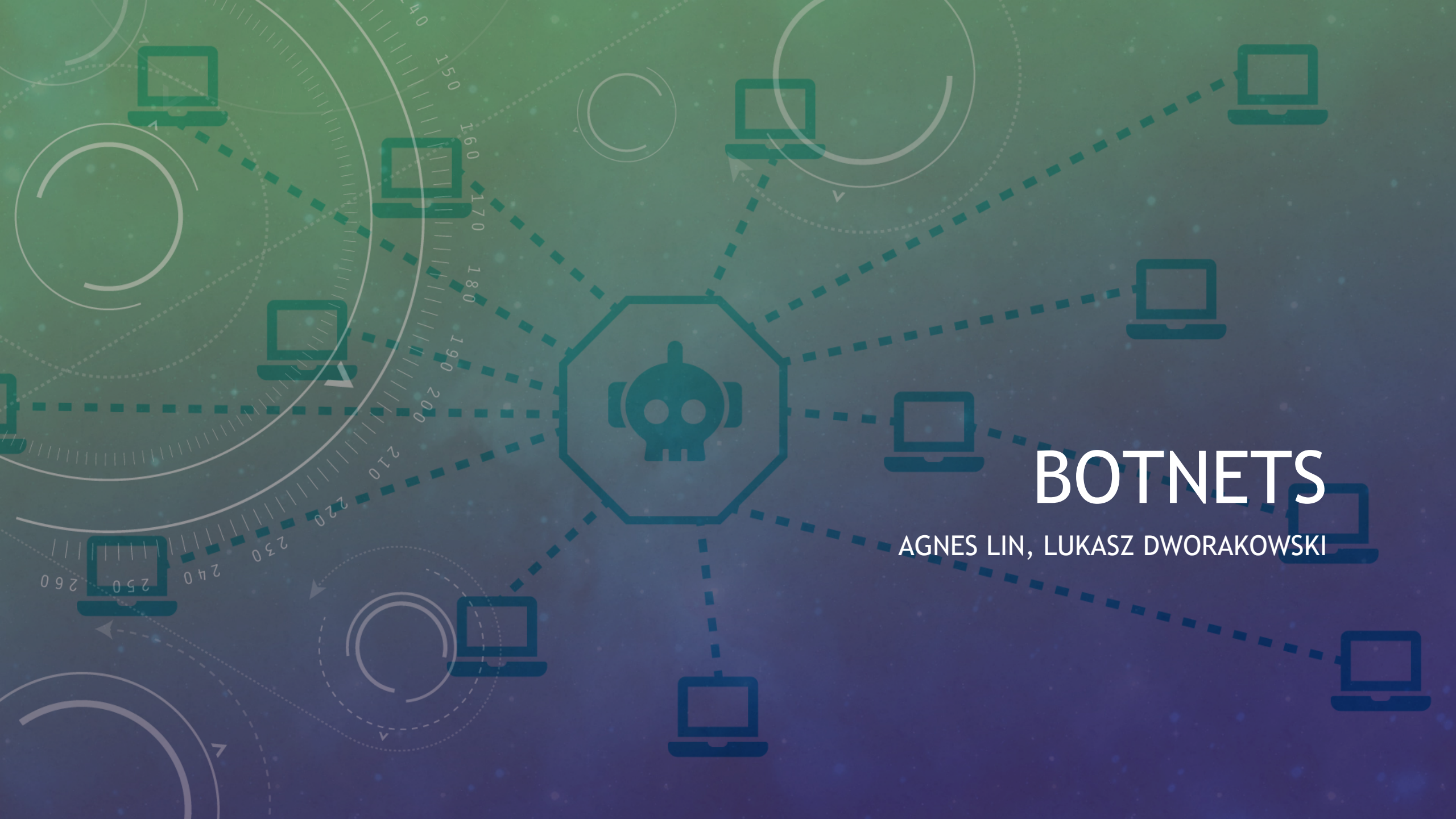


BOTNETS

AGNES LIN, LUKASZ DWORAKOWSKI

SECURITY RISKS

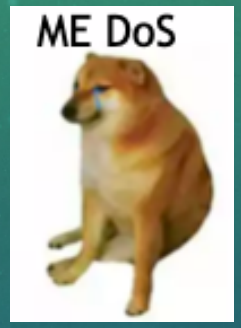
Broken Authentication

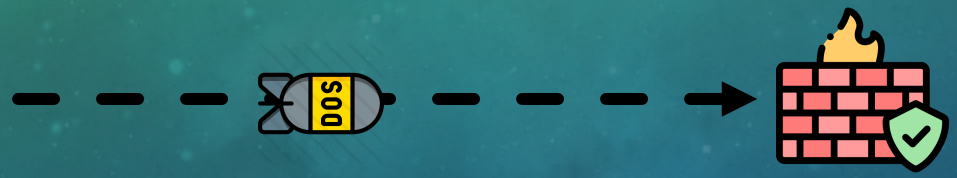
Broken Access Control

XSS

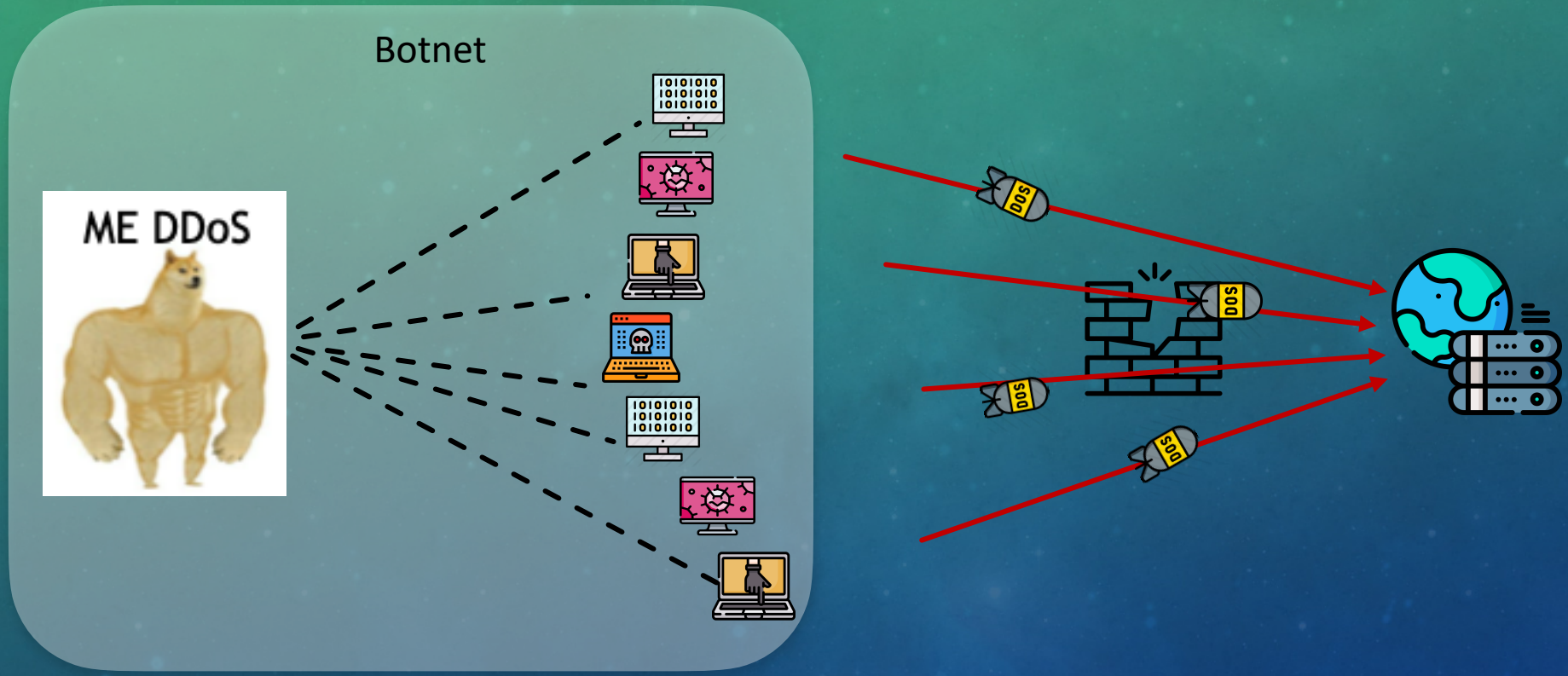
Sensitive Data Exposure

SCENARIO:
DENIAL OF SERVICE..?





SCENARIO: DDOS



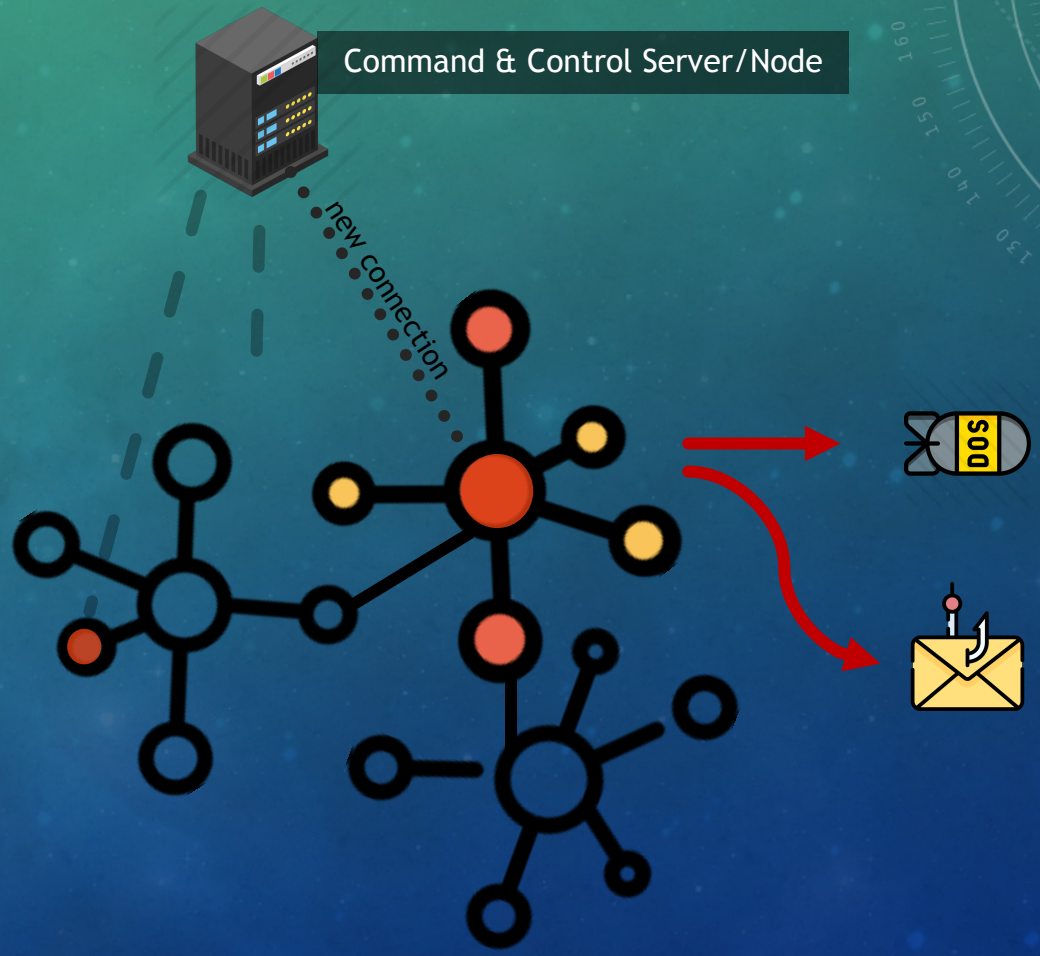
WHAT IS A BOTNET

"A network of computers infected by malware that are under the control of a single attacking party, known as the "bot-herder". Each individual machine under the control of the bot-herder is known as a bot. From one central point, the attacking party can command every computer on its botnet to simultaneously carry out a coordinated criminal action"

