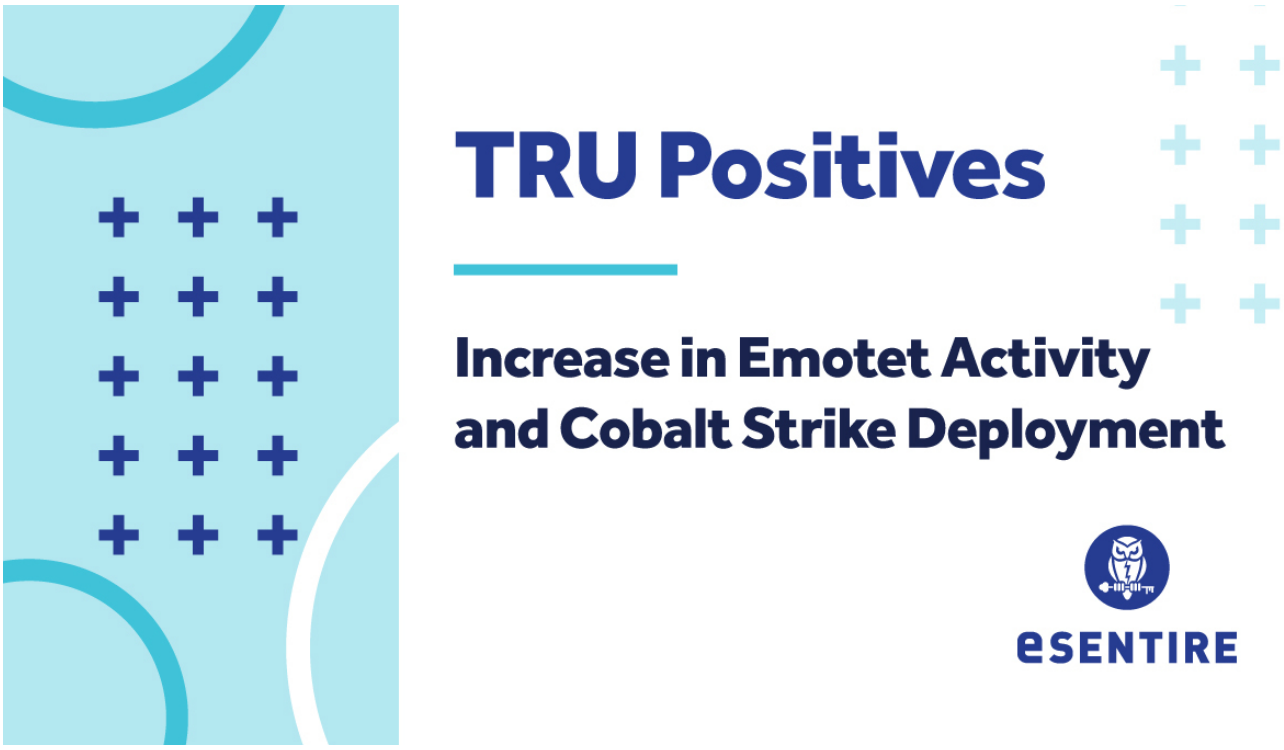
Increase in Emotet Activity and Cobalt Strike Deployment

esentire.com/blog/increase-in-emotet-activity-and-cobalt-strike-deployment



Adversaries don't work 9-5 and neither do we. At eSentire, our 24/7 SOCs are staffed with Elite Threat Hunters and Cyber Analysts who hunt, investigate, contain and respond to threats within minutes.

We have discovered some of the most dangerous threats and nation state attacks in our space – including the Kaseya MSP breach and the more_eggs malware.

Our Security Operations Centers are supported with Threat Intelligence, Tactical Threat Response and Advanced Threat Analytics driven by our Threat Response Unit – the TRU team.

In TRU Positives, eSentire's Threat Response Unit (TRU) provides a summary of a recent threat investigation. We outline how we responded to the confirmed threat and what recommendations we have going forward.

Here's the latest from our TRU Team…

What did we find?

- We found Emotet, a former banking malware, now focused on loading or delivering follow-on malware.
    - Emotet was disrupted in early 2021 but made a comeback in November 2021.
    - Historically, Emotet has installed malware such as Trickbot or Qakbot, which in turn have led to hands-on-keyboard adversaries and ransomware deployment.
- In December 2021, researchers closely monitoring Emotet reported instances of the malware deploying the Cobalt Strike intrusion tool.
- In February 2022, other researchers have reported Cobalt Strike deployment within 5 hours of an Emotet infection originating from the Epoch 5 botnet.
- The direct deployment of the intrusion tool is a concern considering its use in hands-on-intrusions linked to ransomware deployment and extortion attacks.

    Deploying the tool directly expedites network intrusion actions, requiring defenders to act swiftly to contain patient zero or risk the attacker expanding the scope of their access.
- eSentire security teams have identified and disrupted multiple Emotet infections across our customers in recent weeks, none of which escalated to Cobalt Strike deployment.
- These incidents followed the typical Emotet trajectory with macro-laced office files arriving via email resulting in code execution through VBScript and PowerShell.

How did we find it?

Recent activity has been identified through a mix of threat hunting activity and detections from BlueSteel, our machine-learning PowerShell classifier.

What did we do?

- In instances where Emotet activity was identified, our team of 24/7 SOC Cyber Analysts isolated the host(s) and worked with the customer to remediate the threat.
- TRU deployed additional detection content based on the analysis of recent incident observations.

What can you learn from this TRU positive?

- Given the threat of the direct deployment of Cobalt Strike, rapid identification and containment of hosts infected with Emotet is critical now more than ever.
- Infected systems should be examined for presence of Cobalt Strike or other follow-on malware. Emotet stores a copy of itself and Cobalt Strike in C:\Users\user\AppData\Local\Temp\random-directory-name\.

Recommendations from our Threat Response Unit (TRU) Team:

Loader malware attempts to install other malware, so the first priority should be to identify and investigate the presence of follow-on malware on systems. In addition, we recommend:

- Employ email filtering and protection measures.
  - Block or quarantine email attachments such as EXEs, Password Protected ZIPs, JavaScript, Visual Basic scripts.
  - Implement anti-spoofing measures such as DMARC and SPF.
  - Employ an MFA solution to reduce impact of compromised credentials.
  - Train users to identify and report suspicious emails and documents, even if opened.
- Protect your endpoints against malware.
  - Ensure antivirus signatures are up to date.
  - Use a Next-Gen AV (NGAV) or Endpoint Detection and Response (EDR) product to detect and contain threats.
  - Limit or disable macros across the organization. See UK's National Cyber Centre guidance on Macro Security.

Ask Yourself…

> Is your malware identification and remediation process agile enough to disrupt follow-on attacks stemming from loader malware?

If you're not currently engaged with a Managed Detection and Response provider, we highly recommend you partner with us for security services in order to disrupt threats before they impact your business.

Want to learn more? Connect with an eSentire Security Specialist.