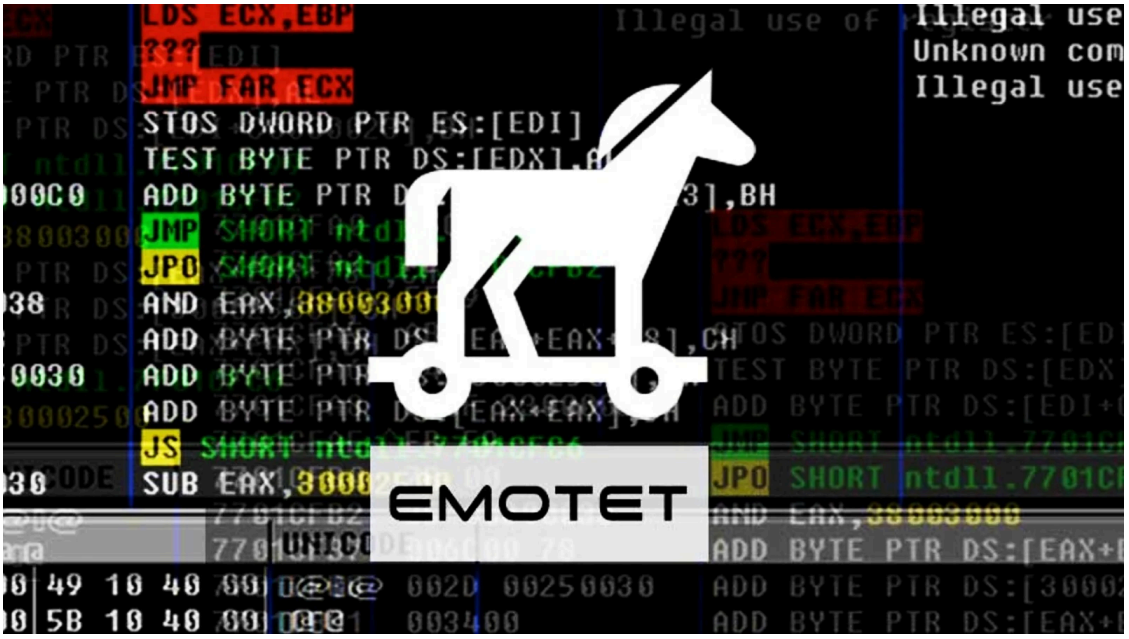
Emotet starts dropping Cobalt Strike again for faster attacks

