Three Lethal Viruses in Action in 2016:

Locky, Tinba, and Mirai

Jaden Ahn

7672488

Technology Infrastructure: Networking

INFO1380-16S-Sec1

Rich Hildred

July 28, 2017

When people talk about ‘viruses’, it sometimes means computer viruses. ‘Virus’ is a general term used to describe a type of code or software which was designed to do bad things to your computer. The reason it is called ‘virus’ is because it acts like the biological virus; it passes from computer to computer, infecting huge numbers of computers in the end. Then, what are some lethal viruses and what can we do about it? This paper will describe three lethal viruses in action in 2016 with their impact on society, along with effective approaches to mitigate them.

**Locky**

Locky is a type of Ransomware discovered in February, 2016. They are called ransomware because they ask for ransom after taking control of important data in victim’s computer. The attackers usually block access to the victim’s data, or threaten to publish it. The data is usually encrypted, and the attackers may give the victim a key or a tool to decrypt it only after ransom is paid. According to Ducklin (2016), the ransom price varies from BTC (Bitcoin) 0.5 to BTC 1.00 (para. 1), where one bitcoin is worth about CDN $3423.41 as of July 23, 2017. In case of Locky virus, it renames all the extension of Office files, videos, images, and source code in a computer to “.locky”, and also scrambles them so that a victim cannot encrypt it.

Since its discovery, there have been many victims suffered from this malicious ransomware including the Hollywood Presbyterian Medical Center, which had to pay a BCN 40.00, equivalent to CDN $135,000, to get their patient data back on February 18, 2016 (Winton, 2016, para. 1). Ducklin explains that the most common way that your PC can get infected with Locky is through an email (2016, para. 2). This email has an attached document, which looks like just gibberish when you open it. Also, it asks you to enable macro to encode this document correctly. However, enabling macro just runs a code that download a Trojan virus which will take control over your local files. It also changes the wallpaper to a notice like Figure 1, telling you what to do to pay ransom and get the decrypt program with private key to activate it.

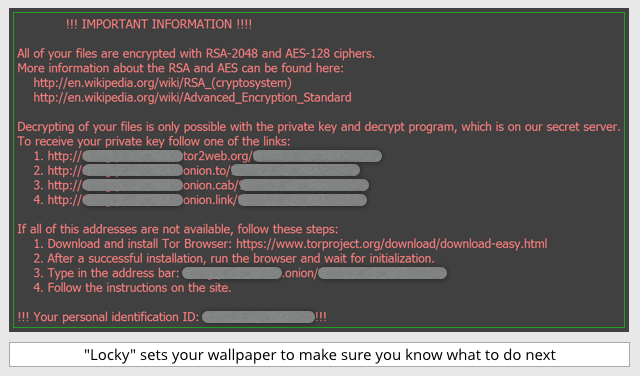


Figure 1. Wallpaper notice of Locky. Adapted from Ducklin. (2016, para. 3).

To prevent this from happening, Ducklin (2016) advises you do the followings (para. 5):

1. Backup your data regularly. There can be other reasons you can lose your data, too, such as fire, flood, theft and etc. Also, encrypting your backup data can prevent it from being abused.
2. Do not enable macros in document sent via email. This is why auto-execution of macros is turned-off by Microsoft many years ago. Also, do not open an email attachment from unknown or suspicious source.
3. Don’t allow more login power than you need. Also, do not stay logged in than necessary. If you are logged in as a domain administrator, the damage can be more serious.
4. Consider using Office viewers because they do not support macros.
5. Patch regularly. Malware sometimes exploits vulnerability in your software, including Office, browser, and Flash.

**Tinba**

Tinba, which is a shortened form of "Tiny Banker", is a type of Trojan virus which mainly aimed at the financial services. Many variants were made from its original version which was discovered in 2012, after its source code was leaked. Tinba held its second position on the list of Top 10 Most Wanted Malware for May 2016, according to a Threat Index released by Check Point (Check Point Threat Intelligence, 2016, para. 2). Also, another Tinba infection campaign was discovered by IBM Security Trusteer researchers, targeting Poland and several more countries (Bach, 2015, para 1). Tinba has infected many major banking institutions in the U.S., too, since its discovery. What makes it so deadly?

When a user tries to connect to a bank’s website, Tinba redirects the user to a fake site which looks and functions exactly the same with the original one. If the user enters information to log on, this virus returns a false message about incorrect information, then sends the user back to the real website so that the user would never notice that his or her credentials were already sent to its host. Schick (2015) mentions that Tinba even detects mouse movement, or screen activity to avoid sandbox, which is used to isolate programs to protect them from hackers (para. 1).

There can be many ways you could get infected by this malicious virus. Maria (2015) mentioned in her article that, “The most common way of catching a Trojan is when your system or any installed program has certain vulnerabilities” (para. 3). Also, you can get Tinba from visiting suspicious websites, or downloading unknown files using torrents. Therefore, it is important to be careful when using Internet. If you noticed that your PC is infected with Tinba, you need to do the following steps to remove Tinba (Maria, 2015, para. 5):

1. Reboot your PC in safe mode.
2. Open Control Panel and delete suspicious programs.
3. Open System Configuration and uncheck entries which have “Unknown” as Manufacturer or otherwise look suspicious.
4. Check your host file to see if there are any IPs listed below Localhost.
5. Open process tab and check each process to determine which ones are vires. Then run Regedit to delete relevant entries.

