Seunghyuk Baek

Sbaek44@vt.edu

ECE5480 Fall 2018

Homework #3

1. Describe the main differences between a virus, worm, and Trojan horse. Also, how are these types of malware similar?

-Computer virus is malicious program codes that inject itself into another file to infect and replicate. Often, this replication is done with human aid.

-Worm is another type of malware that can replicate itself. However, worm does not need human aid nor host file for its replication.

-Trojan horse is a malware that is disguised as legitimate software.

-All of these malwares are stored in host's storage without permission of the user. Often these malwares carry payload that can harm the user's system.

2. Describe a malware attack that causes the victim to receive physical advertisements (*material* advertisements, not emails).

-A hacker creates a malware that designed to set backdoor. Then the hacker sent it to employees of Guitar Center as new product promotion. If an employee clicks the link provided in the email, it sets backdoor to company computer leaking customer information to the hacker. The hacker sells this information to the other musical instrument retailer. The retailer sends catalog books or pamplet to victims.

3. What would be the financial advantage for a malware designer to create lots of different malicious code instances that all exploit the same vulnerability yet have different malware signatures?

-In most cases, vulnerable point of a system is not unique problem of the system. Other systems may share same weak points. Therefore, it is cost efficient to design malwares that attack same vulnerability. In addition, if these malwares have different signatures, even one malware is blocked by an anti-virus software, rest of malwares can still effectively attack other systems even though they use anti-virus software.

4. XYZ Company has just designed a new web browser and they are initiating a major marketing campaign to get this browser to become the exclusive browser used by everyone on the Internet. Why would you expect a reduction in Internet security if this marketing campaign succeeds?

-It is very easy for malicious hackers to analyze and exploit venerable point since there is only one browser exist in internet.

5**. Base your answers to the following on the reading: Kolias, Constantinos, et al. "DDoS in the IoT: Mirai and Other Botnets." Computer 50.7 (2017): 80-84. (http://ieeexplore.ieee.org/document/7971869/#full-textsection) Provide a technical summary (https://www.kendallgiles.com/ 2017/01/summarize-technical-paper/) of this article, including the steps of the Mirai botnet operation and communication**.

Introduction

This is short summary of an article “DDoS in the IoT: Mirai and Other Botnets” by Kolias et. al. from ‘Computer’ journal published by IEEE. The article can be found from “http://ieeexplore.ieee.org

/document/7971869/#full-textsection”. The article mainly states how Mirai malware operates to infect IoT devices and other malware that derived from Mirai.

Description

Mirai is a malware that targets IoT devices. IoT devise such as security camera or thermostat has very limited capability compare to PC. However, due to their limitation, it is hard to prevent simple vulnerability attack. In addition, their limited computing ability does not hinder infected IoT devices to conduct DDoS attack to a target. The author first analysis basic behavior and characteristics of Mirai. Mirai is comprised of four major components. Bot is malware that infect other devices and attack the target. C&C is centralized command tower. Loader is sending binary malware to new host devices. Finally, Report server manages and reports all active bots and new infectible hosts to C&C. Once an IoT device is infected by Mirai malware, it becomes a bot blocking further security bleach by other types of malwares and takes order from C&C. To initiate an attack toward the target, first, bots seek other public IoT devices with vulnerability points. This done by brute-force attack via TCP port 23 or 2323. Bots are loaded with 62 possible username and password combinations. Once a vulnerable device is found, a bot report back to the report server about various status of the new host. Bot master who controls these Mirai bots checks new hosts and current bots using C&C server. C&C server connect to report server via Tor browser to acquire information. Bot master commands loader to infect to new host. The loader sends infect code via GNU widget or File Transport protocol. Once the host is infected it tend to mitigate its vulnerable point preventing further intrusion. If the bot master commands attack, all bots attack the target with one of 10 attack variations. Interestingly, Mirai has several signatures and it left signature footprints in all of its operation stages. Moreover, the signatures are easy to recognize. After an institution released Mirai’s source code, more variation of Mirai emerged with stealthier characteristics.

Analysis

This paper presents a popular malware that targets IoT especially. There are various security best practice and firewalls for PC. IoT devices on the other hand has minimal security barrier compare to that of desktop and often falls under set-up-and-forget. Moreover, there is much less way to access to the status of IoT devices for users compare to PC. These factors lead higher chance of IoT infection. The problem is that IoT devices are powerful enough to conduct DDoS attack causing costly damage.

Conclusion

Just like various IoT bot malwares are emerged after Mirai, he authors warn this malware attack targeting IoT devices will increase as time goes. Because of their limitation of UI, manufacturer's defect plays significant role in IoT attacks. Furthermore, much more attention to IoT security is needed. For example, Mirai didn't try to hide its signatures, reflecting poor attention on IoT security of users.