From Fileless Techniques to Using Steganography: Examining Powload’s Evolution

Terms:
Security Intelligence

Trend Micro

By: Augusto Remillano and Kiyoshi Obuchi (Threats Analysts)

Powload’s staying power in the threat landscape shows how far it has come. In fact, the uptick of macro malware in the first half of 2018 was due to Powload, which was distributed via spam emails. Powload was also one of the most pervasive threats in the North American region in 2018, using various techniques to deliver payloads such as the information-stealing Emotet, Bebloh, and Ursnif. Our Powload detections and the number of related cases/incidents and unique samples we analyzed in 2018 also markedly increased compared to 2017. Powload’s evolving techniques, on the other hand, show how far it will go. While its use of spam email as a distribution method could be its constant, it has employed different ways of delivering payloads, from bypassing mitigations like a document’s preview mode to using fileless techniques and hijacking email accounts.

In some of the recent Powload-related incidents we saw, we noticed significant changes to some of the attachments in the spam emails: the use of steganography and targeting of specific countries. Figure 2 shows the difference. For example, the samples we analyzed in early 2018 had more straightforward infection chains. These updates added another stage to the execution of malicious routines as a way to evade detection.

The Powload variants that use these techniques drop and execute the Ursnif and Bebloh data stealers. We did not see any notable differences in the payloads’ routines. The distribution tactics also resemble a spam campaign we uncovered last year, which delivered the same information stealers but distributed via the Cutwail botnet.

![Figure 1. Detections for Powload based on data from Trend Micro and Smart Protection Network](image1)

![Figure 2. In some of the recent Powload-related incidents we saw, we noticed significant changes to some of the attachments in the spam emails: the use of steganography and targeting of specific countries.](image2)
How Powload uses steganography

The use of steganography — hiding code within an image — isn’t new. Hacking groups, for instance, are known to use steganography for retrieving their backdoors. Exploit kits, for example, use it to hide their command-and-control (C&C) communication.

In Powload’s case, it uses steganography to retrieve an image containing malicious code. Based on the code-extraction routines of the Powload variants we analyzed, they abuse a publicly available script (Invoke-PSImage) to create the images containing their malicious codes.

The attachments in the spam emails have malicious macro code embedded inside the document that executes a PowerShell script, which downloads an image hosted online. It then processes the downloaded image to acquire the code hidden inside the image.
Figure 4. Screenshot of an image containing the malicious code

Another trend we observed in Powload-embedded spam emails is the specificity in their targets. By singling out a country — using region-specific brands and vocabulary — to send their spam to, the email content and its attachment can be more convincing to unwitting recipients.

Another drawback is that automated and traditional sandbox solutions whose regional settings aren't set to the spam email's targeted country won't be able to properly analyze the malware.

The methods for region detection vary from the samples we analyzed. Some use the PowerShell command "Get-Culture" to obtain the computer's regional settings. Others get the value of the xlCountrySetting property (which returns information about the current regional settings) in Excel to determine the affected machine's location. Some samples, on the other hand, determine the location by accessing a URL (hxxp://ipinfo.io/country), a free tool that returns an IP address' country.

Addressing Powload's persistence

Powload's persistence as one of 2018's most prevalent threats highlights the effectiveness of its latest techniques — despite being relatively old. We expect Powload's developers to continue to add more malicious routines to their malware, and given how it serves as a catalyst for other threats, we also expect Powload to deliver payloads other than information stealers. Users must always practice cybersecurity hygiene [40] and be more prudent against dubious, unsolicited emails, while businesses should enforce proactive countermeasures [41] to secure their online perimeters.

The following Trend Micro solutions protect users and businesses by blocking the malicious documents and scripts and preventing access to attacker-specified domains: Trend Micro Smart Protection Suites [42], and Worry-Free Business Security [43].

Indicators of Compromise (IoCs):
