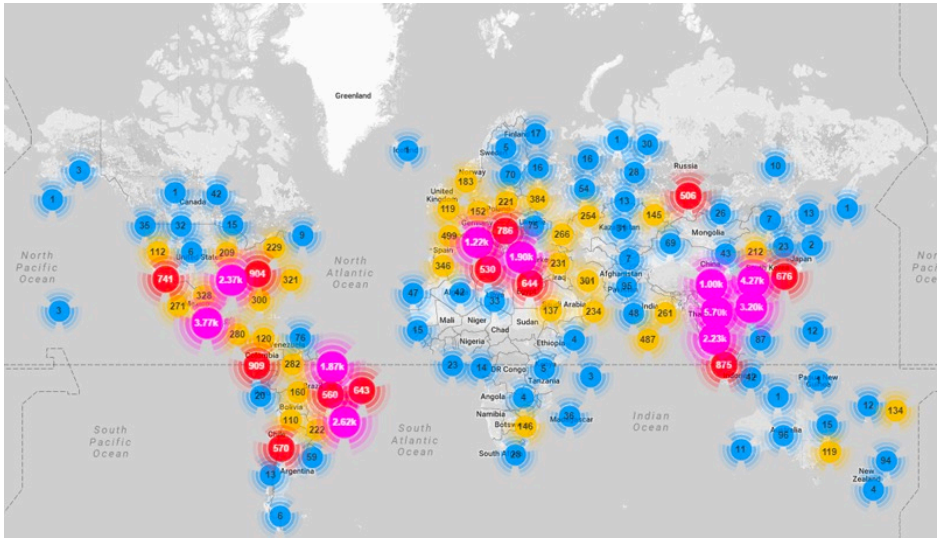
Mirai e Mitre ATT&CK

Mariano Ceccato

mariano.ceccato@univr.it

Mirai

- Botnet composed mainly of IoT devices (>600k infections)
- Massive distributed denial-of-service attack 2016
  - Estimated around 600 Gbps in volume on a single target
- At least on 7 high-profile targets



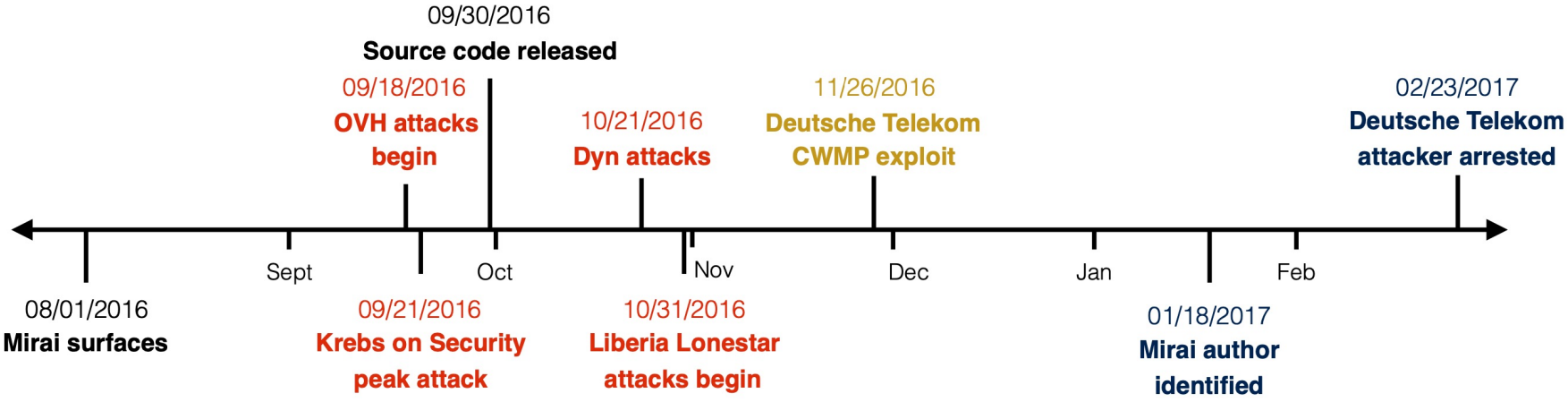
Peculiarities

- Efficient spreading based on internet-wide scanning
- Wide usage of insecure default passwords in IoT devices
- Simple botnet behavior allows to spread on many heterogeneous devices

Bootstrap

- First minutes: already 834 devices were scanning
- 10 minutes: 11k devices infected
  - 75 minutes doubling time
- 20 hours: 64,500 devices
- Steady state: 200k-300k devices
- Peak: 600k devices

