Emotet Malware Returns in 2022 | Deep Instinct

By Chuck EverettеDirector, Cybersecurity Advocacy

Published: 2022-06-09 · Archived: 2026-04-05 13:30:31 UTC

Emotet malware started from humble beginnings as a banking Trojan in 2014. The threat actors behind Emotet have been credited as one of the first criminal groups to provide Malware-as-a-Service (MaaS). They successfully utilized their MaaS to create a massive botnet of infected systems and sold access to third parties, an enterprise that proved so effective it was soon being used by criminal entities such as the Ryuk and Conti ransomware gangs. Emotet also has a history of collaborating with Trickbot, famous for their info-stealing trojan, and Qakbot, another well-known banking trojan.

Emotet Malware: Phishing for victims throughout the pandemic

The Emotet group was prolific throughout the pandemic. They wreaked chaos throughout 2019 and 2020 taking advantage of hot topics as a ruse to convince unsuspecting victims to open malicious phishing emails. Topics included coronavirus information, political news, controversial issues, and supposed state and federal updates around mask mandates.

This all changed for Emotet in January 2021 when a joint task force took down the Emotet botnet infrastructure in a global operation involving eight countries led by Europol, the Netherlands, and the U.S.

Is Emotet malware back from the dead? New Emotet variants emerge

Ransomware gangs with millions in incentives to stay active are difficult to tamp down for long. As we've seen multiple times in the past, ransomware gangs — or at a minimum their source code — never seem to expire completely.

Historically, members of gangs that have been shut down or disbanded tend to flock to other criminal organizations. Ransomware gangs are criminals at the core, and as such their sole purpose is to make money. The Emotet group is no different. Initial reports show that Emotet had reemerged in Q4 of 2021 and really started making waves with reports of massive phishing campaigns targeting Japanese businesses in February and March of 2022. We've now seen several massive new malicious phishing campaigns in April and May targeting new regions.

In an interesting development, the TrickBot gang has been observed helping its longtime partner Emotet deploy to already infected machines in order to download the new Emotet variants. It has been that Emotet detections have spiked upwards of 2700% in Q1 of 2022 compared to Q4 of 2021.

Emotet 2022: New tricks and threats

Looking at the new threats coming from Emotet in 2022 we can see that there has been an almost 900% increase in the use of Microsoft Excel macros compared to what we observed in Q4 2021. The attacks we have seen hitting Japanese victims are using hijacked email threads and then using those accounts as a launch point to trick victims into enabling macros of attached malicious office documents. One of the more troubling behaviors of this "new and improved" Emotet is its effectiveness in collecting and utilizing stolen credentials, which are then being weaponized to further distribute the Emotet binaries.

Key Findings of Emotet's Return in 2022

Threat research teams, including Deep Instinct's leading threat intel team, and HP's Wolf Security, have identified the following key findings:

- 9% of threats are unknown, never-before-seen threats
- 14% of the email malware has bypassed at least one email gateway security scanner before it was captured
- 45% of the malware detected were utilizing some type of office attachment
- The most common attachments used to deliver malware were spreadsheets (33%), executables and scripts (29%), archives (22%), and documents (11%)
- Emotet is now utilizing 64bit shell code, as well as more advanced PowerShell and active scripts
- Almost 20% of all malicious samples were exploiting a 2017 Microsoft vulnerability (CVE-2017-11882)

Deep Instinct's Solution for Combatting Emotet Malware

While Emotet has reemerged and is gaining strength, it still utilizes many of the same attack vectors it has exploited in the past. The issue is that these attacks are getting more sophisticated and are bypassing today's standard security tools for detecting and filtering out these types of attacks.

But here's the news you've been waiting for: here at Deep Instinct, we have a long history of predicting and preventing these types of attacks. While some of the latest attack vectors are new and never-before-seen threats, Deep Instinct has a proven track record of preventing even the newest attacks from Emotet as well as other sophisticated threat groups with technology that was developed and deployed months (and in some cases even years) before the threats were developed and deployed into the wild.

Deep Instinct takes a prevention-first approach to stopping ransomware and other malware using the world's first purpose-built, deep learning cybersecurity framework. We predict and prevent known, unknown, and zero-day threats in <20 milliseconds, 750X faster than the fastest ransomware can encrypt.

For more information, Contact Us or Request a Demo.
