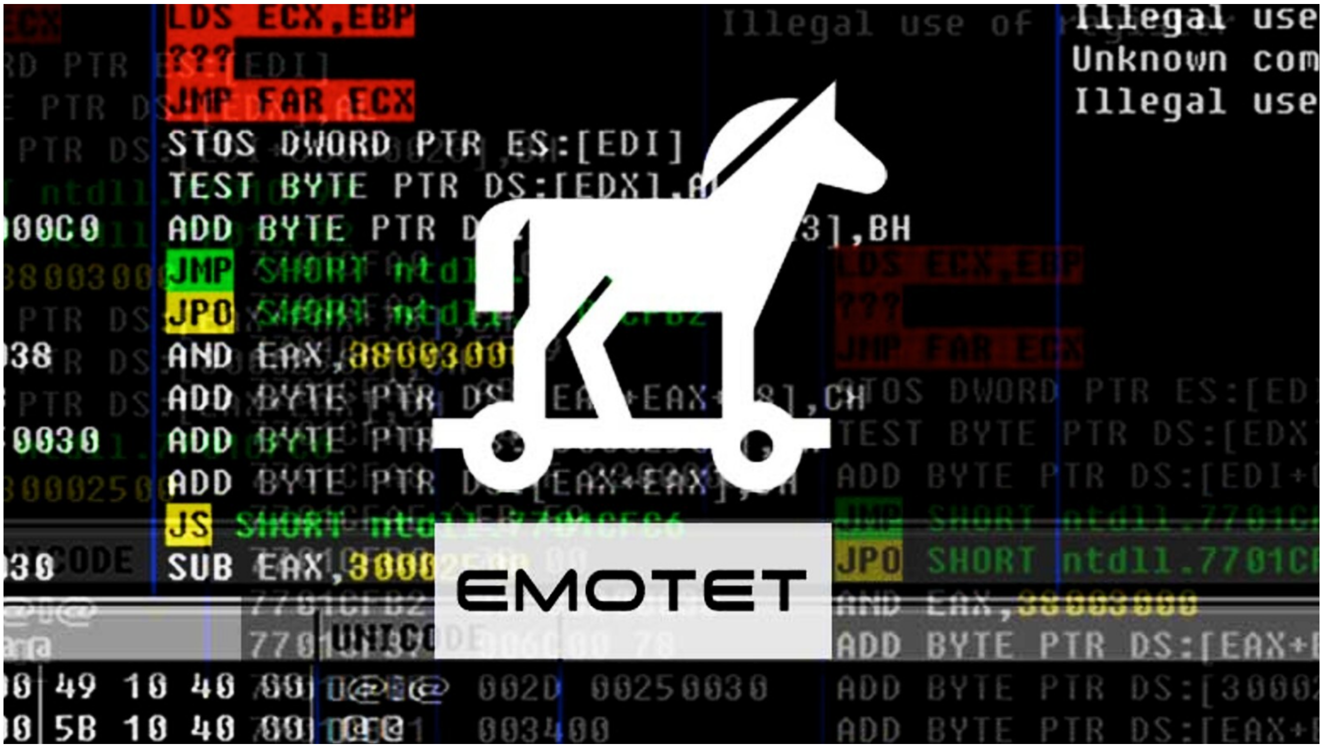
Emotet botnet switches to 64-bit modules, increases activity

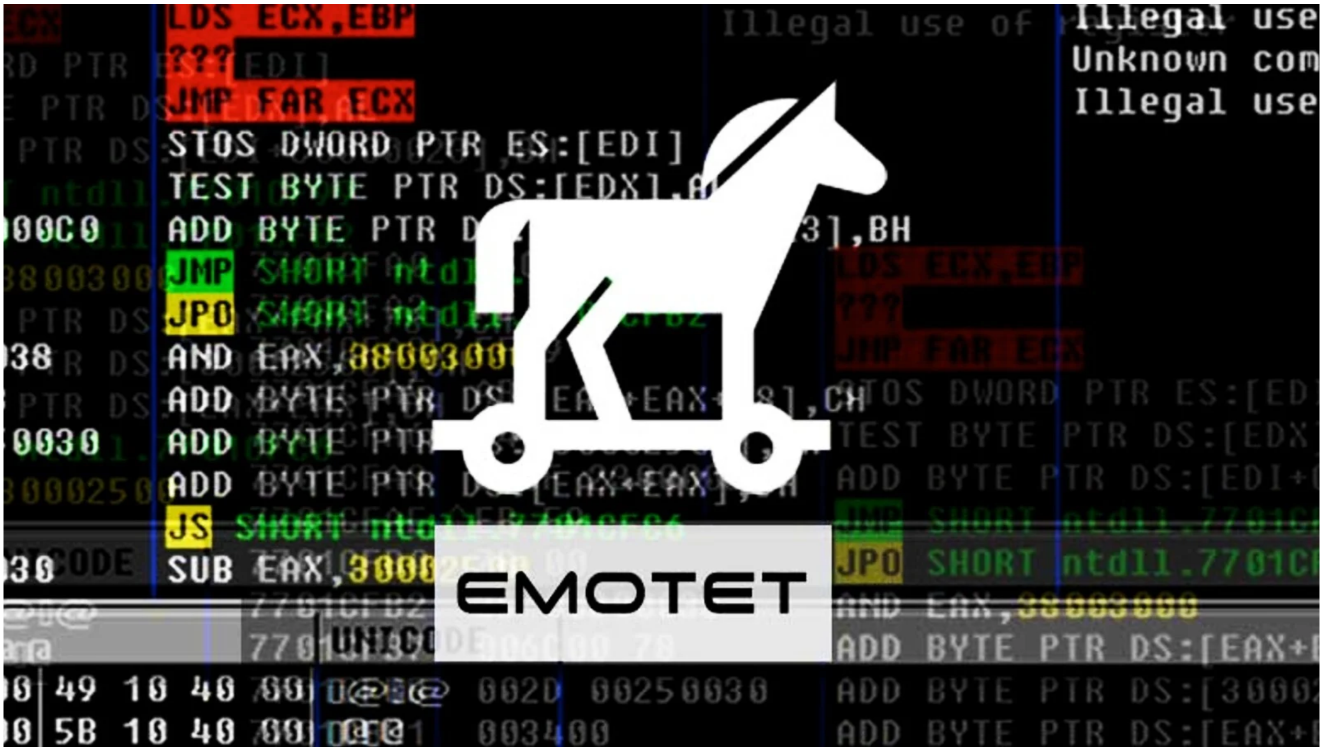
bleepingcomputer.com/news/security/emotet-botnet-switches-to-64-bit-modules-increases-activity/

Bill Toulas



By
Bill Toulas

- April 19, 2022
- 03:57 PM
- 0



The Emotet malware is having a burst in distribution and is likely to soon switch to new payloads that are currently detected by fewer antivirus engines.

Security researchers monitoring the botnet are observing that emails carrying malicious payloads last month have increased tenfold.

Emotet is a self-propagating modular trojan that can maintain persistence on the host. It is used for stealing user data, performing network reconnaissance, moving laterally, or dropping additional payloads such as Cobalt Strike and ransomware in particular.

It has been spotted growing slowly but steadily since the beginning of the year, but its operators may be shifting up a gear now.

