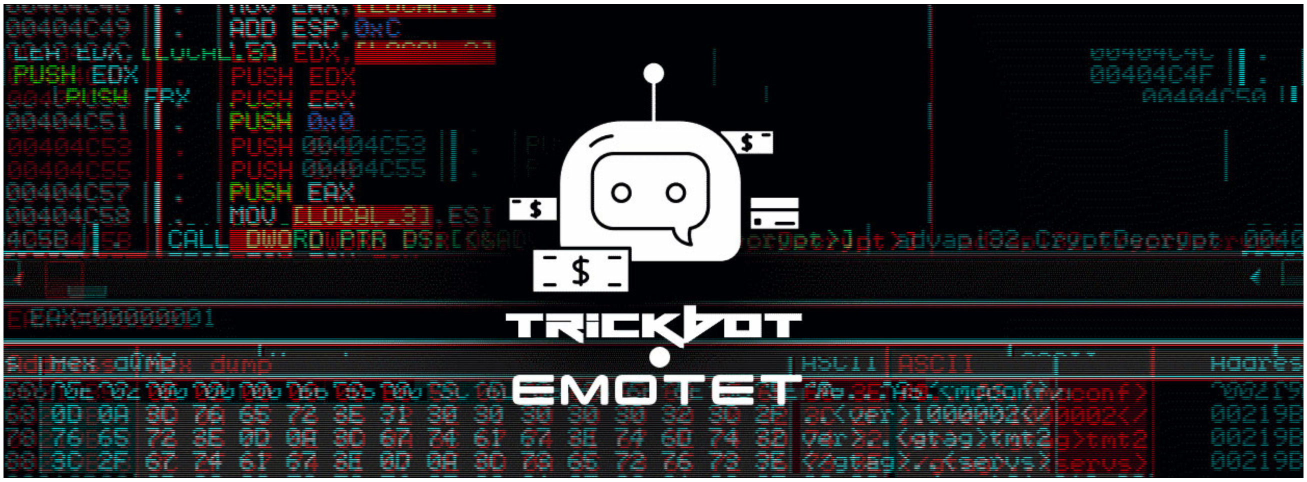
# Emotet-TrickBot malware duo is back infecting Windows machines

bleepingcomputer.com/news/security/emotet-trickbot-malware-duo-is-back-infecting-windows-machines/