Timeline


09/30/2016
Source code released
09/18/2016
OVH attacks begin
10/21/2016
Dyn attacks
11/26/2016
Deutsche Telekom CWMP exploit
02/23/2017
Deutsche Telekom attacker arrested
08/01/2016
Mirai surfaces
09/21/2016
Krebs on Security peak attack
10/31/2016
Liberia Lonestar attacks begin
01/18/2017
Mirai author identified
Sept
Oct
Nov
Dec
Jan
Feb

Devices

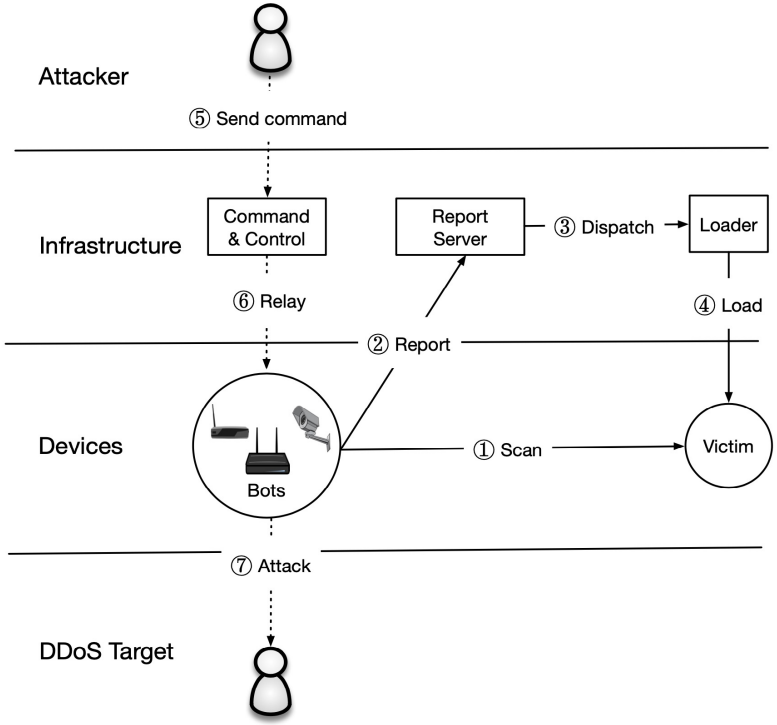
- IoT devices
  - Network attached storage devices
  - Home routers
  - DVR, cameras, printers, TV receivers
- Dozens of different manufacturers
  - Dahua, Huawei, ZTE, Cisco, ZyXEL, MikroTik
- Devices with limited computational capacity, located in regions with low bandwidth

World's top manufacturers of consumer electronics lacked sufficient security practices to mitigate threats like Mirai

Command and control

- Custom bot-to-C2 server protocol
- 64k attack commands from 484 unique C2 servers
- Individual C2 servers often repeat the same attack command in rapid succession
- Multiple distinct C2 severs often issues the same attack command

Propagation overview



TCP ports

- A service accepting incoming connections is listening on a TPC port (identified by a port number)
  - 25: SMTP Simple Mail Transfer Protocol.
  - 143: IMAP Internet Message Access Protocol
  - 80: HTTP Hypertext Transfer Protocol. ...
  - 443: HTTPS secure HTTP
  - 20-21: FTP File Transfer Protocol
  - 23: TELNET to establish connections between remote computers
  - 22: SSH Secure shell login
  - 53: DNS Domain Name System

What “Technique”?

- Probes for open TCP ports:
  - Asynchronously send TCP probes
  - To pseudorandom IPv4 addresses (excluding blacklisted)
  - On Telnet TCP ports 23 and 2323

What “Technique”?

- In case of potential victim is found
  - Brute-force telnet login
  - 10 username/password pairs randomly from a pre-configured list of 62

What “Technique”?

- Turn detection more difficult
- Delete the downloaded binary
  - The threat is not persistent

What “Technique”?

- Turn detection more difficult
- Obfuscate the process name
  - Meaningless name: pseudorandom alphanumeric string

What “Technique”?

