MIRAI BOTNET MALWARE

ANGEL GUEVARA | FERNANDO SANTOS | EMEKA IBICHI | SHARON RIVAS

Cybersecurity Boot Camp, The University of Texas at Austin

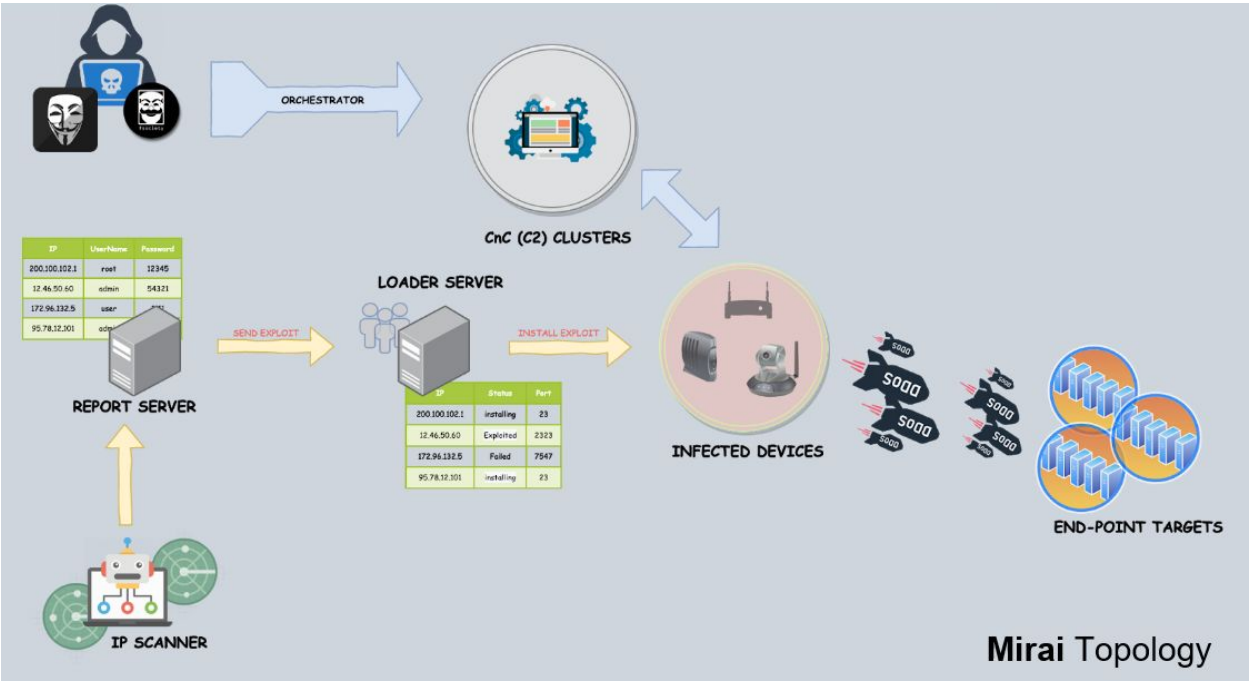
Overview

Mirai is a different botnet malware. First, the mechanism and simplicity of the attack which basically explores the vulnerability of poorly installed IoT devices. Millions of these devices have a well-known set of credentials and use legacy network protocols such as Telnet. Second, the type of device it targets, primarily IoT devices which are largely security DVRs and IP cameras. These devices run a stripped-down version of Linux with the Telnet server (Port TCP/23) enabled.

Mirai connects via Telnet and attempts to log in using a list of 60 known credentials. It operates by continuously scanning the Internet for these weak IoT devices. If the default usernames and passwords are not changed, Mirai is able to log in to the device and cause an infection that turns them into a network of remotely controlled bots or zombies that can be used to launch DDoS attacks to predefined targets.

They are forced to report to a central command control server, which turns them into bots waiting for commands to initiate DDoS attacks.

Processes are attempted to be killed that would prevent it from running and persisting on the device. The Telnet server, and often web server, is killed at this stage.



Who is the author(s) of Mirai?

Mirai was developed by Paras Jha and Josiah White co-founded Protraf Solutions, a company offering mitigation services for DDoS attacks.

When was it first discovered?

Mirai was first found in September 2016, the authors of the Mirai malware launched an extremely large and unusual distributed Denial-of-Service (DDoS) attack to knock offline the website **KrebsOnSecurity.com** of a well-known security expert. The attack began on Sep 20th which generated approximately 620 Gbps in traffic. The largest attack had seen previously clocked in earlier this year at 363 Gbps.

