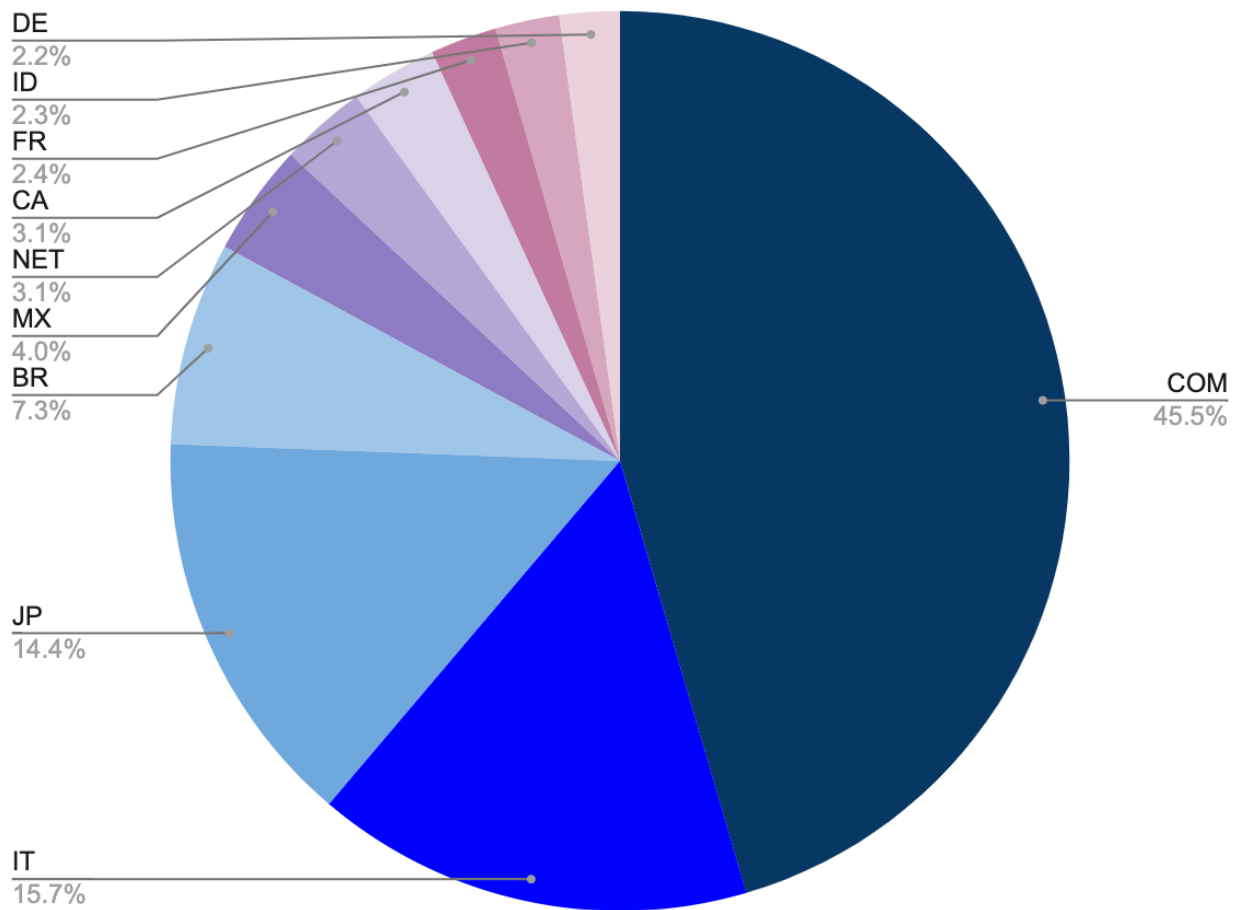


Figure 6. Spam targets top 10 TLD (observed by BitSight)

During the same period, we have observed that .COM, .JP, and .MX (Mexico) are the top-level domains that are observed to have the highest number of stolen email credentials. The remaining top-level domains that complete the top 10 list of TLDs within the stolen credentials are: .IT, .BR, .NET, .ZA, .IN, .ID, and .AR.

