Emotet Adds New Evasion Technique

blog.trendmicro.com/trendlabs-security-intelligence/emotet-adds-new-evasion-technique-and-uses-connected-devices-as-proxy-cc-servers/

April 25, 2019

UPDATE as of May 2, 2019 5AM PDT: A previous version of this blog post speculated that connected devices were used as part of Emotet's command-and-control networks. This was based on speculation derived from Shodan results; that particular section has been removed from the post. We apologize for any confusion our earlier speculation may have caused.

Over the years, Emotet, the banking malware discovered by Trend Micro in 2014, has continued to be a prevalent and costly threat. The United States government estimates that an Emotet incident takes an organization US $1 million to remediate. Unfortunately, it is a widespread and particularly resilient malware. Its authors have continuously updated it with new capabilities, new distribution techniques, and more.

Recently, an analysis of Emotet traffic has revealed that new samples use a different POST-infection traffic than previous versions. It seems Emotet actors are looking for new ways to evade detection.

Arrival via spam

Emotet typically arrives on a victim's system via spam mail. In the beginning of April, samples of Emotet show that the malware still spreads via spam, but with the help of the trojan downloader Powload. The spam messages trick users into downloading malicious files by claiming that an invoice is attached in the email. The attachment is a ZIP file that can be opened with the 4-digit password included in the body of the email. A look into the ZIP file shows that it contains variants of Powload (detected as Trojan.W97M.POWLOAD). If the user enters the password, the file uses Powershell to download an executable file, which is Emotet's payload.

Figure 1. Example of an Emotet spam mail; samples show mail written in many different languages

Changes in POST-infection traffic

The wave of Emotet samples using new POST-infection traffic has been monitored since March 15, 2019. Researchers from Malware-Traffic-Analysis.net and Cofense also noted changes in Emotet's network traffic around this time. As mentioned previously, Emotet has undergone many changes since it was first discovered; but this is the first time we have seen this particular POST-infection traffic technique.

Figure 2. New Emotet post-infection HTTP Post request traffic

Previous connections from Emotet did not use a URI path, but the newer samples show randomized words used as a URI directory path (see Figure 2) and a random number of directory paths. These random words in the URI path help the malware evade network-based detection. An empty URI path is a red flag, so this technique helps the traffic appear more legitimate to security solutions.

Below is a list of random words used in the URI path, found in the new sample. We can also see these same words in the Emotet executable file.

Figure 3. Decrypted dump with list of words to be used in the URI

Apart from the URI path, the data in the HTTP POST message body has also changed. Previous Emotet samples typically used an HTTP GET request to send victim information to the C&C server, and the data is stored in the Cookie header. The data was encrypted using an RSA key, AES, and then encoded in Base64 before being added to the Cookie value (see Figure 4 *HTTP request traffic with Cookie header*).

Newer traffic shows something different. Actors stayed away from using the Cookie header and changed the HTTP request method to POST. The data is still encrypted with an RSA key and AES, and encoded in Base 64. However, instead of being stored in the Cookie value, it was put in the body of the HTTP POST message. This change adds another layer of complexity to help the malware evade detection or delay further investigation if it is detected.

Figure 4. Comparison between the new Emotet C&C traffic and the previous Emotet C&C traffic

How can organizations defend themselves?

The change in POST-infection traffic shows that Emotet is still a constantly evolving and resilient threat. The malware authors are fine-tuning evasion techniques and trying to adapt to security solutions. If left unchecked and undetected, this threat may lead to a substantial loss of money and data for businesses.

Combating threats like Emotet calls for a multilayered and proactive approach to security, protecting all fronts — endpoints, networks, and servers. Trend Micro endpoint solutions such as Trend Micro™ Smart Protection Suites and Worry-Free™ Business Security can protect users and businesses from these threats by detecting malicious files and spammed messages, as well as blocking all related malicious URLs. Enterprises can also monitor all ports and network protocols for advanced threats and be protected from targeted attacks with the Trend Micro™ Deep Discovery™ Inspector network appliance.

Deep Discovery Inspector protects customers from these threats via this DDI Rule:

DDI Rule 2897: EMOTET - HTTP (Request) - Variant 4

Trend Micro XGen™ security provides a cross-generational blend of threat defense techniques against a full range of threats for data centers, cloud environments, networks, and endpoints. Smart, optimized, and connected, XGen™ powers Trend Micro's suite of security solutions: Hybrid Cloud Security, User Protection, and Network Defense.

Malware

Over the years, Emotet, the banking malware discovered by Trend Micro in 2014, has continued to be a prevalent and costly threat. Recently, an analysis of Emotet traffic has revealed that new samples use a different POST-infection traffic.

By: Marco Dela Vega, Jeanne Jocson, Mark Manahan April 25, 2019 Read time: (words)

Content added to Folio