-Palo Alto Networks

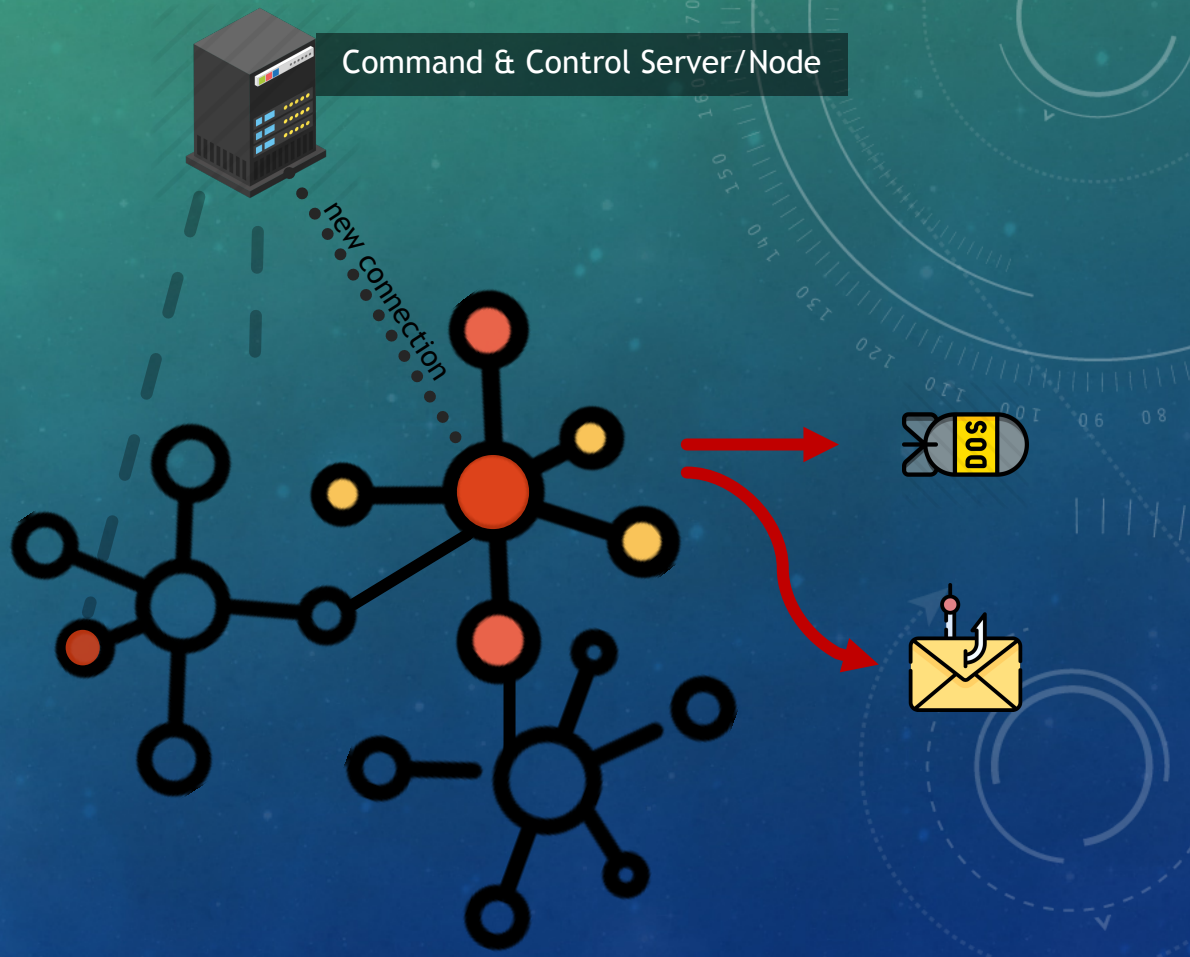
HOW A BOT IS BEING RECRUITED AND ORGANIZED

1. Device is infected
2. Device registers with server and become a part of the botnet
3. … (wait for command)
4. Profit???



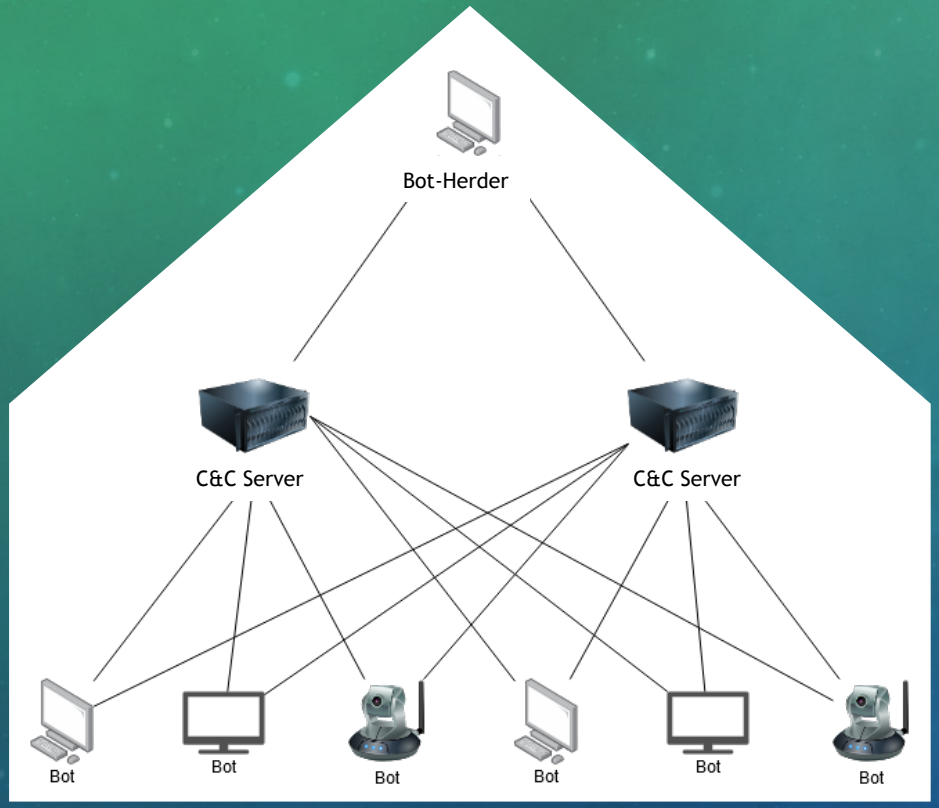
BOTNET LIFECYCLE

1. Initial Infection
   - Search for vulnerable machines
2. Secondary Injection
   - Installation of the actual bot and persistence
3. Connection
   - Bot connects with the C&C server or P2P network
4. Malicious Command and Control
   - Bot-master broadcasts commands to initiate activity
5. Maintenance of Bots
   - Keep bots alive and updated