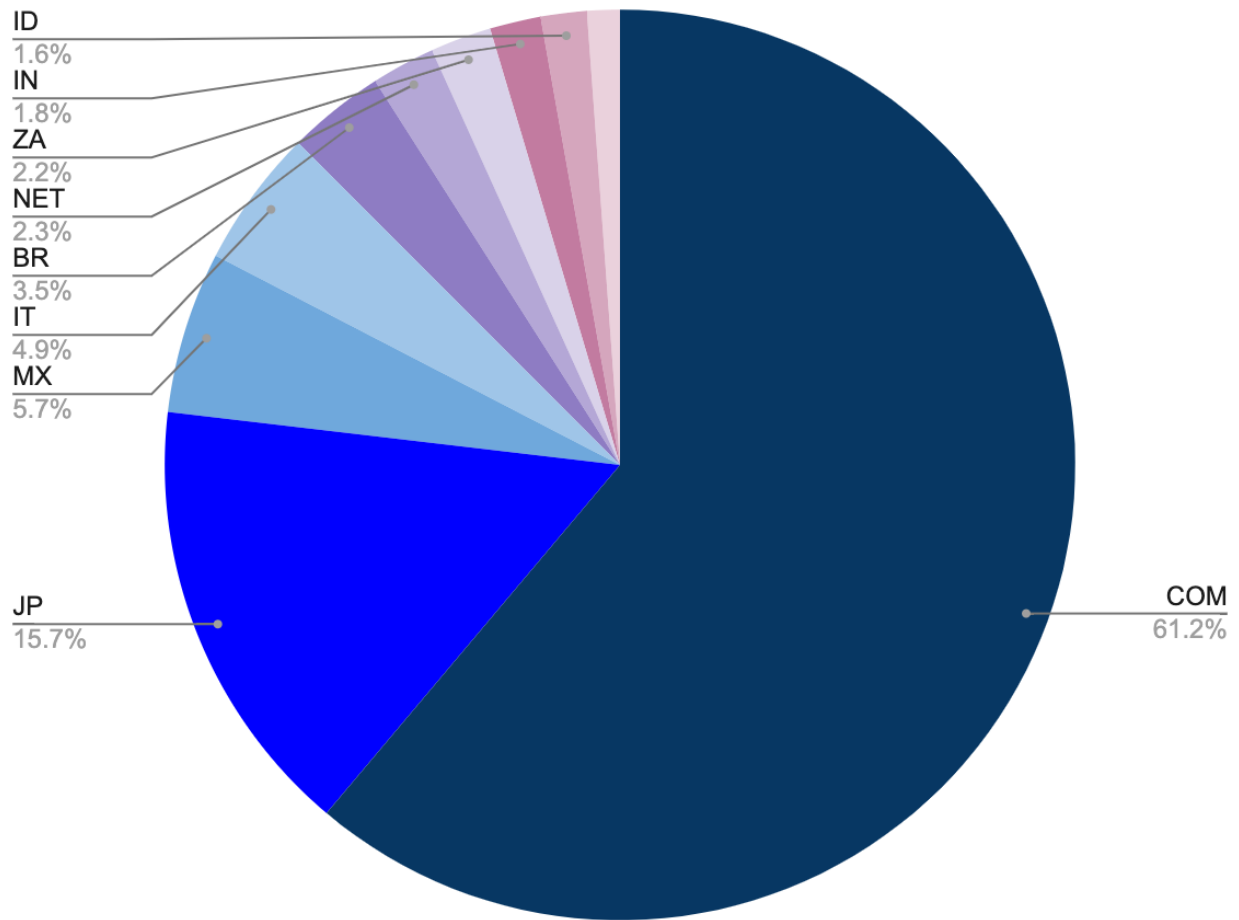


Figure 7. Stolen SMTP accounts top 10 TLD (observed by BitSight)

Ransomware: The Rapidly Evolving Trend



Ransomware: The Rapidly Evolving Trend

Ransomware attacks have been rising at an alarming rate — with victims ranging from one of the largest fuel suppliers in the United States to Ireland’s Department of Health. Download our ebook to learn more about:

- The latest tactics used by ransomware groups
- BitSight’s analysis of data on hundreds of ransomware events
- Best practices to protect your organization

[Download eBook](#)

[Button Arrow](#)

