KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Emotet rises with sophisticated attacks and evasion techniques

Tracker ID: TN1012 **Date:** 20/Oct/2022 **Category:** Threat Actor **Industry:** All **Region**: All

Background

Threat actors connected to the prominent Emotet malware have been observed changing their tactics and command-and-control (C2) infrastructure to evade detection. Emotet is a highly elusive and destructive malware delivery system that did significant harm during its initial reign. Following a coordinated takedown by authorities in early 2021, Emotet has resurfaced as a global danger that will persist for organizations.

Mummy Spider, aka TA542, is the threat actor behind Emotet, which first appeared in June 2014 as a banking trojan before evolving into an all-purpose loader capable of delivering second-stage payloads such as ransomware in 2016. The IP addresses of the bulk of the identified servers were found in the United States, Germany, and France, while the majority of the Emotet modules were hosted in France, Singapore, Ghana, Korea, Thailand, and India.

While the actual infrastructure of Emotet's botnet was destroyed in January 2021, it reappeared in November 2021 via further malware known as TrickBot. Emotet's resurgence, sponsored by the now-dissolved Conti team, provided the path for Cobalt Strike infections and, more recently, Quantum and BlackCat ransomware attacks. Its attack flows are also characterized by the use of multiple target routes to remain undetected over extended periods. These assaults frequently rely on spam message waves that deliver malware-laden documents or embedded URLs that, when opened or clicked, enable the malware to be deployed.

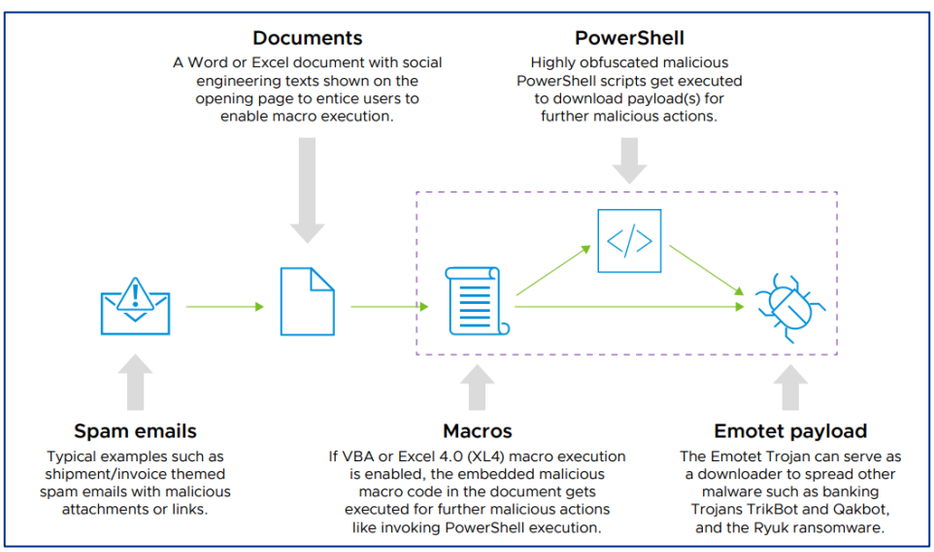

Figure1 Typical Emotet payload delivery chain | Source: VMware

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Emotet rises with sophisticated attacks and evasion techniques

Tracker ID: TN1012 **Date:** 20/Oct/2022 **Category:** Threat Actor **Industry:** All **Region**: All

Another notable characteristic of several of these infection lifecycles was the use of the legitimate executable mshta.exe to launch a malicious HTA file and then drop the Emotet virus. Threat actors typically use living-off-the-land binaries (LOLBINs), also known as mshta and PowerShell, since they are signed by Microsoft and recognized by Windows. As a result, the attacker can carry out a confused deputy attack, in which trustworthy tools carry out malicious activities. Aside from the changes to the C2 IP addresses and execution chains, Emotet has been seen propagating two new plugins: one is aimed at harvesting credit card information from the Google Chrome browser, and the other is a spreader module that goes laterally using the SMB protocol.

In January 2022 alone, there were three unique sets of attacks, each of which delivered the Emotet payload using an Excel 4.0 (XL4) macro, an XL4 macro with PowerShell, or a Visual Basic Application (VBA) macro with PowerShell. A closer look at around 25,000 different Emotet DLL artefacts reveals that 26.7% of them were discarded by Excel documents. There have been as many as 139 distinct program chains discovered. The threat actor is in charge of two new botnet clusters termed Epochs 4 and 5, as well as changing the C2 infrastructure, which has aided Emotet's revival. Before the takedown, the Emotet operation used three separate botnets known as Epochs 1, 2, and 3. In addition, between March 15, 2022 and June 18, 2022, 10,235 Emotet payloads were discovered in the wild.

MITRE ATT&CK Tactics

Defense Evasion, and Command and Control.

Recommendations

- Implement regular phishing awareness and training throughout the workplace. Make sure employees are aware of any active phishing threats. Refrain from opening untrusted links and email attachments without verifying their authenticity.
- Check that all security software components are enabled on all systems and that a policy is in place requiring the administrator password to be entered in the event of attempts to disable protection.
- Provide a prevention, detection and response framework for protecting email accounts, content and communications. Threat actors commonly use email to proliferate malware, spam and phishing attacks, so it’s important to protect email privacy and integrity.
- Continuously monitor for suspicious or anomalous activities. Collect logs from all critical devices, security controls, and endpoints in a central location for correlation and analysis that can uncover TTPs.
- Follow multilayered defense solutions and active monitoring to detect threats before operators can launch their attacks.
- Dynamically analyze file behaviors for threats by using AI and machine learning (ML) to detect malicious code.

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Emotet rises with sophisticated attacks and evasion techniques

Tracker ID: TN1012 **Date:** 20/Oct/2022 **Category:** Threat Actor **Industry:** All **Region**: All

- Implement policy and technical controls that enforce a Zero Trust model to restrict access to all networks, systems, applications and processes. Allow only the minimal access required to perform assigned functions.
- Remove all default, shared and hard-coded authentication processes in place of stronger authentication mechanisms. Encourage the use of multifactor authentication practices where feasible.
- Conduct regular penetration testing and vulnerability assessments to understand and reduce your potential attack surface.
- Monitor everyday activities and traffic across the network and investigate possible anomalies to find any yet-to-be-discovered threats that could lead to a security breach.
- Secure end-to-end connectivity for applications, including end users, microservices, APIs and data, to reduce the spread and lateral movement of threats.

References

- Ravie Lakshmanan, New Report Uncovers Emotet's Delivery and Evasion Techniques Used in Recent Attacks, The Hacker News, 10th October 2022, External Link (thehackernews.com).
- Vmware Security, Vmware Report Exposes Emotet Malware's Supply Chain, 10th October 2022, External Link (news.vmware.com).
- Robert Lemos, Emotet Rises Again With More Sophistication, Evasion, Dark Reading, 11th October 2022, External Link (www.darkreading.com).

In case of a Security Incident, please report to IN-FM KPMG SOC.

For any query or feedback, feel free to reach us at IN-FM KPMG CTI.

KPMG in India Cyber Response Hotline : +91 9176471471

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia