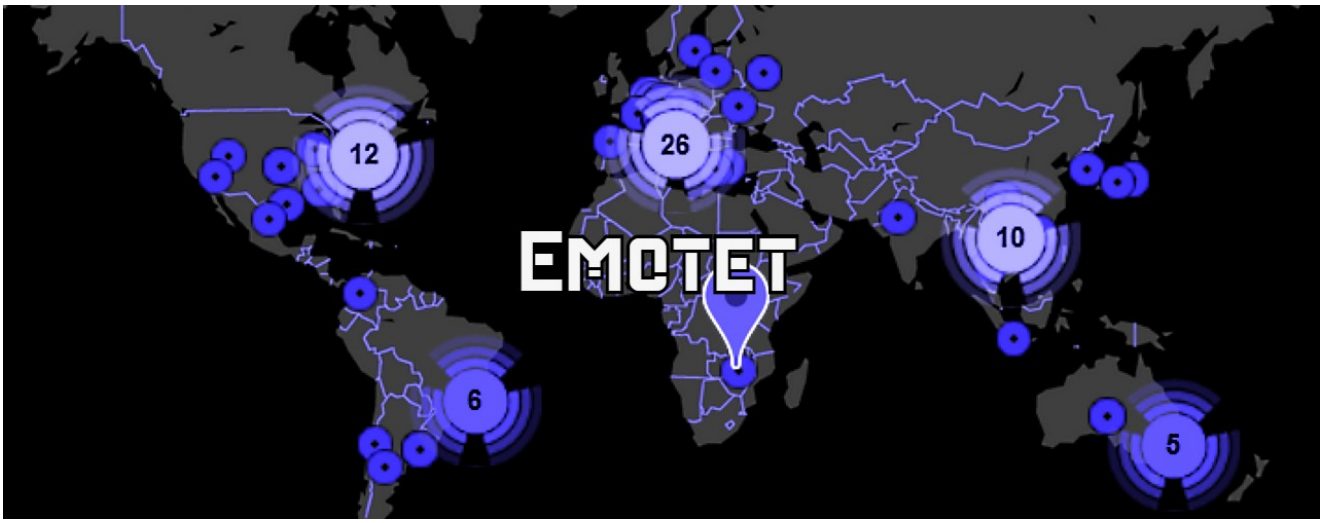
Emotet malware now steals your email attachments to attack contacts

bleepingcomputer.com/news/security/emotet-malware-now-steals-your-email-attachments-to-attack-contacts/

Sergiu Gatlan

By
Sergiu Gatlan

- July 28, 2020
- 03:21 PM
- 1



The Emotet malware botnet is now also using stolen attachments to increase the authenticity of spam emails used for infecting targets' systems.

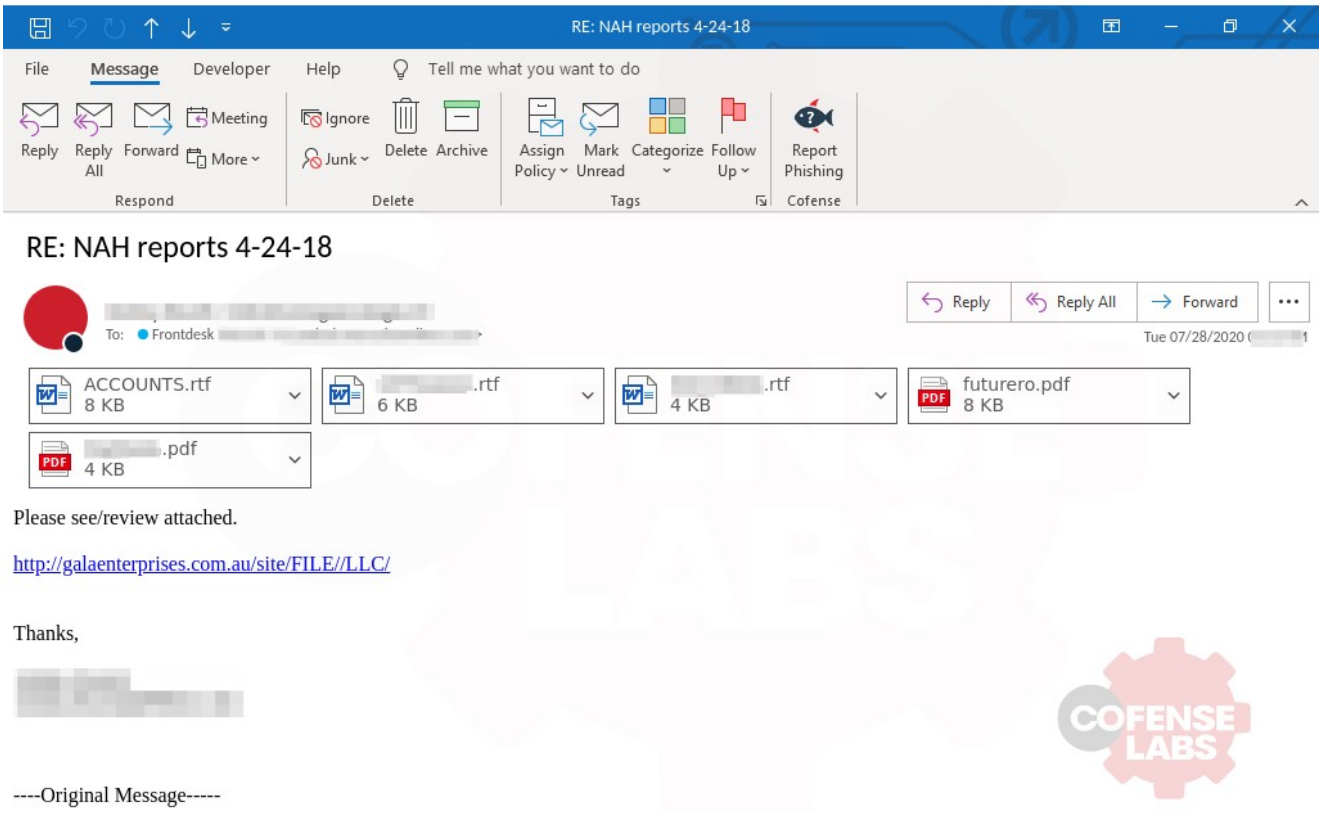
This is the first time the botnet is using stolen attachments to add credibility to emails as Binary Defense threat researcher James Quinn told BleepingComputer.