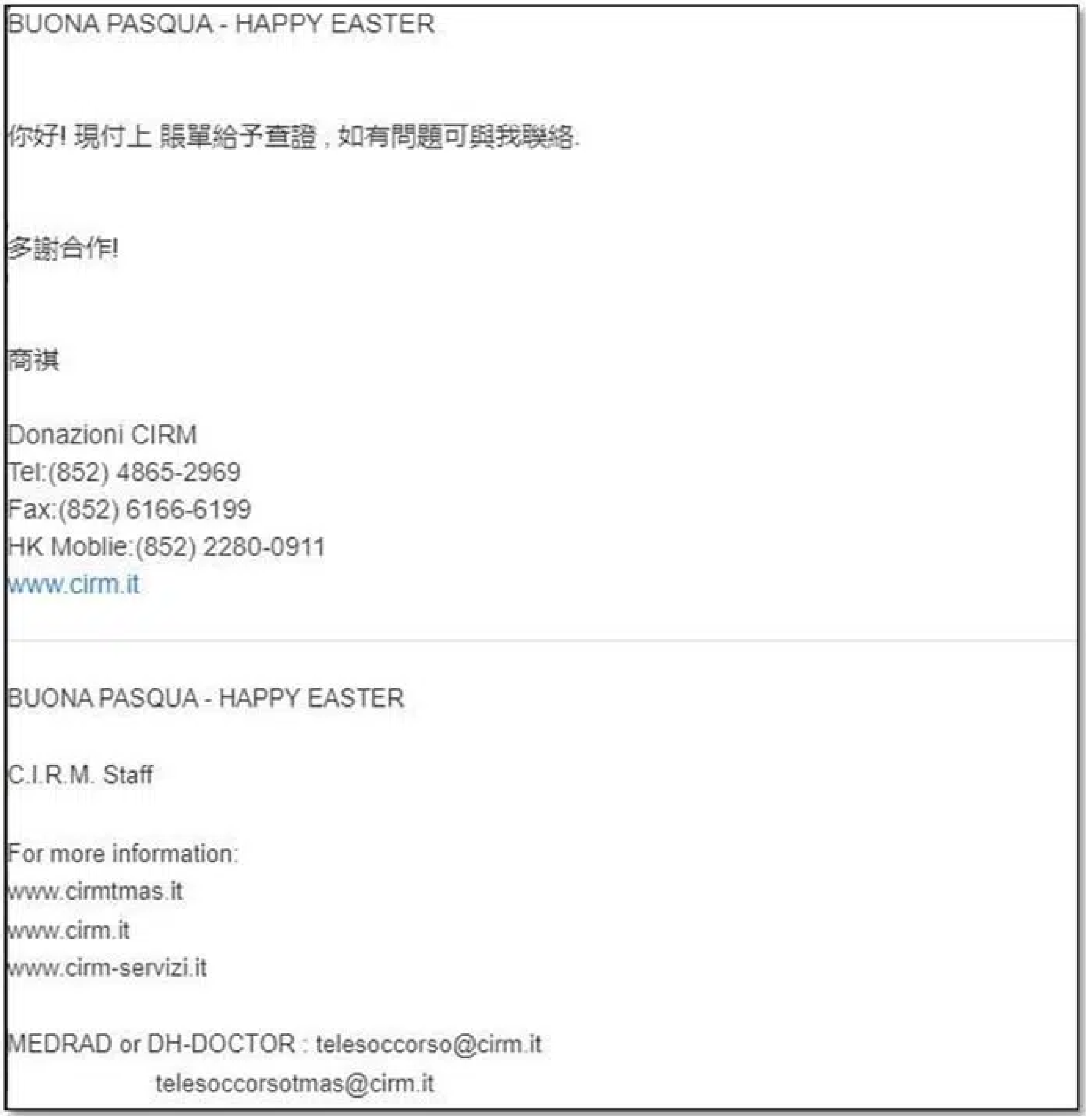
Spike in distribution

According to a report Kaspersky released today, Emotet activity is seeing a sharp rise from February to March, going from 3,000 to 30,000 emails.

The languages used in these messages include English, French, Hungarian, Italian, Norwegian, Polish, Russian, Slovenian, Spanish, and Chinese.

As for the themes, Emotet distributors are known for changing the topics regularly to take advantage of seasonal interest swifts. This time it’s the Easter celebration they're taking advantage of.

Check Point also released a report, which ranked Emotet as the number one most prevalent and active malware in March 2022.



BUONA PASQUA - HAPPY EASTER

你好! 現付上 賬單給予查證，如有問題可與我聯絡.

多謝合作!

商祺

Donazioni CIRM
Tel:(852) 4865-2969
Fax:(852) 6166-6199
HK Moblie:(852) 2280-0911
www.cirm.it

BUONA PASQUA - HAPPY EASTER

C.I.R.M. Staff

For more information:
www.cirmtmas.it
www.cirm.it
www.cirm-servizi.it

MEDRAD or DH-DOCTOR : telesoccorso@cirm.it
telesoccorsotmas@cirm.it

Emotet email using Easter lures on many languages
(Check Point)

Kaspersky mentions that the ongoing Emotet email distribution campaigns also employ discussion thread hijacking tricks, seen in Qbot campaigns linked to the same operators.

“Cybercriminals intercept already existing correspondence and send the recipients an email containing a file or link, which often leads to a legitimate popular cloud-hosting service,” Kaspersky

“The aim of the email is to convince users to either (i) follow the link and download an archived document and open it – sometimes using a password mentioned in the email, or (ii) simply open an email attachment,” the researchers note.

Because the threat actors have access to previous correspondence, it is reasonably easy for them to present the attachment as something the recipient would expect as a continuation of the discussion with colleagues.

Switch to 64-bit

The Cryptolaemus security research group, who is keeping a sharp eye on Emotet botnet activity, said that the malware operators have also switched to 64-bit loaders and stealer modules on Epoch 4, one of subgroups of the botnet that run on separate infrastructure. Previously, it relied on 32-bit code.

> #Emotet Update - Looks like Ivan laid an egg for easter and has been busy. As of about 14:00UTC today 2022/04/18 - Emotet on Epoch 4 has switched over to using 64-bit loaders and stealer modules. Previously everything was 32-bit except for occasional loader shenanigans. 1/x— Cryptolaemus (@Cryptolaemus1) April 19, 2022

The switch is not visible on Epoch 5 but the delay is expected, since Epoch 4 typically serves as a development test-bed for the Emotet operators, researchers from Cryptolaemus say.

Already, the detection rate for Epoch 4 has dropped by 60%, which is believed to be a direct result of this change.

Related Articles:

Emotet malware infects users again after fixing broken installer

Historic Hotel Stay, Complementary Emotet Exposure included

EmoCheck now detects new 64-bit versions of Emotet malware

PDF smuggles Microsoft Word doc to drop Snake Keylogger malware

Microsoft detects massive surge in Linux XorDDoS malware activity

Bill Toulas

Bill Toulas is a technology writer and infosec news reporter with over a decade of experience working on various online publications. An open source advocate and Linux enthusiast, is currently finding pleasure in following hacks, malware campaigns, and data breach incidents, as well as by exploring the intricate ways through which tech is swiftly transforming our lives.