However the worst was still to come, a week later they released the source code into the world, possibly in an attempt to hide the origins of that attack. This code was quickly replicated by other cybercriminals, and is believed to be behind the massive attack that brought down the domain registration services provider in New Hampshire, Dyn, in October 2016.

On Friday, October 21, as **one of the largest and most powerful DDoS attacks in recent history,** a distributed denial of service attack (DDoS) on Domain Name System (DNS) provider Dyn from New Hampshire managed to disrupt an array of the internet's biggest websites, including Spotify, Twitter, Reddit, Amazon, Netflix, and PayPal. Various reports have confirmed it was a sophisticated, highly distributed attack involving 10s of millions of IP addresses.

How much did it cost for KrebsOnSecurity.com and Dyn?

KrebsOnSecurity.com

Berkeley School of Information estimated that the attack to KrebsOnSecurity.com website cost connected device owners nearly $324,000. Their research has calculated that, with the extra energy consumption and bandwidth costs, the botnet used in the attack would have cost device owners $323,973.75, or $13.50 for each device.

On their research, they infected devices with Mirai and observed their activity in a lab, the group found that Mirai-infected devices show only small increases in electricity consumption – by far the greater cost to consumers is in the bandwidth stolen by the infected Things. The research quantifies a worst-case scenario, with the Mirai botnet operating at peak power in a UDP DDoS attack. According to the report, the number of devices controlled by the botnet briefly hit a peak of 600,000 at the end of November 2016. The projected cost to consumers of this attack would be $68 million.

Dyn

Analysis and reports suggest that Dyn lost 8% of its customers which dropped the services after the attack which translate to more than 14,000 Internet domains stopped using managed DNS services from Dyn. Data shows that Dyn lost a pretty big chunk of their customer base because they were affected by Mirai.

This means that a group of unsecured IoT devices can end up causing huge online repercussions resulting in system outages and heavy subsequent losses.

Technical Expose

- Is this a local or remote type of attack?
    - Both. **Mirai** has a few components that make the exploit to be locally install, but remote controllable.
- How is the exploit installed?
    - The exploit is run in memory, so a simple reboot will flush its functionality.
- How does it work?
    - The main motive behind **Mirai** is to create a massive DDoS attack to predefined targets.
    - Combines multiple types of DDoS attack (Volumetric, Amplification/Reflection)
    - A high-level overview of the exploit:
        - Scanning IPv4 → Report Server → Loader Server → Dispatch Exploit → Attacker Gets Control of the device → Send Commands via CnC → Deploy DDoS attack.

Mirai main components:

Scanning:

- Begins its propagation through rapid scanning (Mostly Port 23 or 2323 it expanded its port range later on).
- Script sends finger-printable scan packets to random IPs.
- If the port is open, a brute force attack is started with known vendor credentials.
- Next, the info is sent out to the Report Server.
- Code:
    - https://github.com/jgamblin/Mirai-Source-Code/blob/master/mirai/bot/scanner.h
    - https://github.com/jgamblin/Mirai-Source-Code/blob/master/mirai/bot/scanner.c

Report Server:

- Main purpose of the server is to keep track of incoming bot reports
- Sends the “Dispatch” information to the Loader
- Listens on port TCP 48101

Loader Server:

- This guy keeps track of all the bots.
- It closes ports after infection.
- It maintains a list of IP addresses when the method of infection (TFTP, WGET)
- Good news! Not everything is “infectable”

Attacker infrastructure:

- CnC servers:
  - Multiple clusters were identified based on bots DNS queries
  - These clusters targeted different endpoints
- Relays commands to infected devices.
- Deploy multiple types of attack (all of them created for DoS):
  - UDP Flood
  - TCP flood
  - HTTP flood
  - GRE flood (unusual)

Containment Strategy

This document contains counsel as to the scope and severity of infections by Mirai, as well as steps to fix infected computers and prevent future attacks.

Scope

The scope of the attack surface vulnerable to this sample includes information on:

- Affected operating systems/services and versions
- Types of devices usually targeted

Severity

Determining the severity to look for information on:

- How much damage the malware does to the infected computer (e.g., is it destroyed vs inaccessible vs just a little bit slower?)
- How hard is it to remove the malware without replacing the computer?
- How much data can the malware get access to—is it just adware, or does it expose a full root shell to an attacker?

Based on our findings, we concluded that this sample of Mirai is severe and should be patched as soon as possible.

Solution

Below are steps to fix a computer that has been affected; which patches to use if any; and strategies for preventing future attacks.

To prevent future devices from being infected or to be proactive before buying an IoT device:

- Research the capabilities and security features of an IoT device before purchasing
- Perform an audit of IoT devices used on your network
- Use strong and unique passwords for device accounts and Wi-Fi networks
- Do not allow the default username and/or password to go unchanged
- Disable features and services that are not required
- Disable Universal Plug and Play (UPnP) on routers unless absolutely necessary
- Regularly check the manufacturer’s website for firmware updates
-

- Do not use port forwarding to open ports for IoT reachability, use NAT and ACLs instead
- Perform credential rotation if possible
- When possible, isolate IoT devices on a segregated VLAN allowing only egress traffic
- If possible limit the data rate transfer with QoS settings, DSCP tagging, etc.
- If within budget, buy IoT devices capable of using TLS or Any Cloud Authentication service (Ex. Encrypted S3 buckets)
- Disable all remote (WAN) access to your devices
- To verify that your device is not open to remote access, you can use an online port scanner to scan the following ports: SSH (22), Telnet (23), and HTTP/HTTPS (80/443)
- If you want to check a suspicious file you could go to virus total to review it: https://www.virustotal.com/gui/home/upload

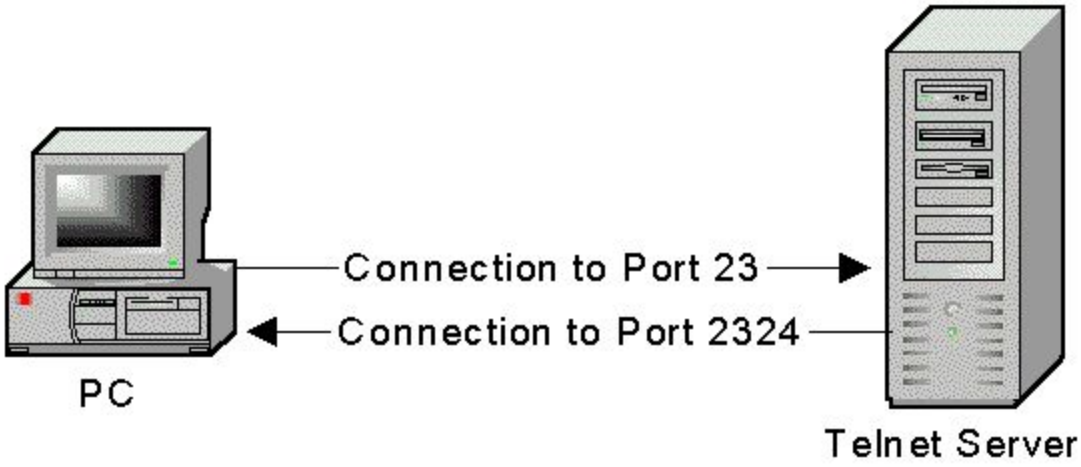
Awareness Training

This document explains how end users can:

- Identify an infection by Mirai
- Protect your data and isolate the infected machine
- Determine which organizational stakeholders to notify in the event of a compromise

Identification

- Infected machines are initially hard to recognize, they keep working in a usual manner despite some periods of slowdowns or random crashes.
- If you have exposed port 23 such as from a DVR or IP camera connected to the Internet, then it is likely you have been infected.
- You can find out if you have this port open by using:
    - ShieldsUP an online port scanning service created by Steve Gibson of Gibson Research Corporation. The purpose of this utility is to alert the users of any ports that have been opened through their firewalls or through their NAT routers.
    - https://www.yougetsignal.com/tools/open-ports/
    - http://www.t1shopper.com/tools/port-scan/



Quarantine and Response

- If you have the original version of Mirai, this does not have any mechanism to survive a reboot of the device. Restarting the device will remove Mirai and because it only takes a few minutes for the device to be found and re-infected, it is also vital that you close the port that allowed you to become infected in the first place.

- You should close off all access to port 23 on the infected device and this will stop Mirai from infecting the device again. If possible, attempt to change the default password but unfortunately, this isn't possible on most devices. Port 23 is used for Telnet purposes. If you do not use Telnet services you can disable it using the following method/s. By default, almost all have this port closed. The steps to opening it is called Port Forwarding.
- If you require remote access such as to a DVR, then it should be done over a VPN connection, preventing anyone else from connecting to the DVR in the first place.
- If you have a variant of Mirai you may need to disconnect from the internet and enter Safe Mode with networking then utilize anti-malware software.

Escalation

- In the event that a device is found to be infected with the Mirai malware, first inform the technical team. Then the entire staff should be informed through various channels. This is to ensure action is taken to minimize affected users and precautions are sent to uninfected users to take preventative measures.
- Ideally, the technical team or I.T. security team would have a Response Plan they can adhere to and quickly go into action.
- Legal counsel may be necessary to include if consumer data is leaked. As well as marketing who could then help inform customers and commence damage control.