Emotet 101: How the Ransomware Works -- and Why It's So Darn Effective

By Samuel Greengard

Published: 2020-10-09 · Archived: 2026-04-06 03:19:57 UTC

5 Min Read

(Image: Alexander Limbach via Adobe Stock)

Ransomware has emerged as a primary threat to organizations of all shapes and sizes. According to "The State of Ransomware 2020" report by cybersecurity firm Sophos, 51% of organizations have been hit by ransomware attacks within the past year, and the average cost to remediate an attack has reached $761,106 globally.

While numerous types of ransomware exist, one of the more prominent and dangerous versions is Emotet. Emotet is a "key component" in ransomware campaigns, noted security firm Mimecast in its 2020 "Threat Intelligence Report." And, per Proofpoint, the most common countries targeted include Germany, Austria, Switzerland, the United States, the United Kingdom, and Canada.

What Is Emotet?

Emotet is a Trojan available through a malware-as-a-service (MaaS) model. This means cybercriminals can download a package, often for a few hundred dollars or a monthly subscription fee, and direct attacks to businesses and individuals.

The initial payload — which is typically delivered via e-mail, infected documents, or websites — unleashes a script, macro, or code that operates as a worm that infects various software applications and systems, such as an

Outlook address book or a cloud-based container.

"In many cases, Emotet often sits idle for 30 to 45 days before it launches a ransomware attack," notes Keith Mularski, managing director in the cybersecurity practice at consulting firm EY.

Emotet is highly effective because it continually downloads malware components as it wends its way through systems, Mularski says. Many conventional security tools, such as firewalls, aren't effective against it because Emotet creates encrypted channels that network defenses can't detect.

Then, once Emotet has captured and encrypted files, cyberthieves demand a ransom, often paid through untraceable cybercurrency, such as Bitcoin. Remarkably, "Cybercriminals operate Emotet very much like a business, including offering customer support," says John Shier, senior security adviser at Sophos.

What Does an Attack Look Like?

Typically, an infection occurs when someone clicks on a link in an e-mail, often through a phishing attack. This directs the user to a site or service that downloads the initial "dropper." Once this macro or code resides on a computer, it begins to seek out other connected computers and spread, further distributing the malware. Frequently, it uses Microsoft Outlook to generate e-mails.

As Emotet infects systems, it conducts brute-force attacks on accounts, seeking to crack passwords and gain access to secure data, Shier notes. At some point, it captures and encrypts these files. Once cybercriminals hold the encrypted data — and the business is locked out — they demand a ransom. The price tag can range from a few thousand dollars to millions of dollars. According to the Sophos report, 94% of organizations ultimately regain control of their data but at an average cost of $732,520 per incident.

Why Is Emotet so Effective?

Emotet exists in several different versions and incorporates a modular design. This makes it more difficult to identify and block. It uses social engineering techniques to gain entry into systems, and it is good at avoiding detection. What's more, Emotet campaigns are constantly evolving. Some versions steal banking credentials and highly sensitive enterprise data, which cybercrooks may threaten to release publicly.

"This may serve as additional leverage to pay the ransom," Shier explains.

An initial e-mail may look like it originated from a trusted source, such as a manager or top company executive, or it may offer a link to what appears to be a legitimate site or service. It usually relies on file compression techniques, such as ZIP, that spread the infection through various file formats, including .doc, docx, and .exe. This hides the actual file name as it moves around within a network.

These documents may contain phrases such as "payment details" or "please update your human resources file" to trick recipients into activating payloads. Some messages have recently revolved around COVID-19. They often arrive from a legitimate e-mail address within the company — and they can include both benign and infected files. What's more, Emotet can detect the environment it is running in. For example, it knows when it resides inside a virtual machine (VM) and stays dormant to avoid detection from malware scanners.

Emotet uses command-and-control (C2) servers to receive updates surreptitiously. This allows attackers to update the malware code and plant other Trojans. It's also possible to clean a computer but then have the malware

reappear.

How Can You Combat Emotet?

There are a number of ways to reduce the risk of an infection — and the resulting problems Emotet causes, Shier says. First, it's wise to deploy security software that identifies and blocks potentially dangerous e-mails. It's also critical to secure all managed and unmanaged devices connecting to the network. Other protections include strong passwords and multifactor authentication, consistent patching, and the use of threat intelligence software. Finally, employees must learn how to spot suspicious e-mails.

Unfortunately, ransomware — and Emotet — aren't going to disappear anytime soon. In recent weeks, it has emerged as the most common form of ransomware. Says Mularski: "The attacks are becoming more sophisticated. They represent a very real risk to all businesses."

About the Author

Freelance Writer

Samuel Greengard writes about business, technology, and cybersecurity for numerous magazines and websites. He is author of the books "The Internet of Things" and "Virtual Reality" (MIT Press).
