EMOTET Returns, Starts Spreading via Spam Botnet

By By: Don Ovid Ladores Sep 07, 2017 Read time: 4 min (1001 words)

Published: 2017-09-07 · Archived: 2026-04-05 15:25:00 UTC

We first detected the banking malware EMOTET back in 2014, we looked into the banking malware's routines and behaviors and took note of its information stealing abilities via network sniffing. In August, we found increased activity coming from new variants (Detected by Trend Micro as TSPY_EMOTET.AUSJLA, TSPY_EMOTET.SMD3, TSPY_EMOTET.AUSJKW, TSPY_EMOTET.AUSJKV) that have the potential to unleash different types of payloads in the affected system.

A Resurgent Malware

While the motivation behind EMOTET—information theft—remain the same, the reason as to *why* the malware resurfaced could be mainly attributed to two main possible reasons.

First, the authors behind this attack may be targeting new regions and industries.

While the earlier variants of EMOTET primarily targeted the banking sector, our Smart Protection Network (SPN) data reveals that this time, the malware isn't being picky about the industries it chooses to attack. The affected companies come from different industries, including manufacturing, food and beverage, and healthcare. Again, it is possible that due to the nature of its distribution, EMOTET now has a wider scope.

The United States, United Kingdom, and Canada made up the bulk of the target regions, with the US taking up 58% of all our detected infections, while Great Britain and Canada were at 12% and 8% respectively.

Figure 1: Regional Distribution of the EMOTET attacks from June 6 to September 6, 2017

Second, these new variants use multiple ways to spread. Its primary propagation method involves the use of a spam botnet, which results in its rapid distribution via email. EMOTET can also spread via a network propagation module that brute forces its way into an account domain using a dictionary attack. EMOTET's use of compromised URLs as C&C servers likely helped it spread as well.

The element of surprise could also have played a role in its effectiveness: due to its recent inactivity, EMOTET's resurgence managed to catch its targets off-guard, making the attacks, new capabilities, and distribution more effective.

For a malware with email-spamming and lateral-movement capabilities, infecting business systems and acquiring corporate e-mails translates to larger and more effective spam targeting and a higher chance of gaining information.

Figure 2: EMOTET Infection Diagram for the recent wave of attacks

Arrival and Installation

The new EMOTET variants initially arrive as spam claiming to be an invoice or payment notification to trick its victims into believing that this is a legitimate email from a supplier.

Figure 3: Sample spam email

In the body of this email is a malicious URL that will download a document containing a malicious macro when a user clicks on it. This macro will then execute a PowerShell command line that is responsible for downloading EMOTET.

Here are some of the sample URLs we discovered:

-
-
-
-

Once downloaded, EMOTET drops and executes copies of itself into the following folders:

-
-

The malware will attempt to ease its entry into the system by deleting the Zone Identifier Alternate Data Stream (ADS), which is a string of information that describes the Internet Explorer Trust Settings of the file's download source. This is one way for the system to find out if a downloaded file is from a high-risk source, blocking the download if it is detected as such.

EMOTET will then register itself as a system service and adds registry entries to ensure that it is automatically executed at every system startup. The typical windows service acts as a “controller” for most hardware-based applications, while others are used to control other applications. The EMOTET malware, on the other hand, uses it for both Elevation of Privilege, and as an autostart mechanism.

Routines

EMOTET will list the system’s currently running processes and then proceed to gather information on both the system itself and the operating system used.

It will then connect to the Command & Control (C&C) servers to update to its latest version, as well as to determine the type of payload that it will deliver. One of the possible payloads is the persistent banking trojan known as DRIDEX, which attempts to harvest banking account information via browser monitoring routines. Furthermore, the malware can also turn the infected system into part of a botnet that sends spam emails intended to spread the malware even further. This allows the trojan to spread quickly, as the more systems it can potentially

infect, the faster it will propagate. The malware is also capable of harvesting email information and stealing username and password information found in installed browsers.

We discovered that in addition to the above payloads, the C&C server is responsible for sending modules that will perform the following routines, which includes:

-
-
-
-

From our recent samples of EMOTET malware, we have observed that it has become a Loader Trojan that decrypts and loads any binary coming from its Command & Control (C&C) server.

Trend Micro Solutions

Addressing threats such as EMOTET need a multilayered and proactive approach to security—from the gatewayproducts, endpointsproducts, networksproducts, and serversproducts. Trend Micro endpoint solutions such as Trend Micro™ Smart Protection Suitesproducts and Worry-Free™ Business Securityworry free services suites can protect users and businesses from these threats by detecting malicious files, and spammed messages as well as blocking all related malicious URLs. Trend Micro Deep Discovery™products has an email inspection layer that can protect enterprises by detecting malicious attachment and URLs.

Trend Micro™ Hosted Email Securityproducts is a no-maintenance cloud solution that delivers continuously updated protection to stop spam, malware, spear phishing, ransomware, and advanced targeted attacks before they reach the network. It protects Microsoft Exchange, Microsoft Office 365products, Google Apps, and other hosted and on-premises email solutions.

Trend Micro™ OfficeScan™products with XGen™ endpoint security infuses high-fidelity machine learning with other detection technologies and global threat intelligence for comprehensive protection against advanced malware.

The list of SHA256 is in this appendixopen on a new tab.