The attachment stealer module code — that also steals email content and contact lists — was added around June 13th according to Marcus 'MalwareTech' Hutchins.

Based on research from the Emotet tracking group Cryptolaemus, the malware now steals 131072 byte or smaller attachments with email contents, later to be used as part of reply chains.

This new tactic adds to the Emotet gang's leveraging of hijacked email conversation threads where a malicious URL or attachment would be included in new emails attached to existing conversations as a concealment measure (as first spotted by Minerva Labs in March 2019).

Emotet, originally a banking Trojan when first spotted in 2014, has now evolved into a malware botnet used by threat actors to download other malware families including the Trickbot (a known vector used in the delivery of Ryuk and Conti ransomware payloads) and QakBot trojans.



Emotet phishing email with stolen attachments (*Cofense*)
"Emotet seems to be using not only stolen email bodies, but is now including stolen attachments as well," email security firm Cofense said today.

"This lends to even more authenticity in their phishing emails. In one example we found 5 benign attachments and a dropper link within the templated portion of the email."

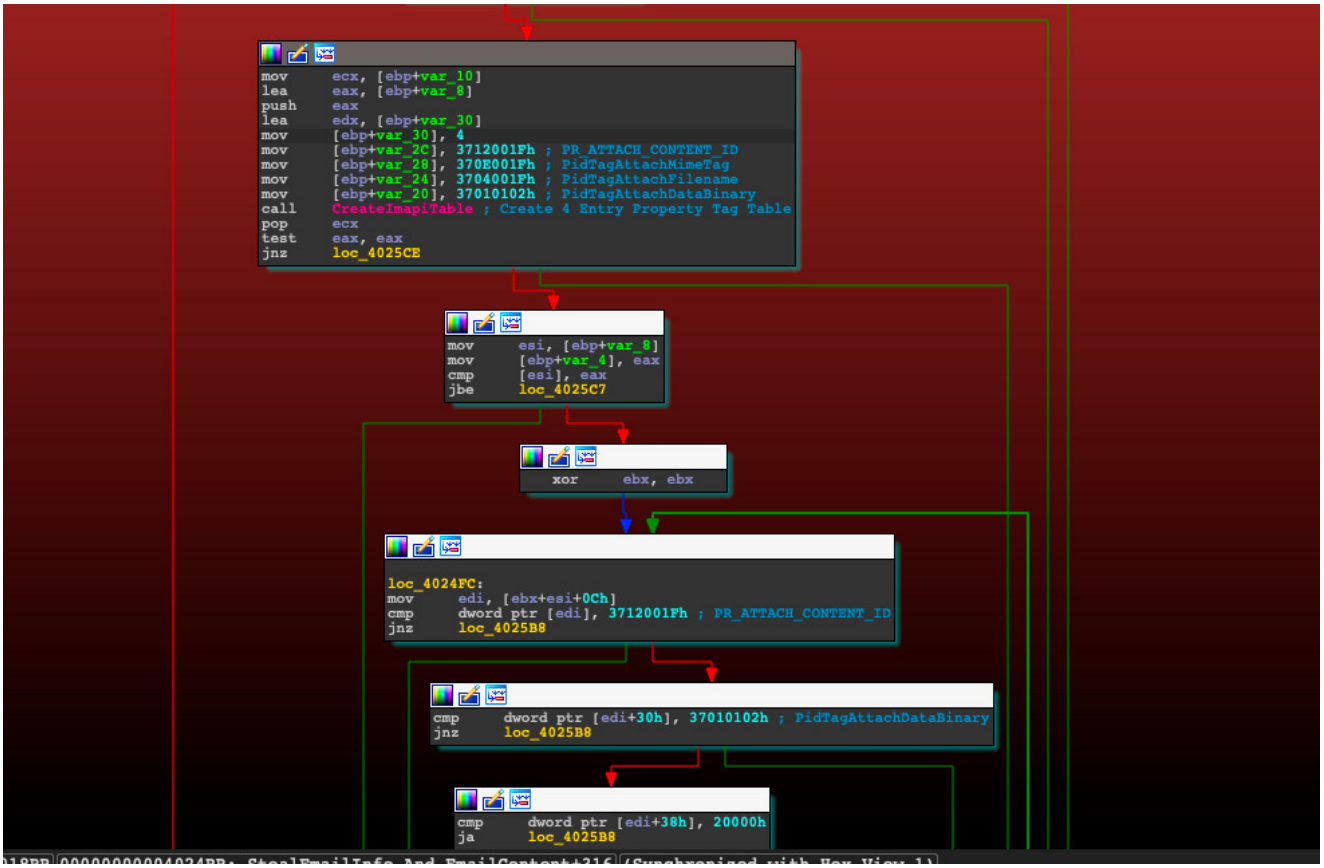
> breaking #emotet news from @CofenseLabs
>
> in addition to stolen body text, emails are now including original attachment content to add even more legitimacy.
>
> significant data breach implications, again demonstrating that emotet infections are serious https://t.co/bWbHxGWZK4
>
> — Cryptolaemus (@Cryptolaemus1) July 28, 2020

