POLYSWARM

Threat Bulletin

October 18, 2022

THREAT LEVEL

HIGH

TROJAN

Emotet Observed Using New TTPs

Related Families: TrickBot, Ryuk, QakBot, Zloader, Quantum, BlackCat

Verticals Targeted: Financial, Various

EXECUTIVE SUMMARY: VMWare recently reported on the evolution of Emotet. New Emotet TTPs include added functionality, new anti analysis techniques, infrastructure changes, and new attack vectors.

KEY TAKEAWAYS

- Emotet has evolved TTPs since its return in late 2021.
- Emotet was originally a banking trojan but now also acts as a botnet and a loader.
- Other changes to Emotet include new functionalities, new anti analysis techniques, infrastructure changes, and new attack vectors.

IOC's

- 56ce2b869b7126e336389f768cc2ec2e60623babe39112c5b27ab9bf7eab7316 PolyScore™ 0.99
- 76c3ab81873cce2881a195e19f3ac02447922e4b5d210699e7e04ce3af16f7c6 PolyScore™ 0.99
- f3e36df2e1c048755eec429cab53ba4d46bdb5a670f975fe86c6293d60fcbd9b PolyScore™ 0.99
- 235455583bf9b5a226fbb67e6653d3ce8ed3edc4b0dedca065aef163f5b515ec PolyScore™ 0.99

What is Emotet?

The Emotet banking trojan, first seen in the wild in 2014, was once considered the "world's most dangerous malware." Previous versions of Emotet were extremely dangerous because they spread quickly, were difficult to detect, and were sometimes used by other threat actor groups to install ransomware, stealers, and other malware. The threat actors behind Emotet created an elaborate infrastructure, the notorious Emotet malware botnet.

Emotet was considered dead after its takedown by law enforcement groups in January 2021. Although leftover samples existed in the wild, there was no network infrastructure to support them. In November 2021, Emotet activity was again observed in the wild. Emotet now primarily functions as a botnet and a loader as a service (LaaS). Last month, industry researchers reported that ransomware as a service (RaaS) groups including Quantum and BlackCat are leveraging Emotet.

How Has Emotet Evolved?

VMWare reported on multiple changes indicating an evolution of Emotet's TTPs:

Functionality Added
Emotet has new models allowing threat actors to steal credit card information from the Google Chrome browser and to leverage SMB to spread laterally.

Anti Analysis
The threat actors behind Emotet are hiding their C2 infrastructure, making analysis more difficult. More recent Emotet variants use a new method of storing the configuration data within the binary.

Infrastructure Changes
VMWare noted a shift in Emotet's infrastructure, with the current versions using clusters known as Epoch 4 and Epoch 5. VMWare researchers examined 23,811 DLL payloads and discovered 328 unique IP addresses used by Emotet. The majority belonged to Epoch 4, with just under 40% belonging to Epoch 5. One IP address overlapped both botnets. Emotet's C2 infrastructure creates redundancy and makes activity harder to track. The ports most commonly used by Emotet include 8080 and 443.

New Attack Vectors
VMWare noted Emotet has been leveraging both malicious URLs embedded in emails and malicious Microsoft documents as an initial infection vector. Some attacks relied on Excel documents containing macros. The macros function to download the next stage payload, use rundll32.exe to execute the payload, and gain registry persistence. Infections observed earlier this year used mshta.exe as an infection vector. This legitimate utility is used for LoLBins (living off the land binaries) techniques and executes Microsoft HTA files.

IOCs

PolySwarm has multiple samples associated with new Emotet activity.

56ce2b869b7126e336389f768cc2ec2e60623babe39112c5b27ab9bf7eab7316
76c3ab81873cce2881a195e19f3ac02447922e4b5d210699e7e04ce3af16f7c6
f3e36df2e1c048755eec429cab53ba4d46bdb5a670f975fe86c6293d60fcbd9b
235455583bf9b5a226fbb67e6653d3ce8ed3edc4b0dedca065aef163f5b515ec
d8ee1390007dd461b6e3b13b2c4ae5e24ce507eabb4453eb543e942f497c7ee4
f163a0536758adee328bb441d74cfb81bc555ee5e6c6730e9d29f57e780178ac
da0438061f080e77f0e3c7a2eedb2419cc4d620bada5b6b68fd43af34455cdf0
fde7d56b1eefd98d5b5d23bcc25c76791cbd6a30a484f654c153c4ed7256c9b9
df0290e3872f77806b035c0e4961b61b2d4153e3549df25e8ef8be3d48f2ca2f
87d289eb424171727cd4dbac5586079565c5685854af5b67faaf7f8efeccf10b
64c2fc6414222bbfcabcb5ea51a31dc58327e12a8681c12af031783fc64cd5bf
8a48876fad741a71b5568466da7990fc337e1f075e3e9a5d20080970f846ba21
d1fe95a2ac103e57269b415bcf76539b31cbf6ee60ec4bcd10b5e4c6197dba84
45e7771d02b931a858b78810ef0f47f07d0389547318935cb53f3b80c8ec9fb2
22e37455267b91afc07533948f45923ca21a36099d0b9645efecc088b86db398
0bd48477ba499ab7e16c463f306eedf443689e9691040bd2aa0328c78c2e446e
1eeec7719ac8c2ccdcd9205bd50d7744881bd79363ec3e4971617fc88a7e95d4
a131c4d00312d496043485355b198b9fac859bc11ac600ab5d49d0a7e3db96e6

a3fa5030fb2a711d3604dd90eebfe7d21bae0611d437dc5b22d7e40d451cd19e
d88679bb2a6d0688997f722e60ac9fbaca2139f8f355e358d1d7ac9ae67e0f20

You can use the following CLI command to search for all Emotet samples in our portal:
$ polyswarm link list -f Emotet