/logpoint
The resurgence of a crippling malware:
How to threat hunt Emotet

Dec 15, 2022 15:42 CET

The resurgence of a crippling malware: How to threat hunt Emotet

- **Logpoint research reveals that Emotet has developed into a Loader-as-a-Service - a dropper of other malware**
- **Logpoint recommends looking out for its common TTPs, IoCs, and malicious macros to detect Emotet**

COPENHAGEN, Denmark & BOSTON, December 15, 2022 – Emotet keeps coming back with renewed force. Despite being taken down by authorities in 2021, it's back again and rapidly evolving. Emotet is now a Loader-as-a-service downloading other malware and wreaking havoc for an increased number of organizations. Logpoint's research team has closely monitored Emotet's emergence, attack patterns, and possible detections to help organizations stop it before it becomes a threat.

An analysis of multiple malware samples reveals that Emotet has changed its tactics from stealing credentials in the banking sector to stealing other sensitive data and acting as a dropper to distribute other malware like IcedID, Trickbot, or Ruyk. Initial access is done mainly through malspam, emails in bulk containing malware, or a link to download it. From the static and dynamic analysis, Logpoint uncovered multiple files, domains, and botnet networks that are still active in the wild.

"Emotet is the most detected malware sample on many platforms. The fact that there has been a variant for several years and it still manages to bypass defenses is a true testament to its amazing adaptability," says Doron Davidson, VP Logpoint Global Services. "At Logpoint, we're working to stop threats like Emotet in their tracks before they wreak havoc and cause detrimental damage."

To safeguard your organization against Emotet, Logpoint recommends to:

- Look out for common Tactics, Techniques and Procedures (TTPs) used by Emotet
- Familiarize yourself with known Indicators of Compromise (IoC) and ensure you can detect and block them.
- Look out for malicious macros, like a download of a macro-enabled document, and delete or isolate the spawned and child processes.
- Isolate the endpoints, i.e., in case of an attack, isolate the system, take proper logs, evaluate the situation and remediate.

Read Logpoint's blog post about Emotet here, and access the full Emerging Threats Protection Report, Emotet-ually Unstable - The resurgence of a nuisance. The report offers in-depth vulnerability analysis, means to detect and respond to the threat, and insights about incident investigation and response.

About Logpoint

Logpoint safeguards society in a digital world by helping customers and

Managed Security Service Providers (MSSPs) detect cyberattacks. Combining reliable technology with a deep understanding of cybersecurity challenges, Logpoint makes security operations easier, giving organizations the freedom to progress. Logpoint's SIEMand NDRtechnologies improve visibility and give a multi-layered approach to cybersecurity that helps customers and MSSPs in Europe navigate the complex threat landscape. Headquartered in Copenhagen, Denmark, Logpoint has a European foundation and is the only European SIEM vendor with a Common Criteria EAL3+ certification. This demonstrates Logpoint's strong focus on data protection and cybersecurity regulations. For more information, visit http://logpoint.com.

Contacts

Maimouna Corr Fonsbøl
Press Contact
Head of PR
PR & Communications
mcf@logpoint.com
+45 25 66 82 98