Mirai Botnet Attack (2016)

Elisa Veloso and Adam Roque

1: The attack

- Emerged in August 2016, and became notorious for launching massive DDoS attacks using insecure IoT devices
- Devices infected included DVRs, IP cameras, home routers, etc., often with default or hardcoded passwords
- The botnet scanned the internet, brute-forced logins via Telnet, attempted to log in default passwords, and then downloaded malware to enslave the device.
- Infected devices were controlled via a central Command and Control (C2) server and used to launch attacks on targets.

1: The attack

- A botnet is a collection of internet-connected computers — the “bots” — that are under remote control from some outside party.
- Because there are many bots, the controllers basically have access to a sort of hacked-together supercomputer that they can use for nefarious purposes, and because the bots are distributed over various parts of the internet, that supercomputer can be hard to stop.
- Paras Jha, an undergraduate at Rutgers, became interested in how DDoS attacks could be used for profit.

2: Key Events

- Aug 1, 2016: First Mirai scans detected.
- Sep 20–21: Record-breaking 623 Gbps DDoS attack on Krebs on Security.
- Sep 30: Mirai source code publicly released, leading to multiple variants.
- Oct 21: Major attack on Dyn DNS provider, disrupting access to Twitter, Netflix, Reddit, etc.
- Nov: Attack on Liberia's telecom infrastructure via CWMP protocol.
- Feb 2017: Arrests of some attackers and operators

2 : Explain affected assets and consequences.

Affected assets:

- **Hundreds of thousands of IoT devices**: IP cameras Digital video recorders (DVRs),Routers,Baby monitors and Other embedded Linux IoT devices

.

- **DNS provider Dyn**: critical to internet routing.
- **High-profile websites** relying on Dyn: GitHub, Netflix, Reddit, Airbnb, Amazon, etc.

Consequence:

- Large-scale internet outages.
- Disruption of online services for millions of users.
- Highlighted the weakness of IoT security and dependency on core internet infrastructure.
- Public and regulatory wake-up call about IoT security practices.

3 : The countermeasures taken and their effectiveness.

1. **Arrest of the Creators**

   Action: The FBI identified and arrested Paras Jha, Josiah White, and Dalton Norman in late 2017. They pleaded guilty to creating and deploying Mirai.

   Effectiveness:
   - **High (for the original botnet)** – The original operators stopped creating new attacks after arrest.
   - **Limited (for future threats)** – The source code was already released publicly, leading to many **copycat variants**

2. **Takedown and Blocking of C2 Servers**

- **Action**: Internet service providers and cybersecurity firms **identified and blocked** known **command-and-control (C2) servers** used by Mirai.

- **Effectiveness**:
  - **Short-term**: Disrupted communication between bots and attackers, reducing immediate threat.
  - **Long-term**: Attackers **quickly adapted**, rotating IPs or setting up new C2 servers. Blocking is a **cat-and-mouse game**.

3 : the countermeasures taken and their effectiveness.

3. Patching and Firmware Updates by Vendors:

- **Action**: Some manufacturers released **patches** to fix default credentials and vulnerabilities.

- **Effectiveness**:
  - **Mixed**:
    - **Effective** on devices that were patchable and used by tech-savvy users.
    - **Ineffective** for devices that: Had no update mechanism,Were already deployed and forgotten,Had hardcoded credentials.

4. Awareness and Best Practice Campaigns:

- **Action**: Public and private cybersecurity entities promoted:Changing default passwords,Disabling remote access,Network segmentation

- **Effectiveness**:
  - **Moderate**: Awareness increased among enterprises, but millions of consumers still leave devices unsecured. Low adoption in the consumer IoT market.

3 : the countermeasures taken and their effectiveness.

5. Development of Detection and Mitigation Tools:

- **Action**: Researchers and companies built tools to: Detect Mirai-infected devices ,Auto-block traffic patterns.

- **Effectiveness**:
  - **Good in enterprise networks** with strong monitoring.
  - **Less effective** in home networks or unmanaged environments.

6. Improvements in DNS and DDoS Resilience:

- **Action**: Dyn and other DNS provider: Improved DDoS mitigation strategies, Deployed Anycast routing, load balancing, and backup servers

- **Effectiveness**:
  - **High**: Major DNS providers are now more resilient to volumetric attacks.

References:

- https://www.csoonline.com/article/564711/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html
- Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman, J. A., Invernizzi, L., Kallitsis, M., Kumar, D., Lever, C., Ma, Z., Mason, J., Menscher, D., Seaman, C., Sullivan, N., Thomas, K., & Zhou, Y. (2017). *Understanding the Mirai Botnet*. In **26th USENIX Security Symposium (USENIX Security 17)** (pp. 1093–1110). USENIX Association. https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis

Thank You