By Lawrence Abrams

Published: 2021-12-15 · Archived: 2026-04-05 13:35:36 UTC

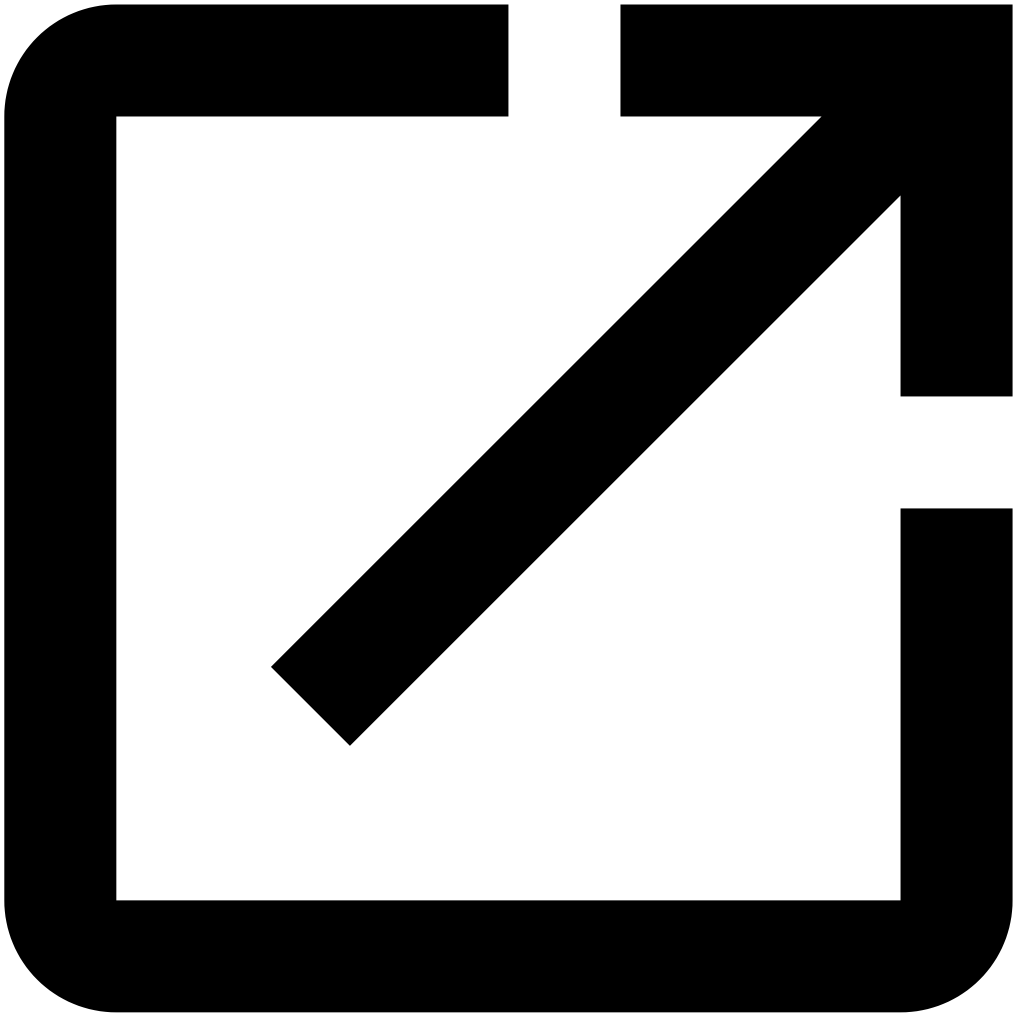


Right in time for the holidays, the notorious Emotet malware is once again directly installing Cobalt Strike beacons for rapid cyberattacks.

For those not familiar with Emotet, it is considered one of the most widespread malware infections and is distributed through phishing emails that include malicious attachments.

Historically, once a device becomes infected, Emotet will steal a victim's email to use in future campaigns and then drops malware payloads, such as TrickBot and Qbot.


DIE LINKE.
0:00



However, earlier this month, Emotet began to test installing Cobalt Strike beacons on infected devices instead of their regular payloads.

Cobalt Strike is a legitimate pentesting tool that threat actors commonly use to spread laterally through an organization and ultimately deploy ransomware on a network.

This test was brief, and the threat actors soon went back to distributing their typical payloads.

Emotet resumes Cobalt Strike installs

Last week, the Emotet threat actors suspended their phishing campaigns, and since then, researchers have not seen any further activity from the group.

"Spamming stopped last week on Thursday, and since then, they have been quiet with very little of ANYTHING going on until today." Joseph Roosen of the Cryptolaemus Emotet group told BleepingComputer.

However, Cryptolaemus is now warning that starting today, the threat actors have once again begun installing Cobalt Strike beacons to devices already infected by Emotet.

Roosen told BleepingComputer that Emotet is now downloading the Cobalt Strike modules directly from its command and control server and then executing them on the infected device.

With Cobalt Strike beacons directly installed by Emotet, threat actors who use them to spread laterally through a network, steal files, and deploy malware will have immediate access to compromised networks.

This access will speed up the delivery of attacks, and with it being right before the holidays, it could lead to numerous breaches since enterprises now have limited staff to monitor for and respond to attacks.

C2 communications disguised as jQuery

In a sample of the Cobalt Strike beacon shared with BleepingComputer, the malware will communicate with the attacker's command and control servers through a fake 'jquery-3.3.1.min.js' file.

Each time the malware communicates with the C2, it will attempt to download the jQuery file, which will have a variable changed with new instructions each time, as shown by the highlighted text in the image below.

Cobalt Strike C2 traffic disguised as a jQuery JavaScript file

As most of the file is legitimate jQuery source code, and only some content is changed, it blends into legitimate traffic and makes it easier to bypass security software.

The rapid deployment of Cobalt Strike through Emotet is a significant development that should be on the radars of all Windows and network admins and security professionals.

With this increased distribution of beacons to already infected devices, it is anticipated that we will see an increased number of corporate breaches and ultimately ransomware attacks right before or during the holidays.

Source: https://www.bleepingcomputer.com/news/security/emotet-starts-dropping-cobalt-strike-again-for-faster-attacks/