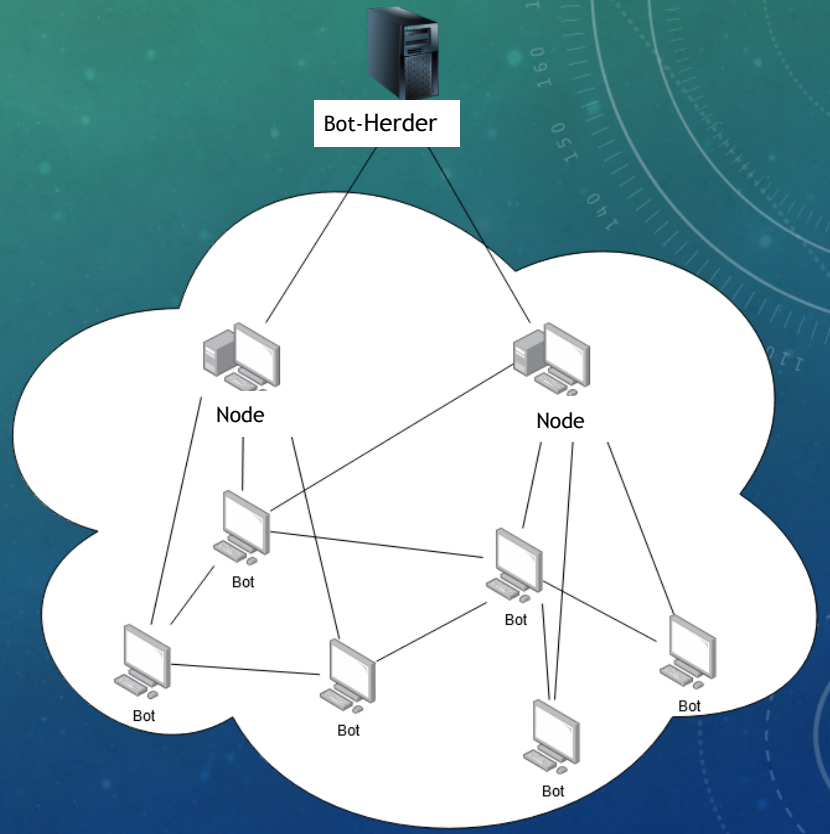


BOTNET STRUCTURES

Command and Control Server

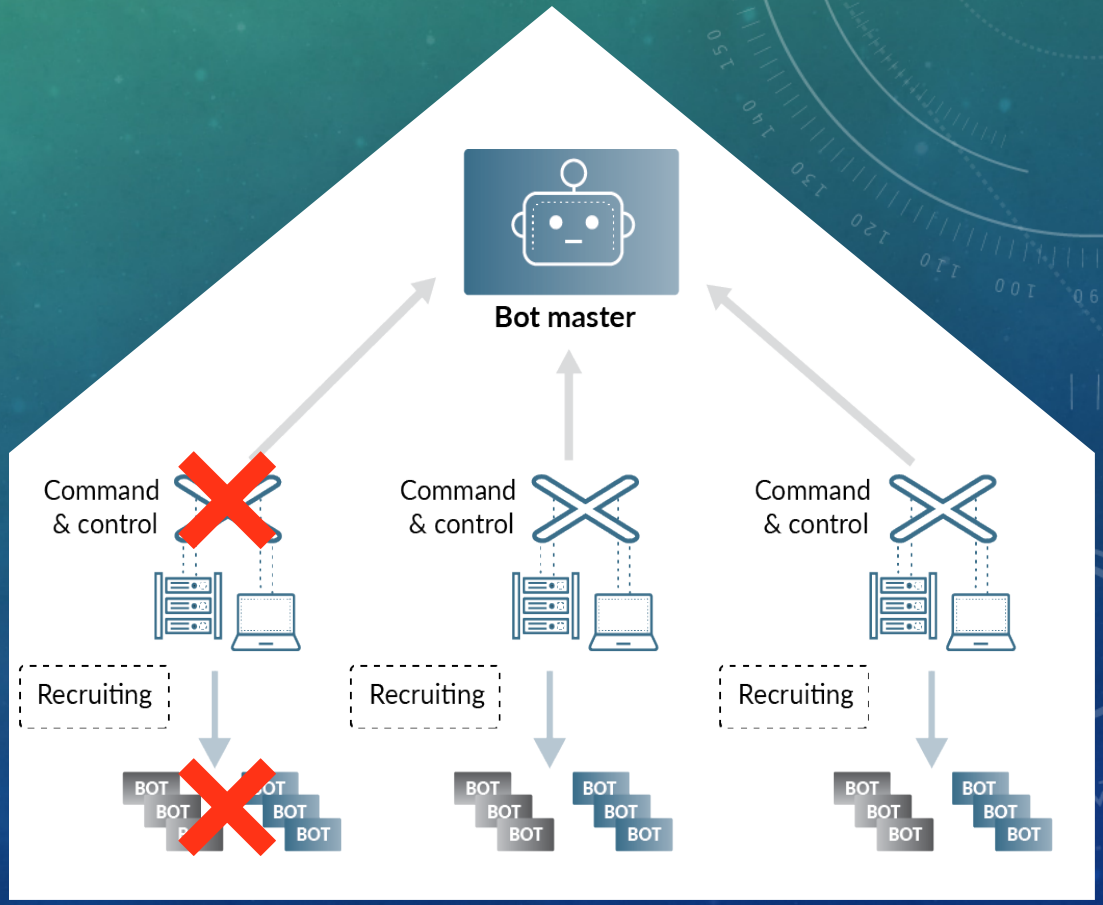


Peer to Peer

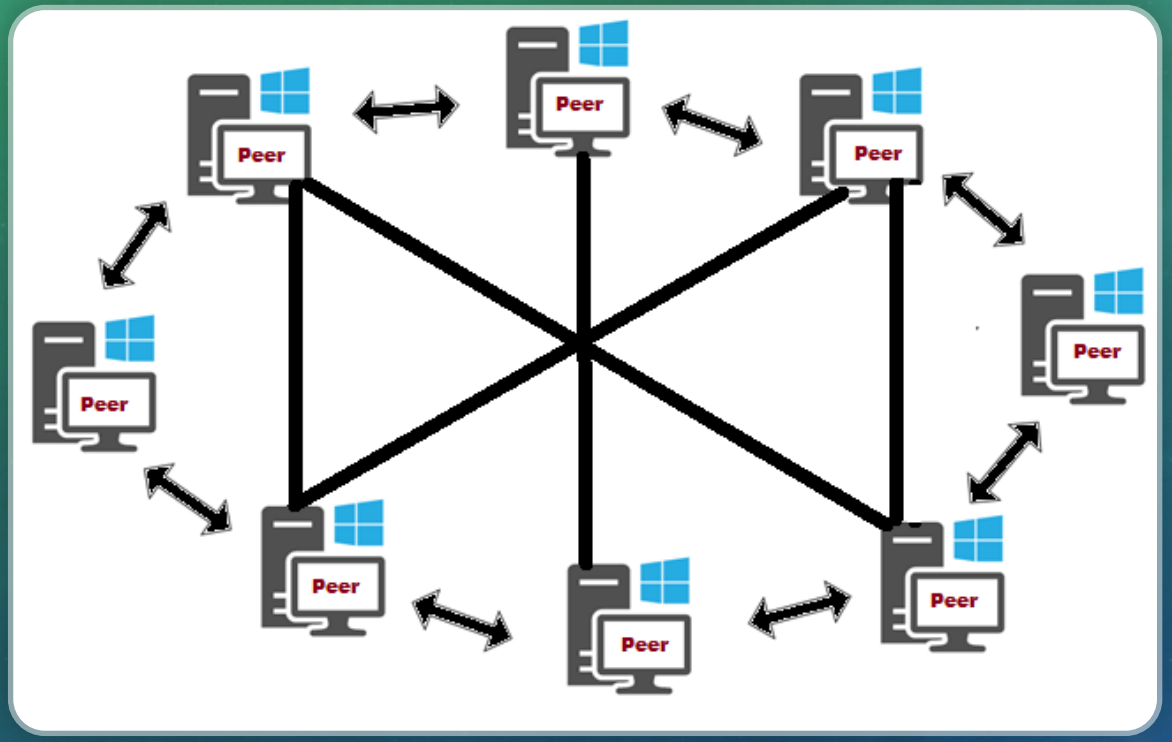


COMMAND AND CONTROL (C2) STRUCTURE

- All bots connect to one or more command and control servers
  - The IP address of the server the bot should connect to is in the malware
- Fast and direct communication to bots
  - Direct communication as servers and bots are connected directly
  - Usually used communication protocols: IRC, HTTP, TOR
- If a C2 server is being moved, bots that connect to it are gone
  - The centralized structure means the servers and the master can be located and taken down