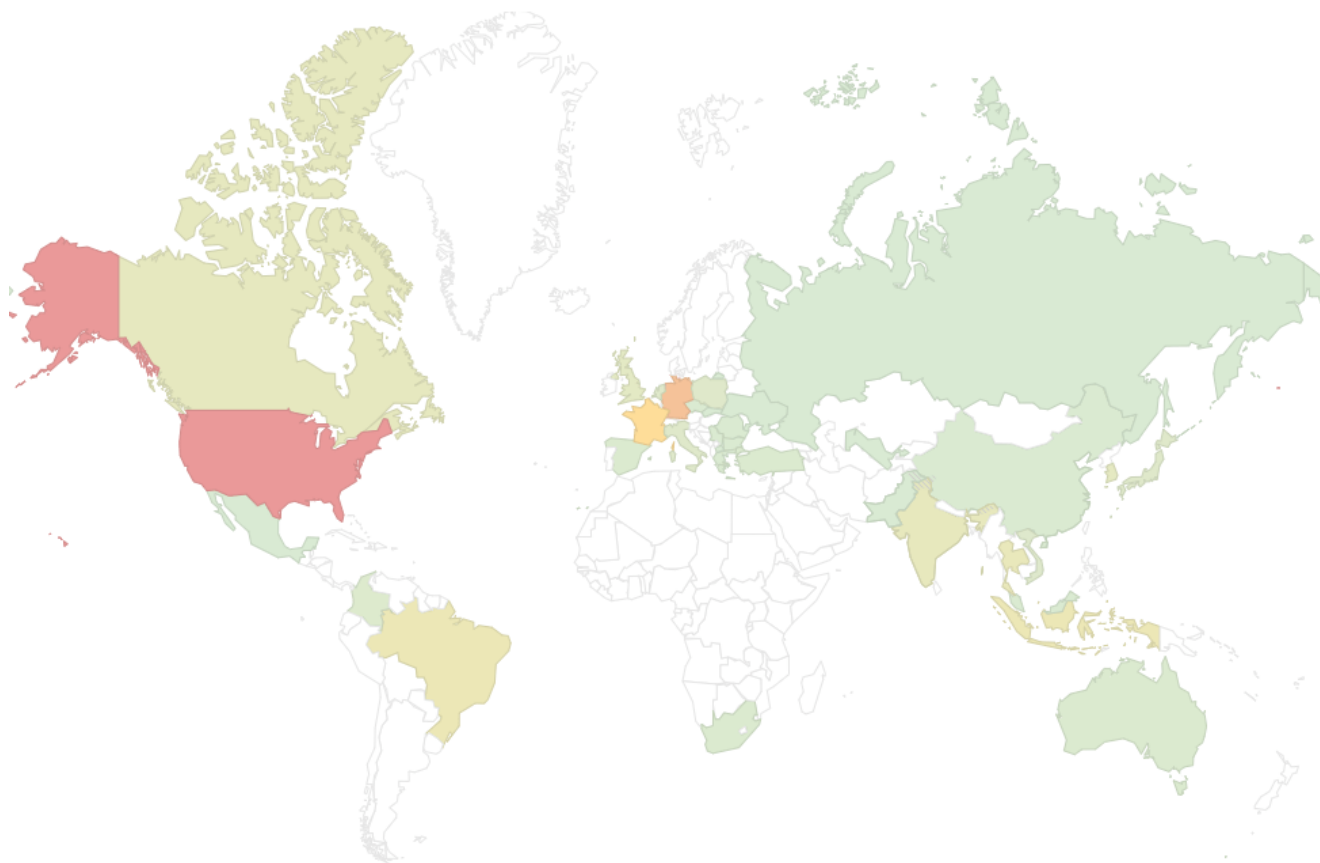
Global Distribution of Command and Control Systems

Before the takedown, Emotet had three distinct botnets (Epoch1, Epoch2, and Epoch3). Currently, Emotet already has two botnets, known as Epoch4 and Epoch5.

The botnets have a tiered infrastructure where their command and control (Tier-1 C2) server IP addresses are hard-coded within the malware samples. These servers are reverse proxies that forward bot requests to upstream servers (Tier-2 C2), which in turn forward requests to another tier of upstream servers (Tier-3 C2), and so on.

