Emotet emerges as a leader in Malware-as-a-Service

By Barracuda Networks

Published: 2020-06-19 · Archived: 2026-04-05 23:41:21 UTC

One of the reasons that cybercrime has grown so rapidly is that the criminals at the top of the "food chain" have built scalable business models for their crimes. This allows experienced hacking groups to collaborate, and new criminals to leverage the resources of veteran hackers. "Crime-as-a-service" is nothing new, but the tools change rapidly as crimeware developers work to exploit the latest vulnerabilities and stay ahead of security. The Emotet banking trojan has emerged as a leader in providing malware delivery services to other hacking groups, and you will want to make sure you understand and defend against this threat.

The evolution of Emotet

Banking attacks are sometimes collaborative, but banking trojans do not usually provide services to third party attackers. Emotet has been in constant development since it's discovery as a banking trojan in 2014. Developers have added new evasion capabilities, new methods of delivery, and improvements to its core function of stealing data. The long-term success of this malware suggests that it is run by a sophisticated criminal organization, which is consistent with recent findings that organized crime is responsible for the majority of data breaches. Here are some highlights in the life of Emotet:

2014

Emotet surfaced as a modular malware, designed to steal banking credentials and exfiltrate sensitive information from individual endpoints. Notable capabilities included evading multi-factor authentication (MFA) and infecting other systems with its worm-like behavior.

2015

New evasion capabilities were added that allowed Emotet to detect the presence of a virtual machine. MFA evasion was improved and new banking capabilities were added that allowed Emotet to transfer funds from the victim to attacker.

2017

Emotet was observed targeting multiple sectors outside of banking. New capabilities included new anti-analysis techniques and a Windows API component that made detection more difficult.

2018

Emotet developers add abilities to steal email content and contact lists, spread itself to infect protected systems, and deliver other malware.

Emotet connects to a command and control server (C2) so that the infected machines become part of the Emotet botnet. It's worth noting here that 'Emotet' refers to both the malware and the criminal organization that develops the malware and controls these servers. The Emotet group uses the C2 servers to install new malware, remotely control infected machines, and transmit stolen information back to the attacker. The Emotet infrastructure makes it possible for other hacking groups to buy access to Emotet-infected machines. In this way, Emotet acts as Malware-as-a-Service (MaaS) to distribute third-party malware.

Emotet today

Emotet uses brand impersonation and spear-phishing emails to trick victims into thinking an email is from a trusted source. The email either carries a malicious attachment or will include a link to a compromised website. Once the attachment or link is executed, Emotet will begin downloading to the victim's machine. When the attack gets underway Emotet will attempt to distribute itself laterally across the network using both wired and wifi connections to do this.

The US Department of Homeland Security published an alert on this threat which details the attack and warns the public,

> *"Emotet continues to be among the most costly and destructive malware affecting SLTT governments. Its worm-like features result in rapidly spreading network-wide infection, which are difficult to combat. Emotet infections have cost SLTT governments up to $1 million per incident to remediate."*

A successful Emotet attack can expose sensitive information, interrupt your business, damage your brand reputation. Downtime and recovery costs can be devastating. Allentown (PA) spent $1 million to recover from an Emotet attack in 2018. Other notable victims include a large public library and the city of Quincy (MA).

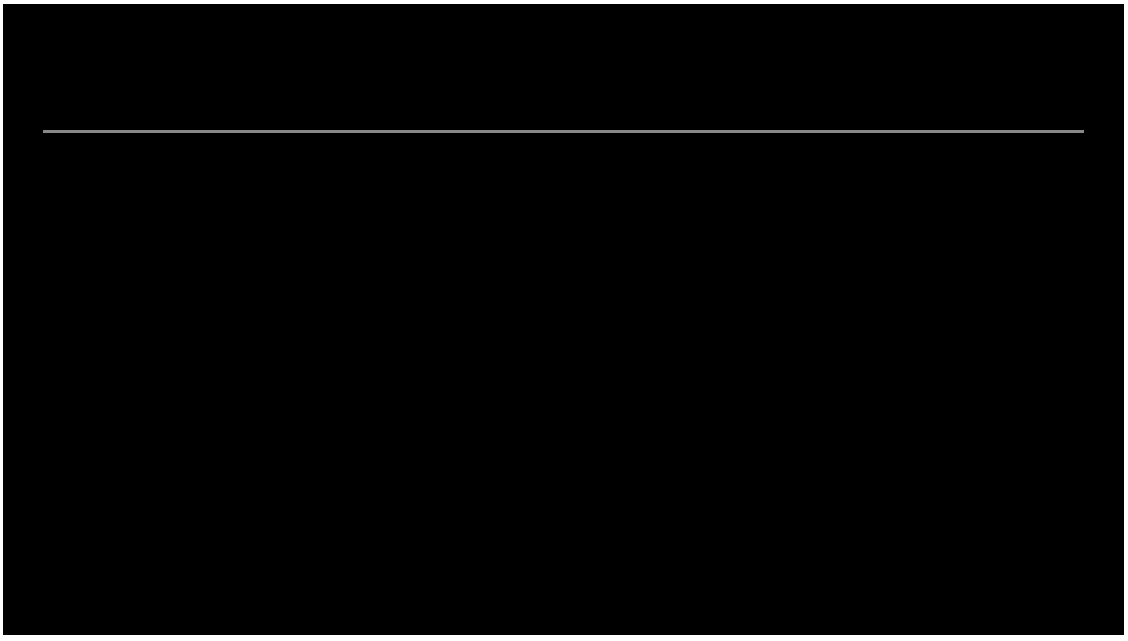
Protect yourself

Because Emotet has multiple attack capabilities, you need multiple layers of security to fully defend your network. Here are some tips to get you started:

- Maintain updated endpoint antimalware software and apply updates and patches immediately.
- Deploy email protection to block suspicious file attachments as well as indicators such as known URLs, subject lines, and IP addresses.
- Use a web security gateway that will protect your network from incoming malware.
- Secure wifi connections and use the concept of least-privilege access to protect network shares as much as possible.
- Provide security awareness training to network users.

For more information on how to defend your network from threats like Emotet, visit www.barracuda.com

Get your copy of the e-book now



Christine Barry

Christine Barry Senior Chief Cybersecurity Storyteller and Content Manager at Barracuda. Prior to joining Barracuda, Christine was a field engineer and project manager for K12 and SMB clients for over 15 years. She holds several technology and project management credentials, a Bachelor of Arts, and a Master of Business Administration. She is a graduate of the University of Michigan.

Connect with Christine on LinkedIn here.

Join our Reddit community!

Source: https://blog.barracuda.com/2020/06/19/emotet-emerges-as-a-leader-in-maas/