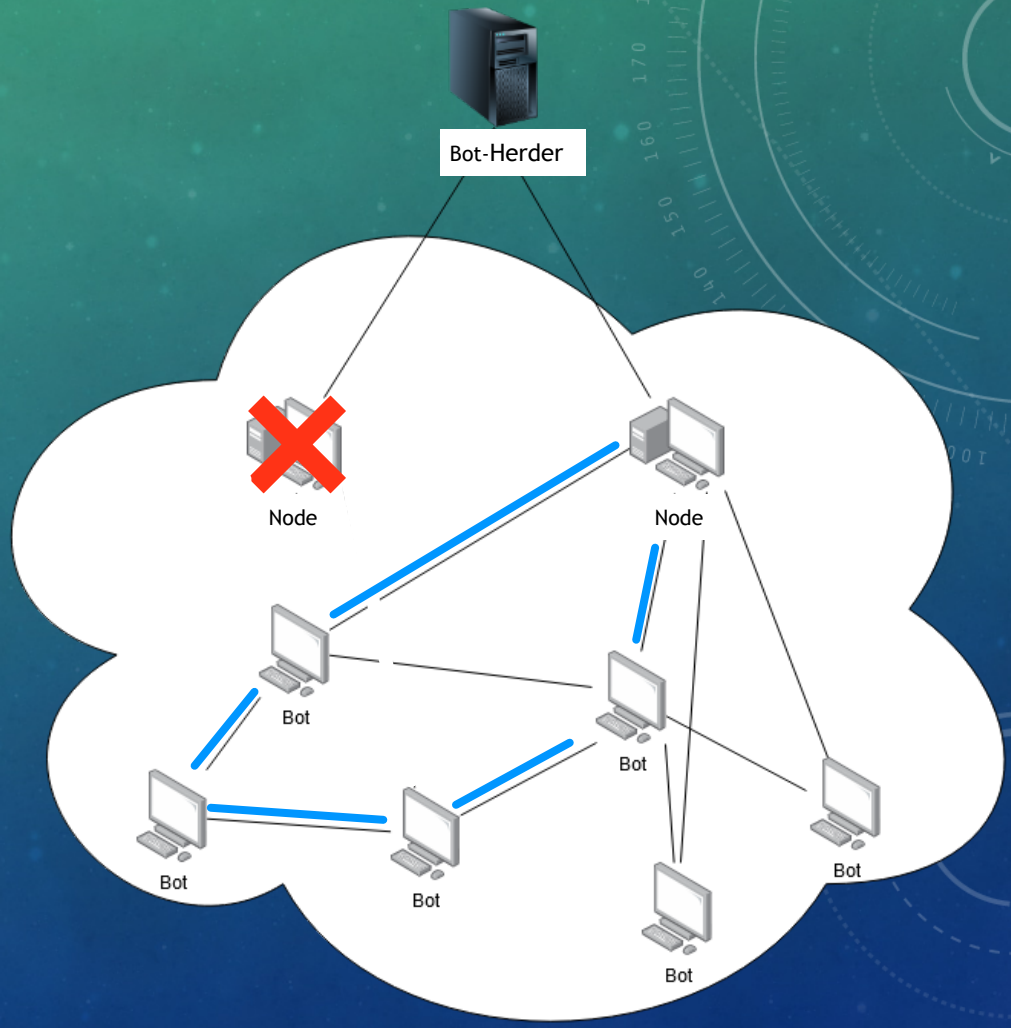
PEER TO PEER NETWORK (P2P) – THE ABSOLUTE BASICS



- Decentralized
- Partitions tasks or workloads between peers
- Peers make a portion of their resources, like CPU or storage, directly available to other network participants, without central coordination
- Requests are propagated through the network until it is fulfilled, or the request dies
- Peers are both suppliers and consumers of resources
  - In purely decentralized architectures, each peer behaves exactly the same
  - This means they are both a client and a server on the network

P2P BOTNET STRUCTURE

- Joining to P2P network
  - Connects to a list of pre-defined peers (bootstrapping)
    - Vulnerability: If the list is obtained by defenders, those peers could be shut down, and the bot would then be isolated
  - Connects to existing peers (dynamic)
    - When a bot A infects a host B, A passes its own peer list to this newly infected host B
- Newer botnets have partially decentralized (hybrid decentralized) structure with some bots promoted as Super peer, or called Node.
  - More scalable
  - Less traffic
  - Communication efficiency
- If a node is removed…
  - Can connect to other peer, which may connect to anther node, so it can stay in the network
  - Or the Herder could promote a new node



P2P BOTNET STRUCTURE (CONT)

- Command propagation methods using P2P protocols such as:
  - Pull mechanism
    - Generate a file with a pre-determined name
    - Bots request for the file or check for new commands on the P2P network periodically
    - Active propagation from the perspective of bots that request for commands or files
  - Push mechanism
    - Bots wait for commands to come then they will forward commands to other bots
    - Harder to detect since no periodic requests are sent
    - Passive propagation from the perspective of bots that wait for files or commands
- No central command structure means commands are typically encrypted when deployed

P2P VS C&C

	C2	P2P
Servers	Clients and servers are distinct devices	Clients and servers are the same
Speed	Direct message to client	Data will propagate to all nodes eventually
Resilience	Take down a server, and those bots are gone	Take down a node, and its connections are likely still in the network

WHY WOULD SOMEONE DEPLOY ONE

- Highly distributed infrastructure of devices
- Self-propagating data collection
- What attacks can a botnet do?
  - Denial of service attacks - Mirai, C2, 600,000 infected
  - Ad fraud through fake websites - 3ve, C2, infected 1,000,000+ infected
  - Email spam - Necurs, P2P, Infected 9,000,000+ infected
  - Brute force website logins - GoldBrute, C2, 1,500,000+ infected
  - Crypto mining - Fritzfrog, P2P, breached 500+ infected
- Their own profit

HOW DOES IT GET INTO THE WILD

- Unpatched or poorly made software
  - Public facing computers with open ports
  - Scan those ports for known vulnerabilities
    - May remember from 347 last semester we did this!
    - https://www.cvedetails.com/vulnerability-list/
  - Devices using default passwords
    - Check out shodan to see a scary site!
- Malicious software
  - Trojans
  - Modified programs