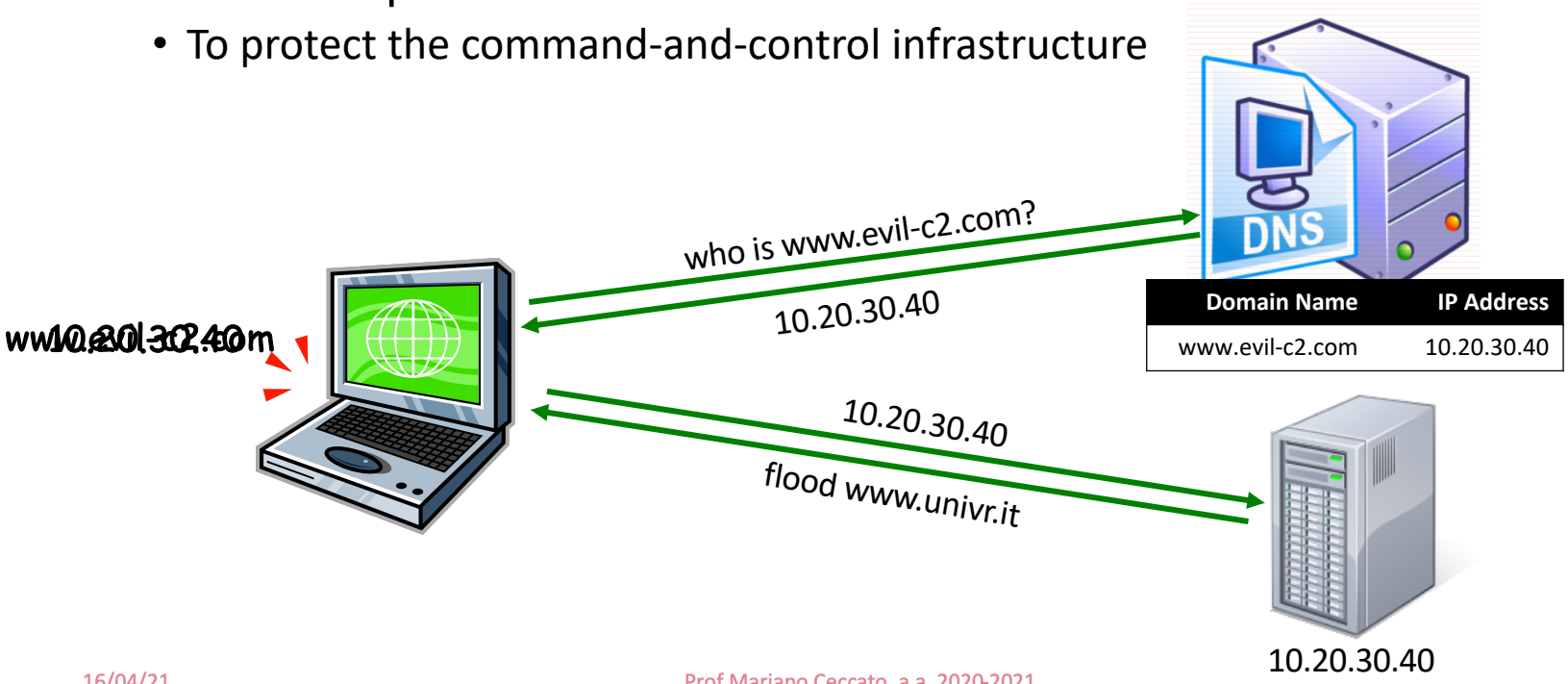
- Determine system environment
  - Processor family, operating system
- Download and execute architecture-specific malicious executable

What “Technique”?

- Wait for attack commands from the server controlled by the attacker

What “Technique”?

- Initially the C2 server was contacted using the server IP address
- Move from ip-based C2 to domain-based C2
  - To protect the command-and-control infrastructure



What “Technique”?

- Flood a victim server with many requests
- The victim server can not handle the high volume of requests
  - Some requests can not be processed before the timeout
  - Including benign requests
- Estimated around 600 Gbps in volume on a single target

Summary

Tactic	Technique	Description
Reconnaissance	Active scanning	Asynchronously send TCP probes to pseudorandom IPv4 addresses (excluding blacklisted) on Telnet TCP ports 23 and 2323
Credential access	Brute Force: Password Spraying	In case of potential victim is found, brute-force telnet login, 10 username/password pairs randomly from a pre-configured list of 62
Defense evasion	Indicator Removal on Host: File Deletion	Delete the downloaded binary (not persistent)
Defense evasion	Hide Artifacts	Obfuscate its process name as pseudorandom alphanumeric string
Lateral movement	Remote Services: SSH	Determine system environment Download and execute architecture-specific malware
Command and Control	Web protocols	Listen for attack commands from the command and control server
Command and Control	Dynamic resolution	Move from ip-based C2 to domain-based C2, to protect the command-and-control infrastructure
Impact	Endpoint Denial of Service	Estimated around 600 Gbps in volume on a single target

References

- Antonakakis, Manos, et al. "Understanding the mirai botnet." 26th USENIX security symposium (USENIX Security 17). 2017.
- https://www.radware.com/security/ddos-experts-insider/hackers-corner/tactics-techniques-procedures/