Emotet and Trickbot: The Battle of the Botnets

Published: 2021-04-12 · Archived: 2026-04-05 17:53:17 UTC

Emotet began as a banking trojan in 2014 — but from this inauspicious start, it grew to become "the world's most dangerous malware" according to Europol, and one of the Cybersecurity and Infrastructure Security Agency's "most prevalent ongoing threats."

The botnet earned its reputation in a number of ways.

- **It was strikingly common**. By 2021, Emotet was involved in one-third of malware attacks.
- **It was resilient.** The botnet was capable of spreading laterally once it had gotten access to just a small number of devices in a network.
- **It was targeted.** One Emotet module collected a portion of each email in a victim's inbox, enabling highly targeted phishing attempts capable of replying to and quoting legitimate emails.
- **It was automated.** Once it gained control of a device, it distributed itself to the user's contacts and attempted to brute force its way onto any other devices connected over the same network.

And in many cases, it was just the beginning. In the SonicWall 2021 Cyber Threat Report, we detailed the meteoric rise of Ryuk ransomware. While Ryuk is certainly formidable in its own right (see rapid growth in graph below), a key to its swift success was the leg up it received in the form of Emotet. Emotet was offered for hire to Ryuk operators, who used access already established by Emotet to deploy the ransomware upon networks of those deemed valuable targets.

To compare it to crime in the physical space, consider a group of burglars with plans to rob a bank. What would be easier: finding a way to break in themselves, or hiring someone on the inside to simply leave a door open?

The End of Emotet

But in the end, it was Emotet's success and versatility that led to its downfall. In response to the rampant proliferation of the botnet, law-enforcement agencies from at least eight different countries formed a multinational organization with the goal of disrupting it and taking it down.

In January 2021, law enforcement and judicial authorities succeeded in gaining control of the servers used by Emotet. Then, they replaced the Emotet malware on these servers with a harmless file created by law enforcement. By preventing new devices from downloading the malware, the spread of Emotet to additional targets was halted.

While this disruption will likely prevent a number of infections — some costing more than a million dollars to mitigate — in the short term, the long-term impact remains much less clear.

As Fernando Ruiz, Europol's European Cybercrime Centre head of operations, told ZDNet, "We expect it will have an impact because we're removing one of the main droppers in the market. For sure there will be a gap that other criminals will try to fill, but for a bit of time, this will have a positive impact on cybersecurity."

History Repeating

It's possible that, in a best-case scenario, this disruption will eliminate Emotet for good, and have a long-term positive effect on the amount of malware going forward.

For an idea of how a worst-case scenario might play out, however, we only have to look back about six months — to none other than the rumored Emotet heir apparent, Trickbot.

Since its development in late 2016, the operators of Trickbot have successfully infected over a million devices globally. As with Emotet, there are a variety of factors that contribute to make Trickbot an oversized threat, including its ever-evolving modular capabilities, ability to infect IoT devices and its proficiency at stealing information.

But it was Trickbot's potential to deploy ransomware or DDoS attacks in advance of the 2020 U.S. presidential election that presented the most pressing danger.

Hoping to prevent a large-scale disturbance in the democratic process, Microsoft obtained a court order allowing it to shut down Trickbot's operations. In a joint effort with global telecommunications companies, Microsoft was able to disable Trickbot's infrastructure, taking down new servers that Trickbot was attempting to use as replacements almost as soon as they went online. The actual operation itself took less than a week, and by October 18, 2020, the vast majority of Trickbot's critical infrastructure had been disabled.

While the takedown was a success in terms of preventing election tampering, this respite wasn't long-lived: By the time the U.S. Electoral College held its confirmation vote in December, Trickbot was already showing signs of a resurgence. A new version was spotted that included upgraded means of evading detection, along with other features. And in January, ZDNet reported a malware campaign that "has the hallmarks of previous Trickbot activity."

Will Emotet take a similar path and come roaring back to life? We don't know yet, but with so much money to be made, it certainly isn't out of the realm of possibility.

In the meantime, the takedown of Emotet in early 2021 seems to be fueling the ongoing resurgence in Trickbot, which is rising to fill the void left behind.

Until both are gone for good, the best protection against botnets like Emotet and Trickbot is a sound and proven security posture, frequent software and firmware updates, and comprehensive cybersecurity awareness. The latter includes everyday vigilance and adherence to best practices, along with staying up to date on current trends in cybercrime.

For more on Ryuk, Emotet and other malware, download the 2021 SonicWall Cyber Threat Report.

Know The Threats. Know Your Exposure.

Download the complete 2021 SonicWall Cyber Threat Report to find out how 2020 changed cybercrime forever — and what you need to do to stay ahead of the latest threats in 2021 and beyond.

READ IT NOW

Securing Smart Cities Over Distributed Networks

Re-envisioning distributed community networks using smart end-to-end security and centralized management.

READ THE BRIEF

Holding Federal Government Agencies for Ransom

Recent ransomware attacks on government have become all the more pertinent in light of geopolitical tensions. This brief explores known steps you can take to help prevent being a victim.

READ THE BRIEF

How to Increase Access and Security for Today's Schools

Mobility, cloud apps and emerging threats demand more from today’s next-gen firewall. This brief examines critical network security needs for today’s school networks and explores best practices for selecting an effective next-generation firewall platform.

READ THE BRIEF

What’s the Best NGFW for State and Local Governments?

State and local governments are increasingly dependent on cloud-based apps and mobile connectivity. This brief examines critical network security needs for today's agencies and explores best practices for selecting an effective next-generation firewall platform.

READ THE BRIEF

Best Practices for Global Endpoint Security Operations for MSSPs and Distributed Enterprises

Concerns, considerations and guidelines for a multi-tenant environment.

READ THE BRIEF

Securing IT Ecosystems for Higher Education

Higher education and information technology are inseparable. Today's complex higher education IT ecosystem requires unified network security.

READ THE BRIEF

Source: https://blog.sonicwall.com/en-us/2021/04/emotet-and-trickbot-the-battle-of-the-botnets/