ANALYZING REAL WORLD BOTNET

- Mirai
- 3ve
- MethBot
- GoldBrute
- MegaD

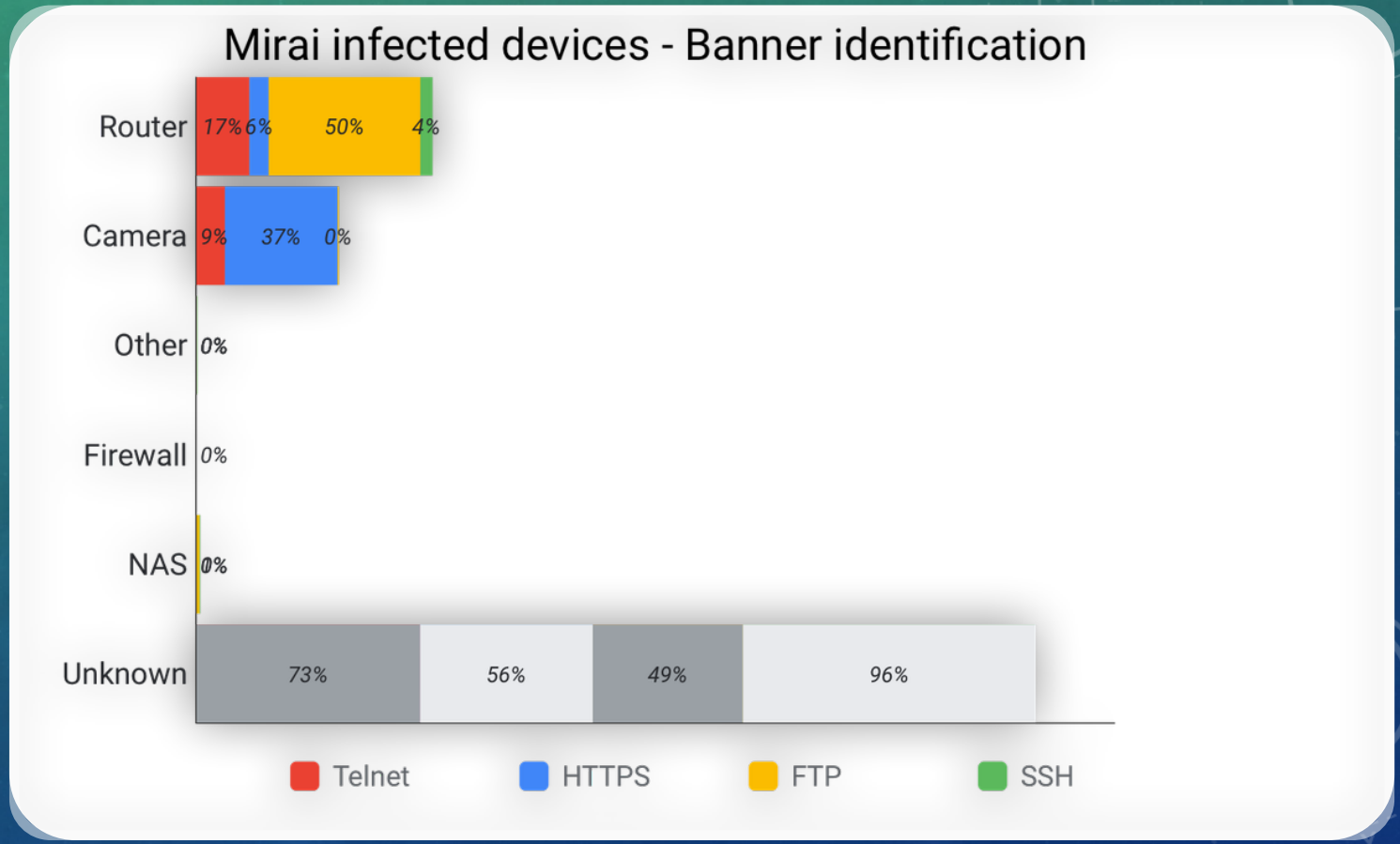
C2 Botnets

- Fritzfrog
- Necurs
- StormWorm
- Gnutella
- DDG

P2P Botnets

BOTNET ANALYSIS – MIRAI (INTRO)

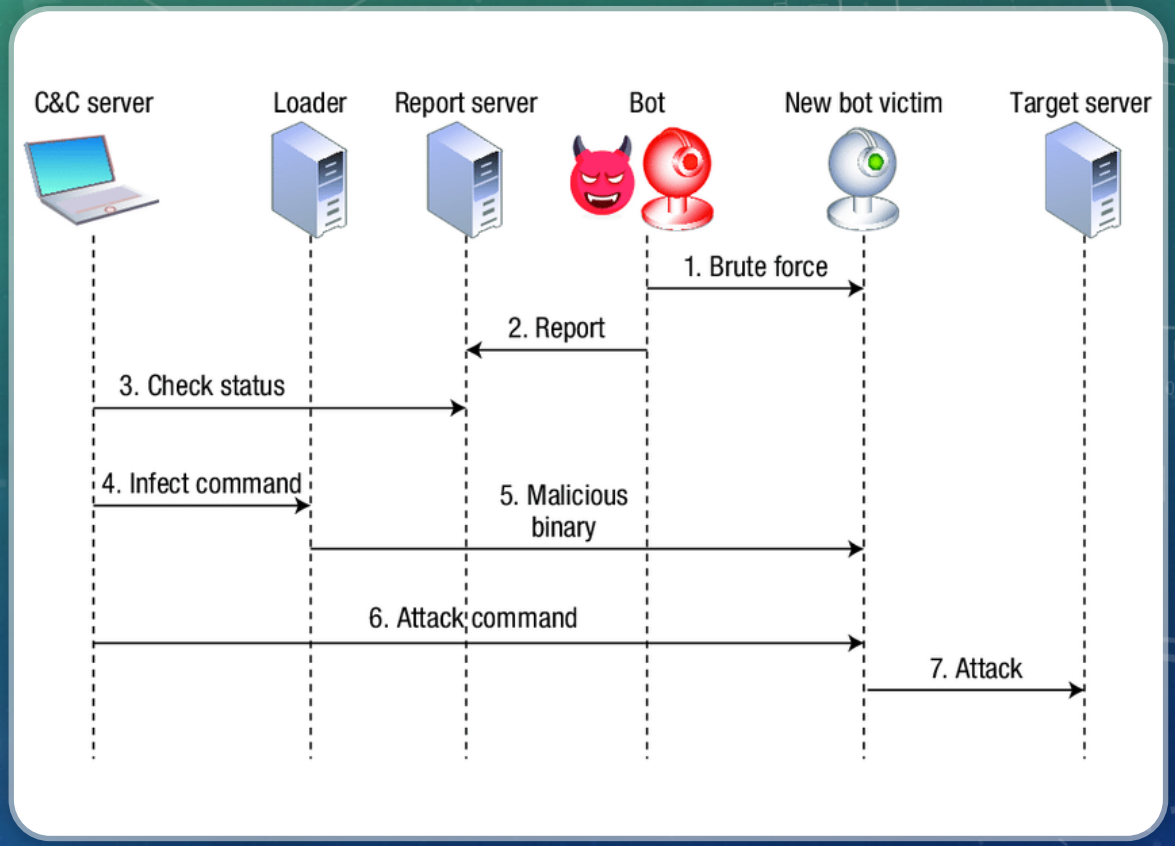
- A specific piece of malware designed for IOT devices
- Responsible for attacks against:
  - Krebs on Security
  - OVH
- Scans the internet for vulnerable IOT devices
- Infected over 600,000 devices
- It is self-propagating
- Used centralized C&C Servers