The botnet has been delivering massive amounts of malicious spam emails — camouflaged as payment reports, invoices, employment opportunities, and shipping information — through all its server clusters starting with July 17, after more than five months of inactivity.

"Since reemerging on July 17, Emotet has sustained its activities with daily spam runs spewing more than 500K emails every day (except weekends) starting at around 2:00 AM Pacific Time (UTC -7)," Microsoft said.

After returning back to life, Emotet first started installing the TrickBot trojan on compromised Windows computers, later to switch to once again heavily spreading QakBot malware, fully replacing the TrickBot payloads.

At the moment, there is no exact info on QakBot's final payloads but reports say that it will deploy ProLock ransomware on some of the systems initially infected with Emotet.



Emotet's attachment stealer module (*James Quinn*)

Most prevalent malware of the week

In a warning issued by the Australian Cyber Security Centre (ACSC) about the dangers posed by Emotet attacks, the malware is described as providing attackers "with a foothold in a network from which additional attacks can be performed, often leading to further compromise through the deployment of ransomware."

The Cybersecurity and Infrastructure Security Agency (CISA) also issued a warning on targeted Emotet attacks earlier this year, advising admins and users to review its Emotet Malware alert for guidance.

Emotet spreads using spam emails containing malicious URLs and attachments (Word or Excel documents designed to use macros) for downloading and installing the Emotet Trojan on victims' computers, which will then download other malware over time and will also use the infected device to send more spam emails.

Since the botnet was revived on July 17th, it started delivering massive amounts of Emotet malware payloads as part of campaign of malicious emails targeting users worldwide.

This huge spike of activity was behind Emotet being ranked first in a list of top 10 malware strains analyzed on the interactive malware analysis platform Any.Run during the last week, head and shoulders above the next malware in the top (the njRAT Remote Access Trojan), with more than double the number of sample uploads submitted for analysis.

> TOP10 last week's threats by uploads
>
> #Emotet 1371 (315)
> #njRAT 150 (146)
> #AgentTesla 118 (176)
> #FormBook 105 (121)
> #NanoCore 75 (84)
> #AsyncRAT 61 (49)
> #LokiBot 57 (67)
> #Qealler 55 (106)
> #Masslogger 44 (38)
> #Remcos 42 (68)https://t.co/98nRpXOxWw
>
> — ANY.RUN (@anyrun_app) July 27, 2020

If you want to find out more information about active Emotet campaigns you should follow the Cryptolaemus group on Twitter, a collective of security researchers who are keeping an eye on this malware's activity.

Update July 29, 17:59 EDT: Added more info on Emotet's attachment stealer module and the number of spam emails sent each day.

Related Articles:

Emotet botnet switches to 64-bit modules, increases activity

Microsoft detects massive surge in Linux XorDDoS malware activity

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

New cryptomining malware builds an army of Windows, Linux bots

Historic Hotel Stay, Complementary Emotet Exposure included