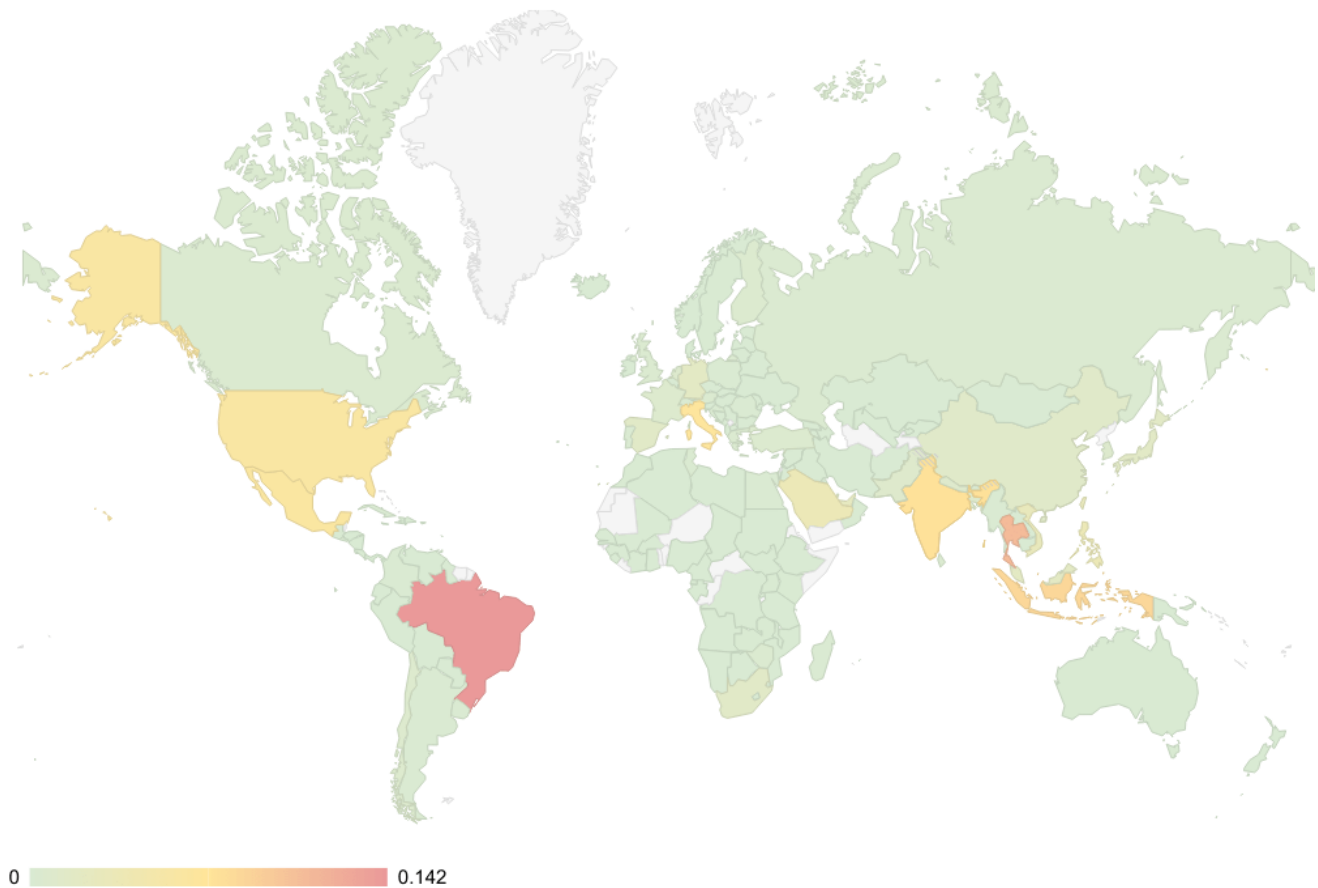
BitSight has identified a total of 339 Tier-1 C2s. These servers were most prevalent in the US, Germany, and France. Other countries observed hosting a high number of Tier-1 C2s include: Singapore, Brazil, Indonesia, Thailand, South Korea, Canada, and the UK. These 10 countries hosted roughly 70% of the identified Tier-1 C2s.

In all, BitSight observed a total of 47 countries hosting Tier-1 C2s. The map below highlights the distribution of these servers by country (red indicates the highest number of servers).



Global Distribution of Emotet Infected Systems

Network telemetry of the communications with the Tier-1 C2s since the beginning of March allowed us to estimate the distribution of Emotet infected systems around this time. We can easily see that, by now, there are infected systems, or bots, all over the world. Based on that telemetry, the most affected countries are: Brazil, Thailand, and Indonesia. These three countries amount to roughly 33% of all infected systems. The remaining countries in the top 10 of countries with most infections are: India, Italy, Mexico, United States, Saudi Arabia, Philippines, and Vietnam. The top 10 amount to 69% of all infected systems.



Responding to Emotet: Best Practices and IOCs

Emotet is a notorious malware family that has resurfaced after suffering a takedown. Organizations should treat it as a significant adversary to their infrastructures since it can cause lots of damage to them and enable access to other criminals, such as ransomware operators. Emotet is most likely still in a growing/testing phase and recovering from the effects of a takedown. Nevertheless, organizations should know that this threat is back and, once again, targeting companies worldwide.

The main spread method for Emotet is via email malicious files or links, so following cyber risk best practices and preventing the opening of suspicious emails is the best preemptive measure to avoid getting infected. BitSight has published a short list of [cyber risk best practices](#).

For network administrators, please consider adding BitSight's IOCs IP list to traffic filtering solutions to successfully prevent compromised systems communicating effectively with their C2 servers, downloading and installing further malware. BitSight is sharing the Tier-1 C2 IOC list here: https://github.com/bitsight-research/threat_research/blob/main/emotet/emotet.csv

Get the Weekly Cybersecurity Newsletter

Subscribe to get security news and industry ratings updates in your inbox.

-

- *

[Read more](#)

By checking this box, I consent to sharing this information with BitSight Technologies, Inc. to receive email and phone communications for sales and marketing purposes as described in our [privacy_policy](#). I understand I may unsubscribe at any time.