Monitoring Network Traffic To Prevent Attacking By Torri - Team 17

Abhilash Kulkarni
New York University
New York, NY
ak7352@nyu.edu

Christian Jushin Lee
New York University
New York, NY
cjl573@nyu.edu

Eric Gan
New York University
New York, NY
eg2584@nyu.edu

Zhaofeng Jin
New York University
New York, NY
zj617@nyu.edu

Joseph Baum
New York University
New York, NY
jb5910@nyu.edu

Abstract

Torii is a new, sophisticated botnet that targets Internet of Things (IoT) devices of a multitude of different architectures. Once infected by telnet attack, IoT devices will download binary payloads which allow the botnet to communicate with a master Command and Control (CnC) server. Since network traffic patterns of the Torii botnet have already been researched and identified, network monitoring tools should allow users to identify and prevent botnet attacks on their system.

1. Introduction

The Internet of Things is an emerging class of products that network devices together using the internet. There are numerous benefits to linking the sensors of devices together, especially in manufacturing and healthcare. In 2017, there were 2.5 billion connected devices in RFID tags and other industry sensors, and it can only expected to increase. [2] It vast potential to increase quality of life and medical benefits, providing personalized healthcare and real updates through biomonitors and remote monitoring [3].

However, there are many concerns with security in IoT devices. Current devices are vulnerable to many forms of attack. Many devices have weak security, including default passwords, physical inaccessibility, and inability to be patched that make them easy targets. Once one device on the network is compromised, the rest of the machines on the network may be easily targeted as well. These factors make IoT devices an ideal platform for botnets.

Botnets are groups of internet connected devices that are infected and controlled by malware. Attackers can use these large networks to perform denial of service attacks (DDoS), steal private information, mine cryptocurrency, and other forms of attack. The recent attack DDoS in 2016 against the internet company Dyn, using the Mirai botnet on IoT devices, brought now internet connectivity for several hours [6].

With the increasing prevalence of IoT devices, it becomes much more important to secure them against malware attacks. There are many challenges to overcome. IoT devices are often cheap devices that are poorly secured and rarely updated, or even no longer supported but still in use. Many times, infected IoT devices continue working after being compromised with malware, so its owners could not realise.

Thus have been little consequences for companies that sell vulnerable IoT devices, or attackers that often operate internationally to make prosecution difficult [7]. A potential solution to mitigating future botnet attack may be through monitoring network data.

2. Background

Our solution to the botnet Torii relies on the network communication that the botnet needs both before and after infection. While a good preventative measure would be to ensure strong passwords and credentials on all IoT devices, a safe system starts with securing any vulnerable ports as well. [8] Torii will infect IoT devices via telnet attack and bypassing weak credentials. After executing an initial shell script, the botnet will download a binary payload from an FTP and NGINX server, one of the first external network communications that the botnet makes. The second stage of the payload allows Torii to communicate with a master CnC server using three different CnC addresses. Torii will both extract information about its host to send to the CnC while constantly polling the CnC server to receive commands through TCP. [10]

By monitoring network traffic in a system and watching

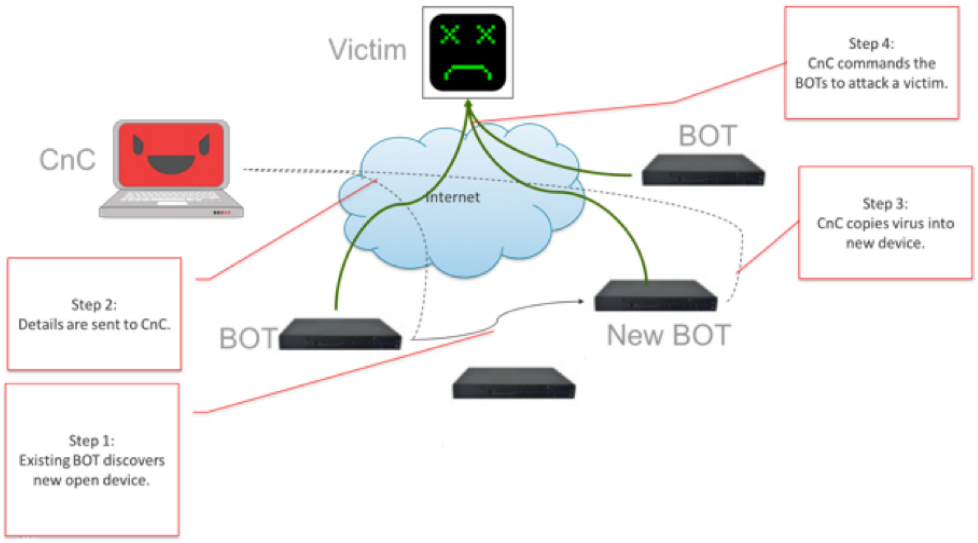

Figure 1. How Torri Infect A Victim

for suspicious data, hosts, self-signed certificates and other suspicious activities over the network we can detect Torii to certain extent. Figure 1 show the summary of a botnet attacks on the IoT device.

3. Threat Model

In the previous paper (Assignment 3.2), we had come with the attack tree, shown in Figure 2 for the way Torii attacks a IoT device. We can now access the tree and see how we can address them.

3.1. Solution Suggested By Designers

All nodes in the attack tree of the Torri can be mitigated to certain extent. Users can use firewalls for the routers and filter the IP address that look suspicious. Also users can set up block list with some known Torri IP address to prevent accessing and communication with them. Torii starts with Telnet attack on the weak passwords. As long as we have a secure way or a tool that always suggest us to use strong passwords on every application we use, these attacks can be mitigated.

4. Design

An implementation that best suites the detection of botnet activity should have following features:

1. Detect and alert the user when there is any telnet attack on the device. Telnet attack is in the first phase of the attack by botnet Torii. As long as we have a tool that stops Torri at the first phase, we need not look into its other phases. However, this is only according to the current investigation about the botnet. We may have to look into other attacks as well if the botnet starts attacking with other protocols.

2. Block a list of IP addresses from making any kind of connection with device. This can be very effective in securing the IoT device as we avoiding all the communications with suspicious IP addresses.

3. Always prompt the user to use strong passwords. We can't stop the botnet from attacking no matter what if the device has weak credentials. However, we can detect its activities with network monitors.

5. Implementation

In order to block any unwanted connections, we recommend using firewall hardware systems to ensure maximum protection across the entire network. Using the firewall, we are able to allow and disallow connections to specific sites, as well as to a range of IP addresses. Firewalls also have the capability of limiting the types of protocols that are allowed to be used over the network, so Torii would not be able to gain access through telnet. Regular workflow does not get hindered by firewalls, as they can be set up to only block unrequested incoming connections, to ensure all requests sent out by users can be answered. Firewalls can also be setup to monitor outgoing traffic to protect against suspicious links, to protect from phishing sites and other malicious sources.

In order to efficiently protect against Torii, the firewall should be set up in a specific manner. It should not allow unrequested incoming connections to the network, and it should maintain a list of suspicious links, as well as a list of