As it is described here, dealing with Tinba manually takes lots of time and effort. Therefore, it is recommended to use professional vaccine programs for victims who are not an virus expert.

**Mirai**

Mirai is a virus that turns network devices into bots which can be used for distributed denial of service, also known as DDoS, attack. Mirai means ‘the future’ (未来, みらい) in Japanese. Mirai primarily infects the Internet of Things(IoT), such as IP cameras, or home routers. Symantec Security Response reports that Mirai virus was first publicly known after a huge DDoS attack against a website on September 20, 2016 (2016, para. 1).

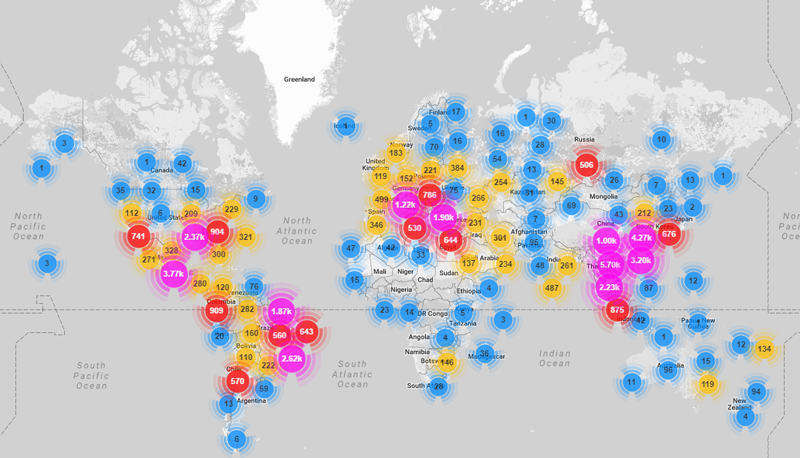
According to an investigation on an attack on August 17, 2016, 49,657 unique IPs were uncovered which hosted devices infected by Mirai. These IP addresses were spotted in 164 countries, as shown in Figure 2 (Bekerman et al., 2016, para. 2).

Figure 2. Geo-locations of all Mirai-infected devices uncovered so far. Adapted from Bekerman et al. (2016, para. 2).

Mirai exploits the fact that users of the IoT devices hardly change factory default username and passwords. It scans for accessible IoT devices over the Internet and try to connect them using this default information. Once it succeeds in gaining access, these devices, infected with Mirai malware, are forced to report to a control server, and are ready to be a faithful bot that will possibly be used in DDoS attacks.

What you can do to keep Mirai, or any other kind of malware from your devices is quite simple (Bekerman et al., 2016, para. 3):

1. Do not use default or generic ID and passwords for your network devices.
2. Disable all remote access to your devices.
3. Regularly check for firmware updates for your devices.

**Conclusion**

To sum up, there are many types of malicious and cunning viruses. They can take control of your important data asking for ransom, steal your bank credentials without being noticed, or even turn your network devices into bots to be used in a DDoS attack. Precautions are somewhat simple and common. Do not open files from unknown sources, do not use suspicious internet websites, and update your devices regularly. These simple strategy will keep your devices safe.

**References**

Bach, O. (2015, June 9). Tinba: World’s Smallest Malware Has Big Bag of Nasty Tricks. *Security Intelligence*. Retrieved July 22, 2017 from https://securityintelligence.com/tinba-worlds-smallest-malware-has-big-bag-of-nasty-tricks/

Bekerman, D., Herzberg, B., Zeifman, I. (2016, October 26). *Breaking Down Mirai: An IoT DDoS Botnet Analysis*. Retrieved July 23, 2017 from https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html

Check Point Threat Intelligence. (2016, June 21). *Top 10 Most Wanted Malware.* Retrieved July 23, 2017 from https://blog.checkpoint.com/2016/06/21/top-10-most-wanted-malware/

Ducklin, P. (2016, February 17). “Locky” ransomware – what you need to know. *Naked Security.* Retrieved July 22, 2017 from https://nakedsecurity.sophos.com/2016/02/17/locky-ransomware-what-you-need-to-know/

Krebs, B. (2016, September 22). KrebsOnSecurity Hit with Record DDoS. *Krebs on Security.* Retrieved July 23, 2017 from https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/

Maria, K. (2015). Tinba Virus/Malware Removal. *HowToRemove.Guide.* Retrieved July 22, 2017 from https://howtoremove.guide/tinba-virus-malware-removal/

Schick, S. (2015, May 13). Tinba Malware Watches Mouse Movements, Screen Activity to Avoid Sandbox Detection. *Security Intelligence.* Retrieved July 22, 2017 from https://securityintelligence.com/news/tinba-malware-watches-mouse-movements-screen-activity-to-avoid-sandbox-detection/

Symantec Security Response. (2016, October 27). *Mirai: what you need to know about the botnet behind recent major DDoS attacks.* Retrieved July 23, 2017 from https://www.symantec.com/connect/blogs/mirai-what-you-need-know-about-botnet-behind-recent-major-ddos-attacks

Winton, R (2016, February 18). Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating. LA Times. Retrieved July 23, 2017 from

http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html