BOTNET ANALYSIS – MIRAI (BROKEN DOWN)

- Bot
  - Malware that infects the device
  - Propagate the infection
  - Attack targets
- Command and Control server
  - Centralized management interface
- Loader
  - Facilitates dissementation of executables
- Report server
  - Database with details about all bots in the network

BOTNET ANALYSIS – MIRAI (STEPS)

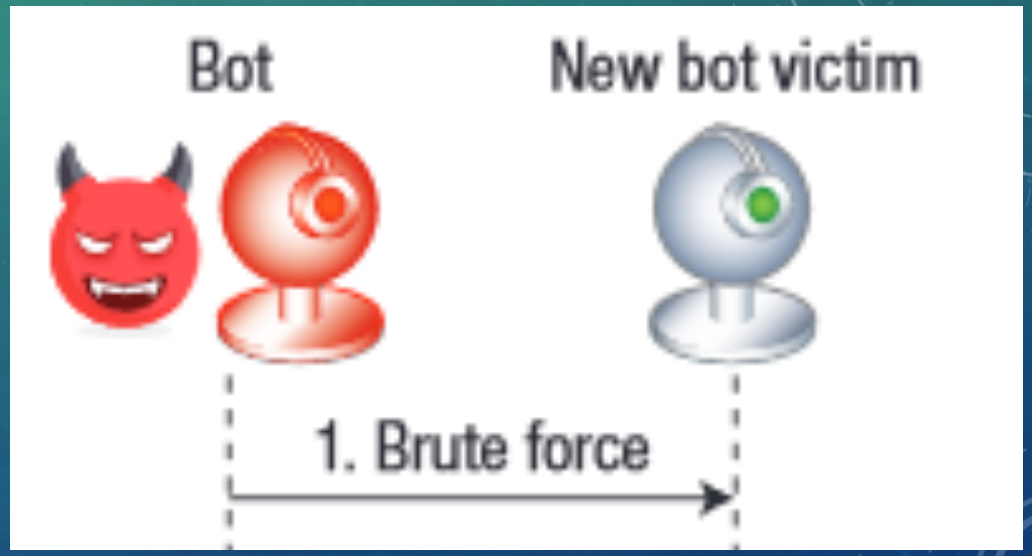


MIRAI STEP 0

- Scans random IP addresses
- Specifically targets:
  - TCP/23
  - TCP/2323
- Deliberatly avoids some IP addresses
  - USPS
  - US DOD
  - GE
  - HP
  - ...

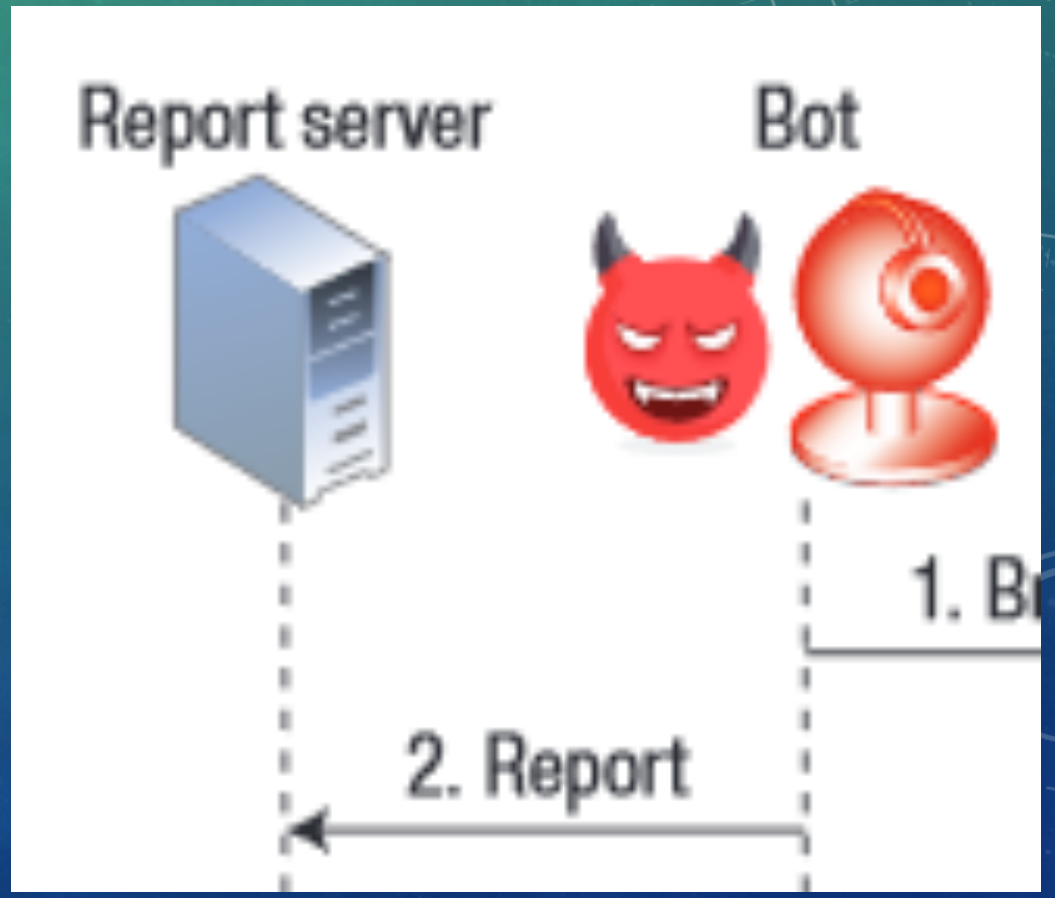
MIRAI STEP 1 - PROPAGATION

- Engages in a brute force attack
- Uses a list of hard coded credentials
  - admin/admin
  - admin/password
  - support/support
  - …
  - mother/fu**er
- https://github.com/danielmiessler/SecLists/blob/master/Passwords/Malware/mirai-botnet.txt



