Japanese Trends in the Aggressive Activity of the "Locky" Ransomware

By Kenichi Terashita

Published: 2016-04-05 · Archived: 2026-04-05 19:32:49 UTC

The Locky ransomware has shown no signs of slowing down its aggressive activity since it was first observed in mid-February up to the present, and it has already emerged as this year's major threat. The following report on Locky trends within Japan is based on information reported to FortiGuard by FortiGate installations around the world.

Overview

A detailed analysis of the ransomware itself has already been provided to our readers by our FortiGuard researchers. For more details, please see this blog entry. The post starts with a description of general ransomware behavior and then summarizes the domain generation algorithm (DGA), command and control, and encryption aspects from a technical perspective.

Command and Control Communications of the Locky Botnet

According to FortiGuard, Locky-related Botnet communications currently have the tenth highest number of detections within Japan. This is second only to the famous Zeus malware, which is frequently documented even today, and the CryptoWall malware, which has been investigated and reported on in detail by the Cyber Threat Alliance:

Figure 1: Top 10 Botnet observations in Japan during March 2016

There is another significant reason why this malware cannot be ignored despite its tenth place ranking. As mentioned in the beginning of this article, Locky is a new type of ransomware which was only documented starting in February of this year. However, it is already showing a level of activity which rivals Zeus and CryptoWall.

Downloaders Used by Locky

Let's take a look at what kind of malware is currently trending in Japan based on the anti-virus statistical data.

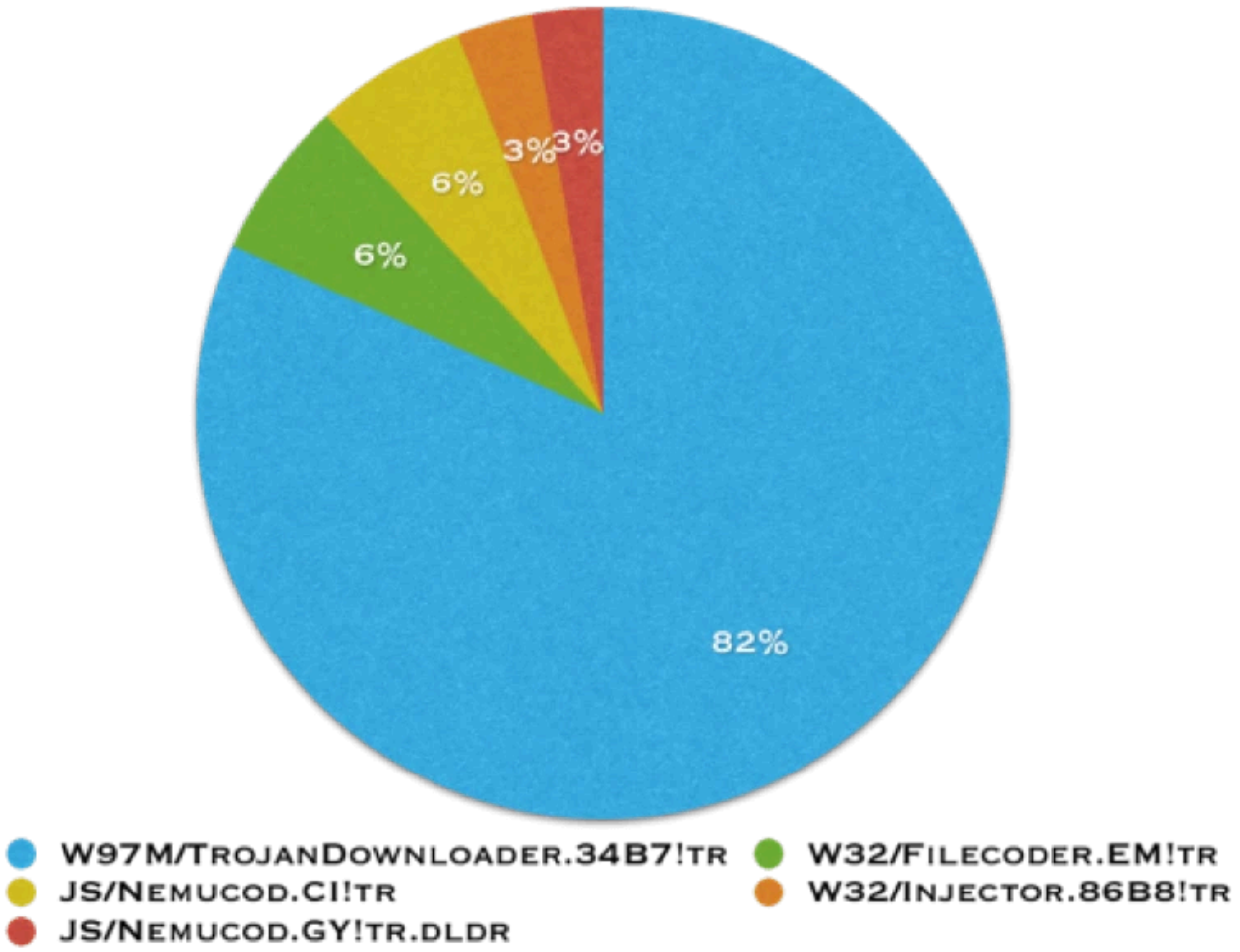

Figure 2: Top 5 Malware detections in Japan between January and March 2016

As this graph clearly demonstrates, the W97M/TrojanDownloader.34B7!tr downloader, which uses a Microsoft Word macro to download and execute an unauthorized program on the infected computer, accounted for over eighty percent of all downloaders.

It is known that this malware is used to download the ransomware as part of the Locky infection scheme. In addition, the rapid expansion in infection activity, which was not apparent in the number of Botnet observations, was revealed by this data due to the fact that anti-virus detections began to be confirmed in parallel with the Locky Botnet activity.

Spread by mail attachment, this malware has already been detected in over one million cases. It is extremely interesting to note that although the number of detections in the U.S. is less than ten thousand cases, the activity of this malware is targeting Japan in particular. In fact, Locky C&C servers are capable of serving the ransomware note in Japanese if the victim is identified to be from Japan:

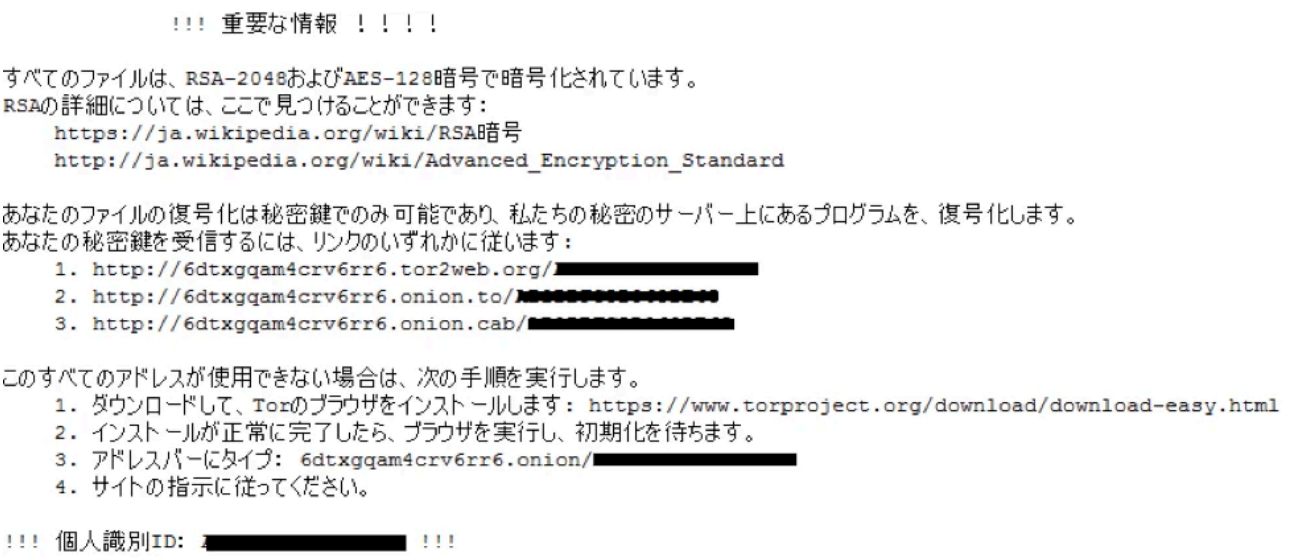

Figure 3: Locky Ransomware Note in Japanese

Furthermore, JS/Nemucod.GY!tr.dldr, a JavaScript downloader with the fifth highest number of detections, is also used by Locky.

Because the downloader itself accounts for most of the detections, we know that the subsequent intrusions by the unauthorized ransomware downloads are being stopped at the border.

Although ransomware related reports seem to be released almost every week by net media sources, it is clear from this research that it is already exerting a greater influence within Japan than previously thought.

It goes without saying that protective measures using security products are needed, but it is imperative that an adequate backup be created on the off chance that your computer is infected with ransomware and your (or your organization's) data is held hostage for a ransom. It is also important that the backup data be stored so that it is not connected to a network. Any backup data that is stored online means that it can be reached by ransomware.

Fortinet Support

As described above, this blog summarizes Fortinet support issues. Customers who use FortiGuard anti-virus are automatically protected from this Locky and malware families that install Locky. Meanwhile, Fortinet customers are advised to use *Locky.Botnet* application control signature to enable protection from this threat.

Related articles

- A Closer Look at the Locky Ransomware
- Statistical Look at CryptoWall, TeslaCrypt, and Locky

Inquiries about the contents of this article

FortiGuard Labs in Japan
fortiguard_jp@fortinet.com

Kenichi Terashita and the FortiGuard Lion Team