Lawrence Abrams

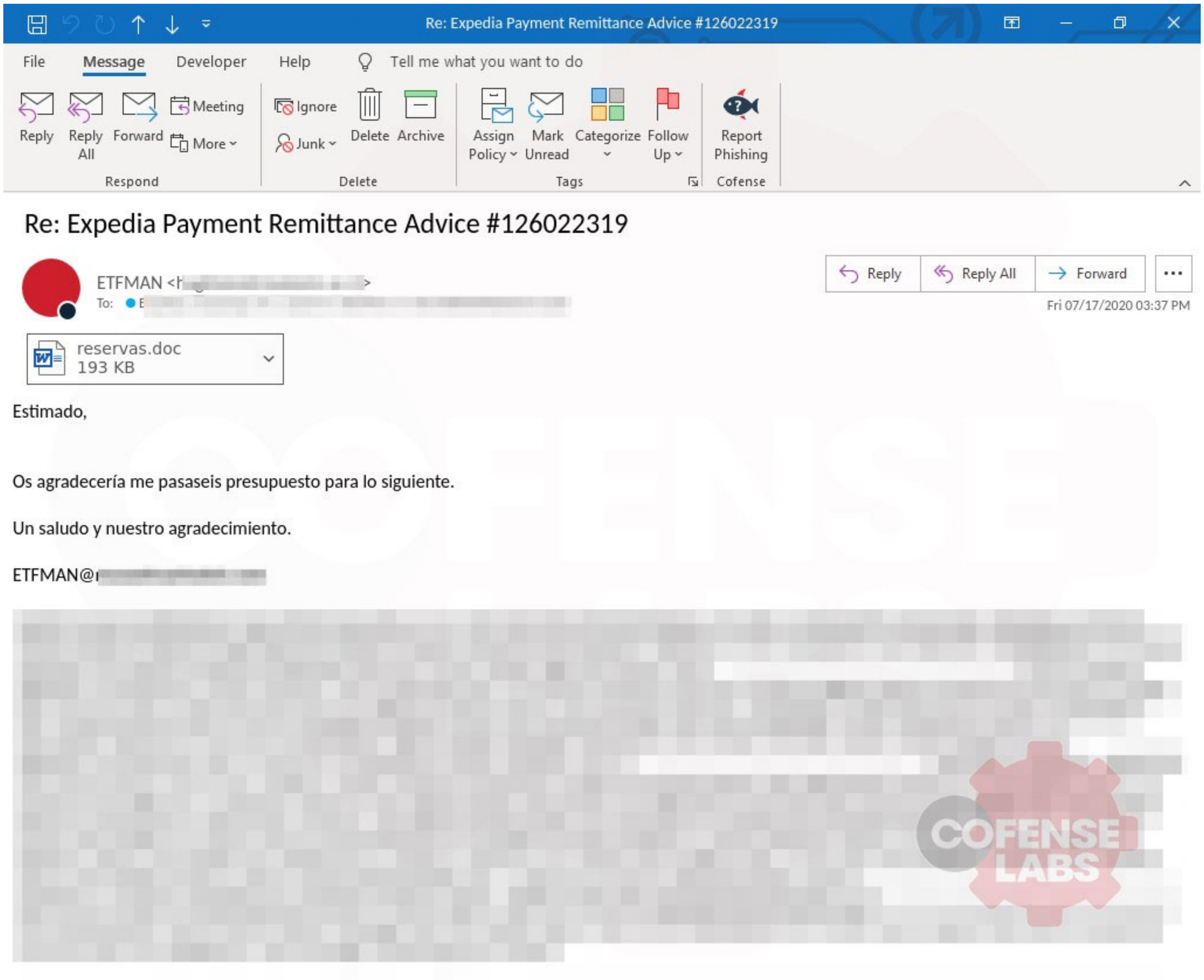
By
Lawrence Abrams

- July 20, 2020
- 03:52 PM
- 1



After awakening last week and starting to send spam worldwide, Emotet is now once again installing the TrickBot trojan on infected Windows computers.

On July 17th, 2020, after over five months of inactivity, the Emotet Trojan woke up and started massive spam campaigns pretending to be payment reports, invoices, shipping information, and employment opportunities.



Re: Expedia Payment Remittance Advice #126022319

ETFMAN <[redacted]>

To: [redacted]

Fri 07/17/2020 03:37 PM

reservas.doc
193 KB

Estimado,

Os agradecería me pasaseis presupuesto para lo siguiente.

Un saludo y nuestro agradecimiento.

ETFMAN@[redacted]

[redacted]

**Current Emotet campaign**

These spam emails contain malicious documents that will install the Emotet trojan on the recipient's computer when opened and macros enabled.

Historically, once a user became infected with Emotet, the trojan would eventually download and install the TrickBot trojan on the infected computer.

It wasn't until today, though, that Binary Defense researcher James Quinn told BleepingComputer that he began to see Emotet once again installing the TrickBot trojan.

## TrickBot and why it is so dangerous

TrickBot is an advanced malware that infects Windows machines and is commonly seen targeting enterprise networks.

What makes TrickBot so dangerous is that it will download modules that perform various malicious activities on an infected computer.

This activity includes:

- Attempting to spread laterally through a network
- Steal Active Directory Services databases
- Harvest login credentials and cookies from browsers
- Steal OpenSSH keys
- Steals RDP, VNC, and Putty credentials
- Steals banking credentials

Even worse, though, once TrickBot has finished harvesting anything of value from a compromised network, it will open up a reverse shell to the Ryuk and Conti Ransomware actors.

This reverse shell will allow the ransomware operators to access the network, steal unencrypted files, and then deploy their ransomware to encrypt all of the network's machines.

Network and security administrators need to be sure users on their network are educated adequately on Emotet spam campaigns and not open any suspicious documents.

Furthermore, if a computer becomes compromised by Emotet, likely, they are also compromised by TrickBot.

A full investigation should be launched, which includes assessing whether the infections have spread to other computers on the network.

## Related Articles:

New Bumblebee malware replaces Conti's BazarLoader in cyberattacks

The Week in Ransomware - May 20th 2022 - Another one bites the dust

Conti ransomware shuts down operation, rebrands into smaller units

The Week in Ransomware - May 13th 2022 - A National Emergency

Costa Rica declares national emergency after Conti ransomware attacks

- Conti
- Emotet
- MalSpam
- Ransomware
- Ryuk
- Spam
- TrickBot
- Windows

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.

- Previous Article
- Next Article

## Comments

R-K - 1 year ago

Death sentences for creating and distributing the very destructive malware.

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

## You may also like: