EDUNET FOUNDATION - Case Studies: IoT Security

Case Study 1 - The Mirai Botnet

What is the Mirai botnet?

In late 2016 in France, telecom company OVH was hit by a distributed denial-of-service (DDoS) attack. Experts were struck by how the assault was 100 times larger than similar threats. The following month, over 175,000 websites suffered, as Dyn, a managed DNS (Domain Name System) provider, was hit by another powerful DDoS attack. Much of the eastern United States and some of Europe suffered a significant drop in Internet quality.

Some hacking groups like Anonymous and New World Hackers claimed responsibility in retaliation for WikiLeaks founder Julian Assange being cut off from the Internet by the Ecuadorian government. However, American officials and security firms cast doubt on these claims. One thing was for sure. The weapon behind these attacks was the Mirai botnet malware.

The timing couldn't have been worse. With the American elections around the corner, there were fears that the malware would impact voters. Experts speculated that the malicious software was the handiwork of a rogue state intent on manipulating the democratic process.

They couldn't have been further from the truth.

An IoT botnet (a network of computers, each of which runs bots) was used to execute the worst DDoS attack against Internet performance management services provider Dyn back in October 2016. As a result, several websites went offline, including majors like CNN, Netflix, and Twitter.

After becoming infected with Mirai malware, computers continuously search the web for susceptible IoT devices before infecting them with malware by logging in using well-known default usernames and passwords. These gadgets included digital cameras and DVR players, for example.

Who created the Mirai botnet?

Three young men named Paras Jha, Dalton Norman, and Josiah White created Mirai as part of a Minecraft scam. Their initial goal was to run an extortion scheme by taking down Minecraft servers and start a protection racket. After Internet user “Anna-senpai," who investigators believe is an alias for Paras Jha, published the source code for Mirai online, the botnet mutated.

How did Mirai botnet get its name?

Mirai is a Japanese given name that means "future." According to a chatlog between Anna-senpai and Robert Coelho, an executive at ProxyPipe.com, the Mirai botnet was named after the Japanese animated series Mirai Nikki.

How does Mirai spread?

Let’s answer some burning questions like “What is a DDoS attack?”, “What is a botnet?”, and “What is IoT?” before explaining how the Mirai botnet spread.

A botnet is a network of hijacked computers under the control of a threat actor, typically called a bot herder. The network of computers, or bots, runs an automated script to perform a task.

Botnets don’t always serve bad actors. For example, the crowdsourced scientific experiment, SETI@home, searched for extraterrestrial life through a voluntary botnet. However, bot herders usually use botnets for attacks like DDoS. Using the extensive resources of the many computers in a botnet, they send excessive traffic to a website or service to overwhelm it and take it down.

The goal of a DDoS attack is anything from mischief to activism to extortion. For example, the Mirai authors wanted to undermine critical Minecraft servers in order to sell DDoS mitigation services. They also allegedly attacked ProxyPipe.com because it provided similar services and was a potential competitor.

The Mirai botnet was unlike other malware because it attacked IoT devices instead of computers. IoT, of course, is a fancy name for devices that carry sensors and software, allowing them to communicate with other devices and systems. Mirai infected vulnerable consumer devices like smart cameras. It also weaponized Realtek-based routers.

Mirai scanned the Internet for targets and breached their security by trying default username and password combinations. It didn’t take long for Mirai to infect hundreds of thousands of IoT devices in countries worldwide and gain significant power. Mirai’s attack in 2016 against OVH peaked at a startling 1TBps.

How was the Mirai botnet stopped?

According to TechTarget, the FBI uncovered the identities of the Mirai creators through the metadata around their anonymous accounts after an extensive investigation. Not only did the trio plead guilty to various computer crimes, but they agreed to help make amends. One of their bigger contributions was to build an IoT honeypot called Watchtower. A honeypot is essentially a digital trap for malware and hackers.

Is Mirai botnet still active?

The authorities may have caught the Mirai creators, but the spirit of their botnet lives on. Numerous groups took advantage of the open-source code to create mini variants. Besides DDoS attacks, botnets can help hackers weaken website security, steal credit card data, and send spam.

How can the Mirai malware be mitigated?

Updating your IoT device firmware to the latest version can help mitigate the risk of a botnet infection. Additionally, changing default username and passwords will prevent threat actors from utilizing known default login credentials. Segmenting your network so your IoT devices are on a separate network can also be useful.

To secure your computer from botnet infections, regularly install the latest security patches for your operating system and download anti-malware tools. You may also be put at risk by old out of date routers — so consider upgrading. A proactive approach can harden your defences against all types of botnet infections.

How does Mirai work?

Mirai scans the Internet for IoT devices that run on the ARC processor. This processor runs a stripped-down version of the Linux operating system. If the default username-and-password combo is not changed, Mirai is able to log into the device and infect it.

IoT, short for Internet of Things, is just a fancy term for smart devices that can connect to the Internet. These devices can be baby monitors, vehicles, network routers, agricultural devices, medical devices, environmental monitoring devices, home appliances, DVRs, CC cameras, headset, or smoke detectors.

The Mirai botnet employed a hundred thousand hijacked IoT devices to bring down Dyn.

Who were the creators of the Mirai botnet?

Twenty-one-year-old Paras Jha and twenty-year-old Josiah White co-founded Protraf Solutions, a company offering mitigation services for DDoS attacks. Theirs was a classic

case of racketeering: Their business offered DDoS mitigation services to the very organizations their malware attacked.

Why does the Mirai malware remain dangerous?

The Mirai is mutating. Though its original creators have been caught, their source code lives on. It has given birth to variants such as the Okiru, the Satori, the Masuta and the PureMasuta. The PureMasuta, for example, is able to weaponize the HNAP bug in D-Link devices. The OMG strain, on the other hand, transforms IoT devices into proxies that allow cybercriminals to remain anonymous.

There is also the recently discovered - and powerful - botnet, variously nicknamed IoTrooper and Reaper, which is able to compromise IoT devices at a much faster rate than Mirai. The Reaper is able to target a larger number of device makers, and has far greater control over its bots.

What are the various botnet models?

Centralized botnets

If you think of a botnet as a theatrical play, the C&C (Command and Control Server, also known as the C2) server is its director. The actors in this play are the various bots that have been compromised by malware infection, and made part of the botnet.

When the malware infects a device, the bot send out timed signals to inform the C&C that it now exists. This connection session is kept open till the C&C is ready to command the bot to do its bidding, which can include sending out spam, password cracking, DDoS attacks, etc.

In a centralized botnet, the C&C is able to convey commands directly to the bots. However, the C&C is also a single point of failure: If taken down, the botnet becomes ineffective.

Tiered C&Cs

Botnet control may be organized in multiple tiers, with multiple C&Cs. Groups of dedicated servers may be designated for a specific purpose, for example, to organize the bots into subgroups, to deliver designated content, and so on. This makes the botnet harder to take down.

Decentralized botnets

Peer-to-peer (P2P) botnets are the next generation of botnets. Rather than communicate with a centralized server, P2P bots act as both a command server, and a client which receives commands. This avoids the single point of failure problem inherent to centralized botnets. Because P2P botnets operate without a C&C, they are harder to

shut down. Trojan, Peacomm and Stormnet are examples of malware behind P2P botnets.

How does malware turn IoT devices into bots or zombies?

In general, email phishing is a demonstrably effective way of infecting the computer - the victim is tricked into either clicking a link that points to a malicious website, or downloading infected attachment. Many times, the malicious code is written in such a way that common antivirus software is not able to detect it.

In the case of Mirai, the user doesn't need to do much beyond leaving the default username and password on a newly installed device unchanged.

What is the connection between Mirai and click fraud?

Pay-per-click (PPC), also known as cost-per-click (CPC), is a form of online advertising in which a company pays a website to host their advertisement. Payment depends on how many of that site's visitors clicked on that ad.