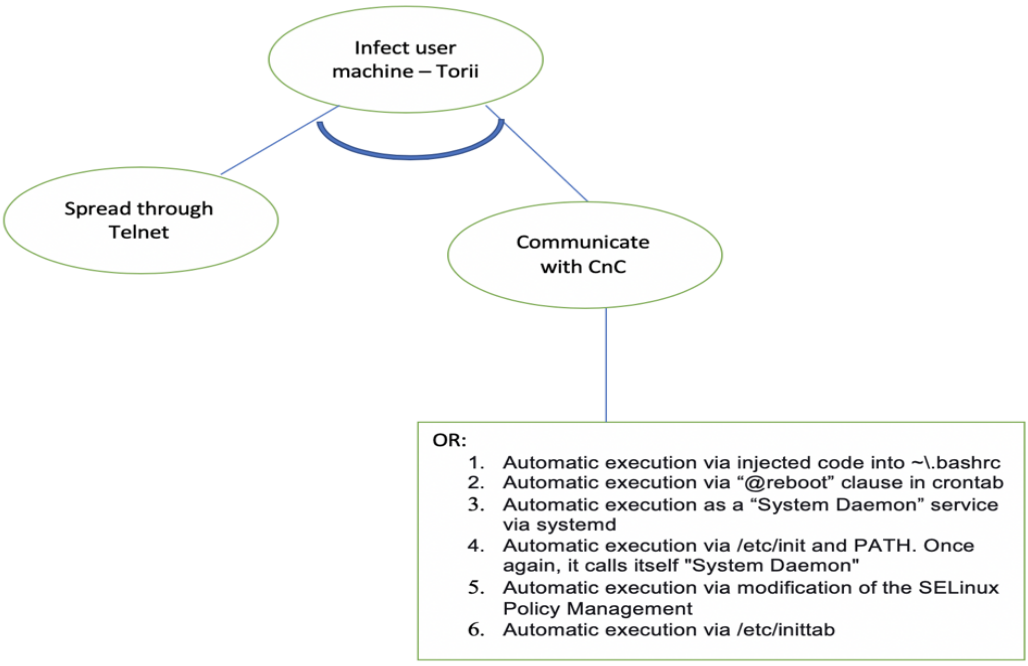

Figure 2. Attack Tree

known malware links. Network Administrators should also regularly monitor the firewall log to ensure no malicious packets were able to get through.

While firewalls cannot prevent users from creating weak passwords, network administrators can force certain password rules that all user passwords must comply with (ie, uppercase letters and numbers/symbols). They can also stress the importance of length over complexity, as in some cases longer passwords are harder to crack than shorter, possible less complex ones. In addition, Network Administrators can force users to change their passwords after a period of time, and many active directory tools, such as Microsoft's Active Directory, have this feature built-in.

6. Evaluation

With current IoT devices, new botnets can be set up only hours after an old one is taken down, as long as the creator is free to work. Many botnets simply target devices with weak or default passwords to construct botnets, so requiring strong passwords would always improve security to the device and would slow down the speed at which botnets can be created. However, it is difficult to enforce, and many companies are not punished for using weak, default passwords in their products. [7]

Firewalls analyze incoming network traffic and can block certain packets based on rules provided to it. Inbound firewalls refuse certain outside connections, while outgoing firewalls prevent communication with suspicious addresses. Torii waits for signals from a CnC server before executing any commands, so it is possible to scan the network traffic to detect its operation.

However, firewalls that merely block suspicious ip addresses and known botnet addresses, can still be susceptible to spoofing attacks. Spoofing attacks impersonate trusted ip addresses to circumvent security. It would be necessary to analyze incoming network traffic to determine suspicious packets to prevent a spoofing attack. However, analyzing packets imposes an overhead on network traffic, and can slow down performance [12].

While currently Torii requires a connection to a CnC server, there has been an emergence of peer to peer (P2P) botnets, that have no centralized control. Instead, other commands are given through many other bots. [11] It would require more advanced and intelligent network behavior monitoring to counteract these botnets types of botnets.

If the device is detected to be infected with malware, with either network monitoring or antivirus software, notifying the user would be ideal. However, the nature of IoT devices today can pose an issue. Many consumer IoT devices are designed to run autonomously, with minimal user input. And as long as the device continues to function, many

