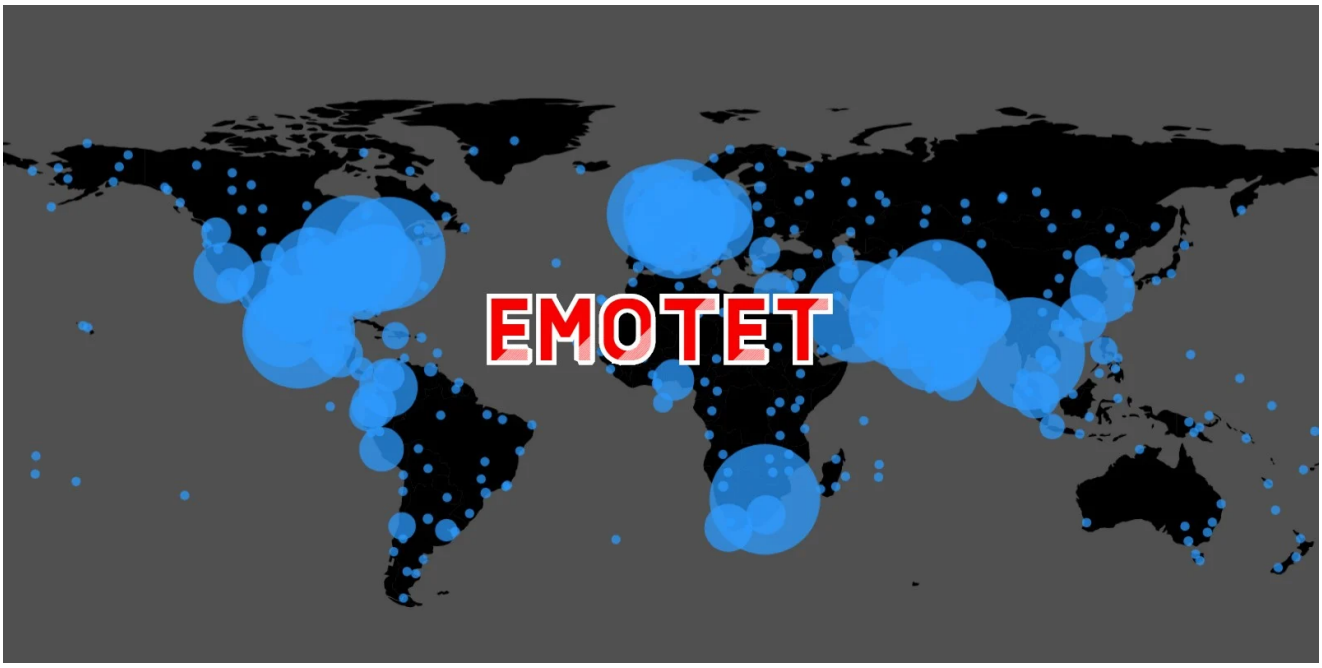
Emotet now drops Cobalt Strike, fast forwards ransomware attacks

bleepingcomputer.com/news/security/emotet-now-drops-cobalt-strike-fast-forwards-ransomware-attacks/

Lawrence Abrams

By
Lawrence Abrams

- December 7, 2021
- 06:21 PM
- 0



In a concerning development, the notorious Emotet malware now installs Cobalt Strike beacons directly, giving immediate network access to threat actors and making ransomware attacks imminent.

Emotet is a malware infection that spreads through spam emails containing malicious Word or Excel documents. These documents utilize macros to download and install the Emotet Trojan on a victim's computer, which is then used to steal email and deploy further malware on the device.

Historically, Emotet would install the TrickBot or Qbot trojans on infected devices. These Trojans would eventually deploy Cobalt Strike on an infected device or perform other malicious behavior.

Cobalt Strike is a legitimate penetration testing toolkit that allows attackers to deploy "beacons" on compromised devices to perform remote network surveillance or execute further commands.

However, Cobalt Strike is very popular among threat actors who use cracked versions as part of their network breaches and is commonly used in ransomware attacks.

Emotet changes its tactics

Today, Emotet research group Cryptolaemus warned that Emotet is now skipping their primary malware payload of TrickBot or Qbot and directly installing Cobalt Strike beacons on infected devices.

> WARNING We have confirmed that #Emotet is dropping CS Beacons on E5 Bots and we have observed the following as of 10:00EST/15:00UTC. The following beacon was dropped: https://t.co/imJDQTGqxV Note the traffic to lartmana[.]com. This is an active CS Teams Server. 1/x
>
> — Cryptolaemus (@Cryptolaemus1) December 7, 2021

A Flash Alert shared with BleepingComputer by email security firm Cofense explained that a limited number of Emotet infections installed Cobalt Strike, attempted to contact a remote domain, and then was uninstalled.

"Today, some infected computers received a command to install Cobalt Strike, a popular post-exploitation tool," warns the Cofense Flash Alert.

"Emotet itself gathers a limited amount of information about an infected machine, but Cobalt Strike can be used to evaluate a broader network or domain, potentially looking for suitable victims for further infection such as ransomware."

"While the Cobalt Strike sample was running, it attempted to contact the domain lartmana[.]com. Shortly afterward, Emotet uninstalled the Cobalt Strike executable."

This is a significant change in tactics as after Emotet installed its primary payload of TrickBot or Qbot, victims typically had some time to detect the infection before Cobalt Strike was deployed.

Now that these initial malware payloads are skipped, threat actors will have immediate access to a network to spread laterally, steal data, and quickly deploy ransomware.

"This is a big deal. Typically Emotet dropped TrickBot or QakBot, which in turn dropped CobaltStrike. You'd usually have about a month between first infection and ransomware. With Emotet dropping CS directly, there's likely to be a much much shorter delay," security researcher Marcus Hutchins tweeted about the development.

This rapid deployment of Cobalt Strike will likely speed up ransomware deployment on compromised networks. This is especially true for the Conti ransomware gang who convinced the Emotet operators to relaunch after they were shut down by law enforcement in January.

Cofense says that it is unclear if this is a test, being used by Emotet for their own network surveillance, or is part of an attack chain for other malware families that partner with the botnet.

> "We don't know yet whether the Emotet operators intend to gather data for their own use, or if this is part of an attack chain belonging to one of the other malware families. Considering the quick removal, it might have been a test, or even unintentional." - Cofense.

Researchers will closely monitor this new development, and as further information becomes available, we will update this article.

Related Articles:

Malicious PyPI package opens backdoors on Windows, Linux, and Macs

Microsoft: Sysrv botnet targets Windows, Linux servers with new exploits

New cryptomining malware builds an army of Windows, Linux bots

Eternity malware kit offers stealer, miner, worm, ransomware tools

Historic Hotel Stay, Complementary Emotet Exposure included

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.