DATA AND NETWORK SECURITY

Case Study I: Dyn DDOS Attack (Mirai)

1

Overview

- Classification: Malware
  - Worm creating a Botnet
  - Worms self replicate on different systems across a network
  - Bots are infected machines that take commands from a central source
  - BotNets are collections of bots
- Botnet comprised of IoT (Internet of Things) devices
- Timeline
  - First appeared : August 2016
  - Source code was 'published' in 2017
- Key actions
  - Replication
  - Attack

2

Architecture

- Mirai
  - Infects IoT devices
    - Routers
    - TVs
    - IP Cameras
  - Holds 60 common factory username/password combinations
  - Holds a blacklist of IP addresses to avoid
    - Private address
    - USPS
    - DoD
  - Identify and remove 'competing' malware

3

4

Infection Process

- Fast scan of pseudo-random IP addresses
  - Bots (infected IoT devices) scan for other vulnerable IoT devices
    - TCP SYN on telnet port
    - If IoT device responds
      - Brute force login with 60 username/pw pairs
      - On success: Send IP and credentials to a 'collection' server
  - Collection servers upload virus to vulnerable IoT devices making them new *Bots* to add to the Botnet
- Victim IoT devices
  - Perform normal operations
  - Occasional lag
  - Increased bandwidth usage

Data Security: Case Study I : Dyn DDOS Attack (Mirai) [Tony Mione, SUNY Korea, 2020]

4

5

Mobilization Process

- Infected IoT devices monitor a *Command and Control* server.
  - The server directs attacks against a target.
  - Collective Botnet generates a huge Distributed Denial of Service attack
  - DDOS attacks circumvent IP blocking defense against standard Denial of Service attacks
- IoT devices can be retasked at any time to attack a new target.

Data Security: Case Study I : Dyn DDOS Attack (Mirai) [Tony Mione, SUNY Korea, 2020]

5

6

History of Mirai Attacks

- Sep 19, 2016 – Attacked OVH – one of the largest European hosting providers
- Original author releases source code
  - Typical tactic
  - Plausible Deniability
  - Future attacks increased [Mostly unskilled 'actors']
- Oct 12, 2016 – Attack against DYN Domain Name Services
  - Crippled most of US ability to reach business and entertainment sites
    - AirBNB, Amazon, Paypal
    - Netflix, Twitter, Reddit, HBO
    - others

Data Security: Case Study I : Dyn DDOS Attack (Mirai) [Tony Mione, SUNY Korea, 2020]

6

7

History of Mirai Attacks

- Oct 31, 2016 – Lonestar Cell – One of Liberia's largest telecom operators
- Nov 26, 2016 – Deutsche Telecom –
  - 900,000 routers knocked offline
  - Advanced Mirai variant

7

8

IoT issues

- Easy targets of malware
- Default credentials are difficult to change
- Very few users of IoT apply security patches

8

9

Sources

- https://en.wikipedia.org/wiki/Mirai_(malware)
- https://blog.attify.com/how-mirai-botnet-hijacks-your-devices/
- https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis

9