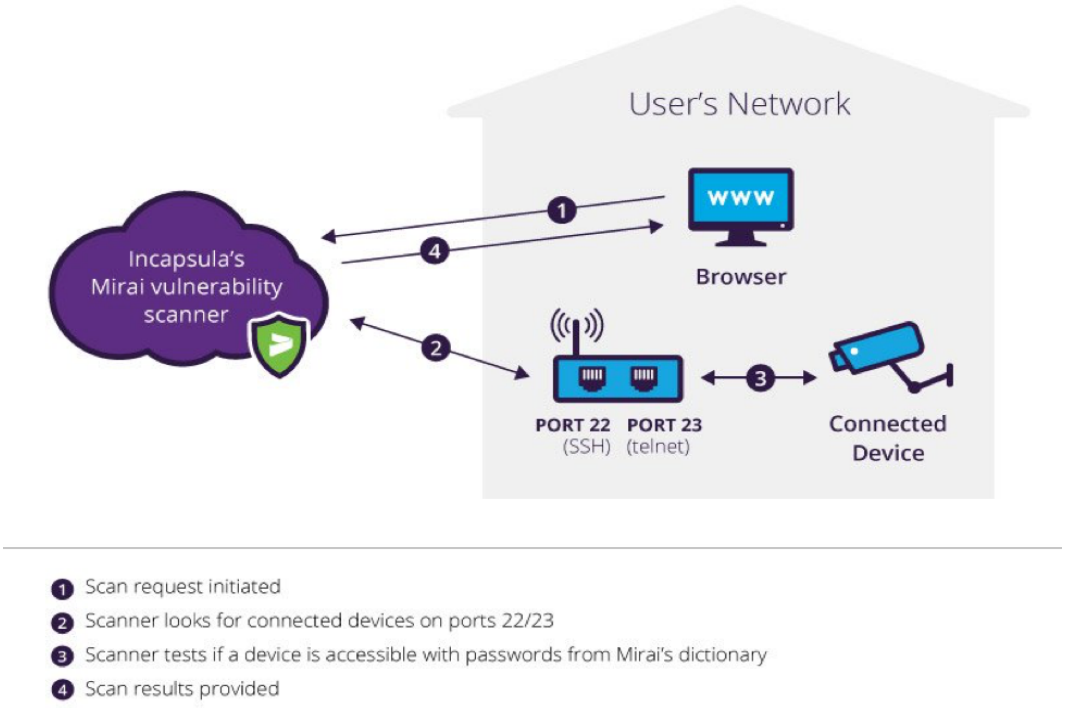

Figure 3. VPNFilter

users may opt to continue to use it, despite the malware. It may be more effective to notify the company and apply security patches, although there is currently little incentive for companies to do so. [7]

7. Related Solutions

7.1. Data Encryption/Isolation

Data encryption is an existing technology which is applied to the data wherever it is stored on disk or transport over network. Encrypting data and storing it securely not only prevent the inappropriate accessing from Torri, but also prevent Torri to transfer it back to sever. There are some tools that client could consider to use: IBM Cloud Object Storage, Microsoft Azure or OpenStack Volume Encryption.

8. Existing tools

8.1. VPNFilter

Details show in Figure 3, and open the link for more information: https://www.trendmicro.com/vinfo/hk-en/security/news/internet-of-things/internet-of-things-iot-security-developments-in-vpnfilter-and-emergence-of-torii-botnet

9. Conclusion

Firewalls and network monitors can be helpful in stopping and detecting any suspicious activities on the IoT devices. We recommend the users to use firewalls to their routers which come with predefined rules and also has the scope to add new rules to block the IP address. Also, keep the devices updated with the latest patches or application updates. However, weak passwords make the devices vulnerable to the telnet attack from where the botnet Torii infects a device. Hence, long and strong passwords are always recommended.

References

[1] https://www.wired.co.uk/article/internet-of-things-what-is-explained-iot

[2] https://www.newgenapps.com/blog/iot-statistics-internet-of-things-future-research-data

[3] https://www.i-scoop.eu/internet-of-things-guide/internet-things-healthcare/

[4] https://www.rambus.com/iot/industrial-iot/

[5] https://www.csoonline.com/article/3258748/security/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html

[6] https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn/

[7] https://www.csoonline.com/article/3240364/hacking/what-is-a-botnet-and-why-they-arent-going-away-anytime-soon.html?page=2

[8] https://www.incapsula.com/blog/mirai-scanner-unwitting-mirai-botnet-recruit.html

[9] https://www.corero.com/resources/ddos-attack-types/mirai-botnet-ddos-attack.html

[10] https://www.networkworld.com/article/3136314/security/the-secret-behind-the-success-of-mirai-iot-botnets.html

[11] https://www.wired.co.uk/article/internet-of-things-what-is-explained-iot

[12] https://www.veracode.com/security/spoofing-attack

[13] https://www.veracode.com/security/spoofing-attack

[14] https://www.techrepublic.com/article/how-to-secure-your-iot-devices-from-botnets-and-other-threats/

[15] https://www.cso.com.au/article/575407/internet-things-iot-threats-countermeasures/