A vigilante is sabotaging the Emotet botnet by replacing malware payloads with GIFs

By Written by Catalin Cimpanu, ContributorContributor July 24, 2020 at 9:41 a.m. PT

Archived: 2026-04-05 19:44:42 UTC

Image: Snapshot from Kung Fury movie

Executive guide

An unknown vigilante hacker has been sabotaging the operations of the recently-revived Emotet botnet by replacing Emotet payloads with animated GIFs, effectively preventing victims from getting infected.

The sabotage, which started three days ago, on July 21, has grown from a simple joke to a serious issue impacting a large portion of the Emotet operation.

According to Cryptolaemus, a group of white-hat security researchers tracking the Emotet botnet, the vigilante is now poisoning around a quarter of all Emotet's payload downloads.

What's actually happening -- the simplified version

Emotet is a complex and multi-component machinery. For readers to understand what's really happening here, a quick intro into Emotet's internal structure and distribution mechanism is needed.

The botnet works by spamming targets with emails perpetrating to be business-related communications. These emails either contain a malicious Office document, or a link to a malicious Office file that users are told to download on their PCs.

When users open one of these files and they press links inside the file or enable the "Enable Editing" feature to allow macros (automated scripts) to execute, the automated scripts download the Emotet malware and various of its components from the internet.

By "the internet" we actually mean "hacked WordPress sites" where the Emotet gang temporarily stores their malware's components (or "payloads" in infosec jargon).

These temporary hosting locations are also Emotet's Achilles' heel.

The Emotet gang controls these hacked sites via web shells -- a type of malware installed on hacked servers to let intruders manipulate the server.

But the Emotet gang isn't using the best web shells available on the market. As it was pointed out last year, the Emotet gang uses open-source scripts and also employs the same password for all of its web shells, exposing its infrastructure to easy hijacks if anyone can guess the web shell's password.

> The Emotet payload distribution method is super insecure, they deploy an open source webshell off Github into the Wordpress sites they hack, all with the same password, so anybody can change the payloads infected PCs are receiving.
>
> — Kevin Beaumont (@GossiTheDog) December 27, 2019

The Emotet sabotage

Emotet, considered today's most dangerous malware strain/botnet, was recently silent for more than five months and came back to life last week.

Since Tuesday, an unknown vigilante appears to have discovered this common password and has been abusing this weakness botnet to sabotage Emotet's comeback.

The unknown intruder has been replacing Emotet payloads on some of the hacked WordPress sites with animated GIFs -- which means that when Emotet victims open the malicious Office files, they won't get infected as the Emotet malware won't get downloaded and executed on their systems.

Over the past three days, the intruder has replaced the Emotet payloads with multiple popular GIFs.

The first, spotted on Tuesday, is this Blink 182 "WTF" GIF.

On the second day, the attackers moved to using a James Franco GIF.

After that, we had the Hackerman GIF.

> 国内の #Emotet 設置サイトの傾向に変化はありません。
> choiphui[.]com
> 133.130.109.0
> (PTR: v133-130-109-0[.]a038[.]g[.]tyo1[.]static[.]cnode[.]io.)
> linhgiangcorp[.]com
> 133.130.97.61

> (PTR: v133-130-97-61[.]a026[.]g[.]tyo1[.]static[.]cnode[.io.)
> HACKERMAN のgifに置き換わっています。 pic.twitter.com/efxnbfaGfc
>
> — tike (@tiketiketikeke) July 24, 2020

The GIFs are usually taken either from Imgur or Giphy, two GIF-hosting services at random.

Defacements are impacting Emotet activity

The current defacements started slow, but currently, around a quarter of all daily Emotet payload links are being replaced with GIFs, causing serious operational losses to the Emotet gang.

According to Cryptolaemus member Joseph Roosen, the Emotet gang is more than aware of this issue. In a conversation yesterday, Roosen told ZDNet the Emotet botnet has been down on Thursday, as the Emotet gang apparently tried to root out the attacker from their web shells network.

Despite Emotet's efforts, Roosen said that today, the vigilante was still present and replacing Emotet payloads with GIF files, albeit the Emotet gang was quicker than before at spotting the "replacement" and restoring the original payload.

Overall, the defacements appear to have caused Emotet activity to seriously go down this week.

"Since Ivan [the Emotet admin] was having technical difficulties today, the hashes are way down and we barely saw much of anything," Roosen wrote in a daily Emotet update.

The security researcher estimates that Emotet is now working at around a quarter of its normal capabilities, as Ivan and the rest of the Emotet crew are still wrestling for control over their web shells.

Currently, the identity of the vigilante is unknown. Based on various theories expressed online, primary suspects include either a rival malware gang or a member of the cyber-security industry.

The 15 top malware threats facing you and your organisation

Security