When CPC data is fraudulently manipulated, it is known as click fraud. This can be done by having people manually click on the ad, by use of automated software, or with bots. Through this process, fraudulent profits can be generated for the website at the expense of the company placing those ads.

The original authors of Mirai were convicted for leasing their botnet out for DDoS attacks and click fraud.

Why are botnets dangerous?

Botnets have the potential to impact virtually every aspect of a person's life, whether or not they use IoT devices, or even the Internet. Botnets can:

- Attack ISPs, sometimes resulting in denial-of-service to legitimate traffic
- Send spam email
- Launch DDoS attacks and bring down websites and APIs
- Perform click fraud
- Solve weak CAPTCHA challenges on websites in order to imitate human behavior during logins
- Steal credit card information
- Hold companies to ransom with threats of DDoS attacks

Let's quickly summarize what you learnt so far.

1. Summary of the Mirai Botnet Attack:

Recap the key details of the Mirai botnet attack, including its origin, its utilization of compromised IoT devices, and the scale of the attack on internet infrastructure.

2. Lessons Learned:

Highlight the urgency of securing IoT devices against botnet attacks like Mirai to prevent their exploitation for malicious purposes.

Stress the need for manufacturers to embed security measures within devices and for users to adopt secure practices.

3. Implications for IoT Security:

Discuss how the Mirai botnet attack exposed the susceptibility of a vast number of poorly secured IoT devices.

Emphasize the cascading impact on broader internet infrastructure due to the use of compromised devices in coordinated attacks.

4. Preventive Measures:

Recommend changing default credentials, regularly updating firmware, and disabling unnecessary services to protect IoT devices from being compromised.

Suggest network segmentation to prevent the spread of botnet infections and the isolation of compromised devices.

5. Supply Chain and Third-Party Considerations:

Explain how the attack highlights the potential risks introduced through the supply chain, especially when devices have weak security measures.

Stress the importance of working with reputable manufacturers and third-party vendors to ensure device security.

6. Regulatory and Compliance Implications:

Discuss the potential legal and regulatory consequences of insecure IoT devices, underscoring the need to comply with data protection and cybersecurity regulations.

Mention the accountability of manufacturers and service providers in preventing their devices from being enlisted in botnets.

7. Collaborative Efforts:

Emphasize that botnet attacks like Mirai require a collective response involving manufacturers, users, cybersecurity experts, and law enforcement.

Encourage collaboration in sharing threat intelligence and implementing security measures to prevent future attacks.

8. Ethical and Privacy Concerns:

Reflect on the ethical implications of devices being enlisted in a botnet without the knowledge or consent of their owners.

Discuss the potential violation of users' privacy and how the attack underscores the importance of securing personal information.

9. Resilience and Mitigation Strategies:

Highlight the significance of having effective incident response plans to swiftly mitigate and contain botnet attacks.

Suggest incorporating network monitoring, traffic analysis, and intrusion detection systems to identify and counter botnet activities.

10. Impact on Internet Infrastructure:

Address the far-reaching consequences of Mirai's attack on internet infrastructure and the disruption it caused to major websites and services.

Emphasize the need for securing IoT devices to prevent their collective exploitation as tools for large-scale attacks.

11. Call to Action:

Urge organizations and individuals to learn from the Mirai botnet attack and take proactive measures to secure IoT devices.

Stress the ongoing effort required to keep pace with evolving cyber threats and to build a more resilient IoT ecosystem.

12. Conclusion:

Summarize the profound impact of the Mirai botnet attack on IoT security and the broader internet landscape.

Conclude by underscoring the collective responsibility to secure IoT devices and mitigate the potential risks associated with botnet attacks.

Feel free to adapt and expand upon these points based on the specific details and focus of your case study.

Reference

https://www.malwarebytes.com/what-was-the-mirai-botnet

https://www.cloudflare.com/en-in/learning/ddos/what-is-a-ddos-botnet/

https://chat.openai.com/

