

DHS warns that Emotet malware is one of the most prevalent threats today

US detects more than 16,000 alerts since July for nasty trojan that's hard to spot.

DAN GOODIN - 10/6/2020, 8:16 PM



[Getty Images](#)

The malware known as Emotet has emerged as “one of the most prevalent ongoing threats” as it increasingly targets state and local governments and infects them with other malware, the cybersecurity arm of the Department of Homeland Security said on Tuesday.

Emotet was first identified in 2014 as a relatively simple trojan for stealing banking account credentials. Within a year or two, it had reinvented itself as a formidable downloader or dropper that, after infecting a PC, installed other malware. The Trickbot banking trojan and the Ryuk ransomware are two of the more common follow-ons. Over the past month, Emotet has successfully burrowed into [Quebec’s Department of Justice](#) and increased its onslaught on governments in [France](#), [Japan](#), and [New Zealand](#). It has also targeted the [Democratic National Committee](#).

Not to be left out, US state and local governments are also receiving unwanted attention, according to the CISA, short for the Cybersecurity and Infrastructure Security Agency. Einstein—the agency’s intrusion-detection system for collecting, analyzing, and sharing security information across the federal civilian departments and agencies—has in recent weeks noticed a big uptick, too. In an advisory issued on Tuesday, officials wrote:

Since July 2020, CISA has seen increased activity involving Emotet-associated indicators. During that time, CISA’s EINSTEIN Intrusion Detection System, which protects federal, civilian executive branch networks, has detected roughly 16,000 alerts related to Emotet activity. CISA observed Emotet being executed in phases during possible targeted campaigns. Emotet used compromised Word documents (.doc) attached to phishing emails as initial insertion vectors. Possible command and control network traffic involved HTTP POST requests to Uniform Resource Identifiers consisting of nonsensical random length alphabetical directories to known Emotet-related domains or IPs with the following user agent string (Application Layer Protocol: Web Protocols [T1071.001]).

FURTHER READING

[One of the most destructive botnets can now spread to nearby Wi-Fi networks](#)

Emotet's success is the result of a host of tricks, a few of which include:

- The ability to [spread to nearby Wi-Fi networks](#)
- A polymorphic design, meaning it constantly changes its identifiable characteristics, making it hard to detect as malicious
- Fileless infections, such as Powershell scripts that also make post-infections difficult to detect
- Worm-like features that steal administrative passwords and use them to spread throughout a network
- "Email thread hijacking," meaning it steals email chains from one infected machine and uses a spoofed identity to respond to trick other people in the thread to open a malicious file or click on a malicious link.

Below is a diagram showing some of the techniques employed by Emotet.



In February, Emotet suddenly went dark, with no clear reason for doing so. Then in July it [just as quickly returned](#).

CISA

Emotet attackers have been blasting out malicious spam ever since. According to a [separate blog post published on Tuesday](#), security firm Intezer said it, too, is seeing a big increase, with 40 percent of the samples analyzed by its enterprise customers and community users being classified as Emotet.

"In a world where everything is seemingly unpredictable, it does seem we can count on Emotet to keep us on our toes," Intezer researchers wrote. "That shouldn't stop us from being more strategic in how we adapt our approach to make it easier to identify this threat."