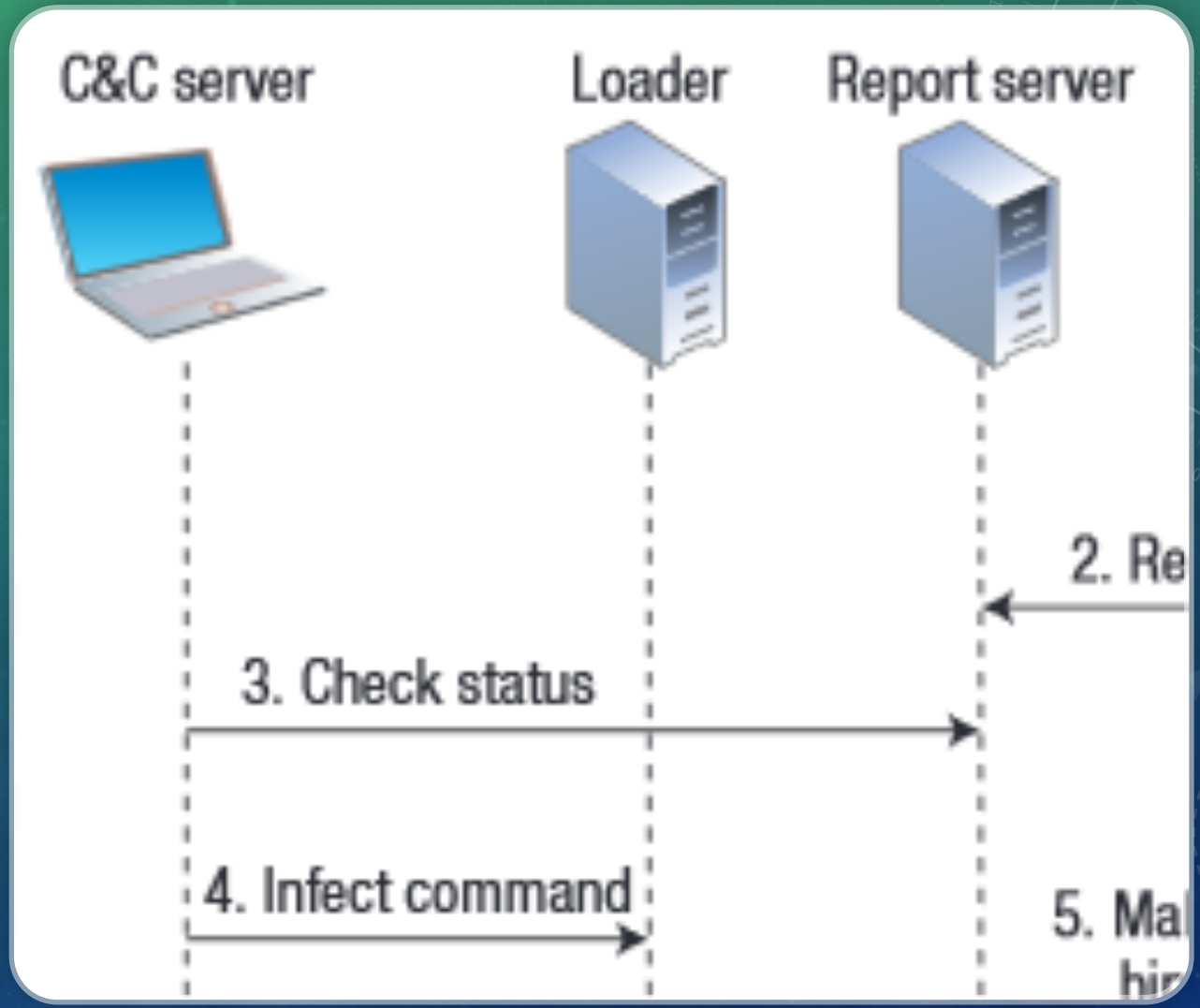
MIRAI STEP 2 – VULNERABLE DEVICE FOUND

- Upon gaining a shell the bot will report the findings



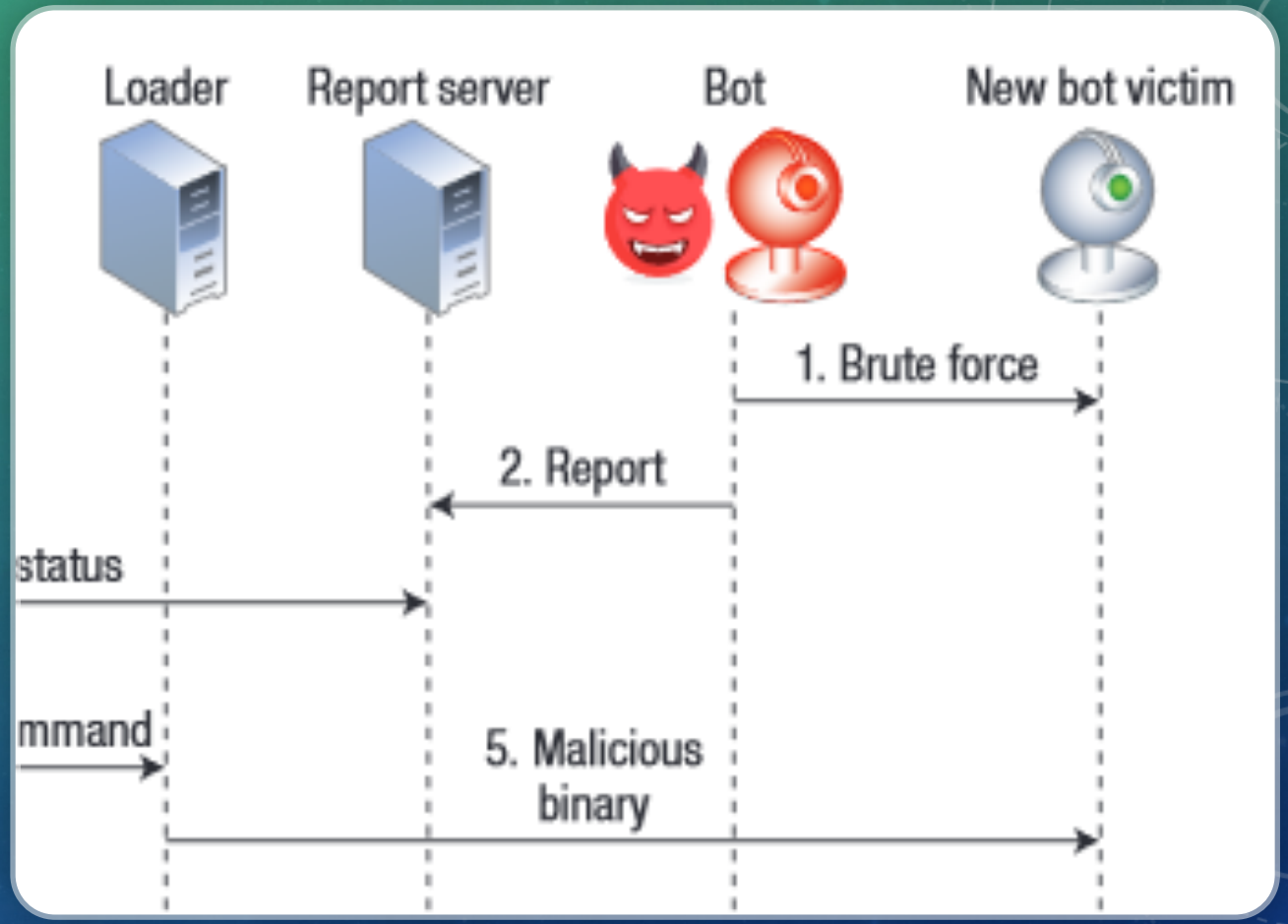
MIRAI STEP 3 & 4 – BOTMASTER MONITORING & ACTION

- Via the C&C server the botmaster will:
  - Check new target victims
  - Botnet's current status via the report server
- Communication done through TOR
- Decide which devices to infect
- Tells loader to infect a device



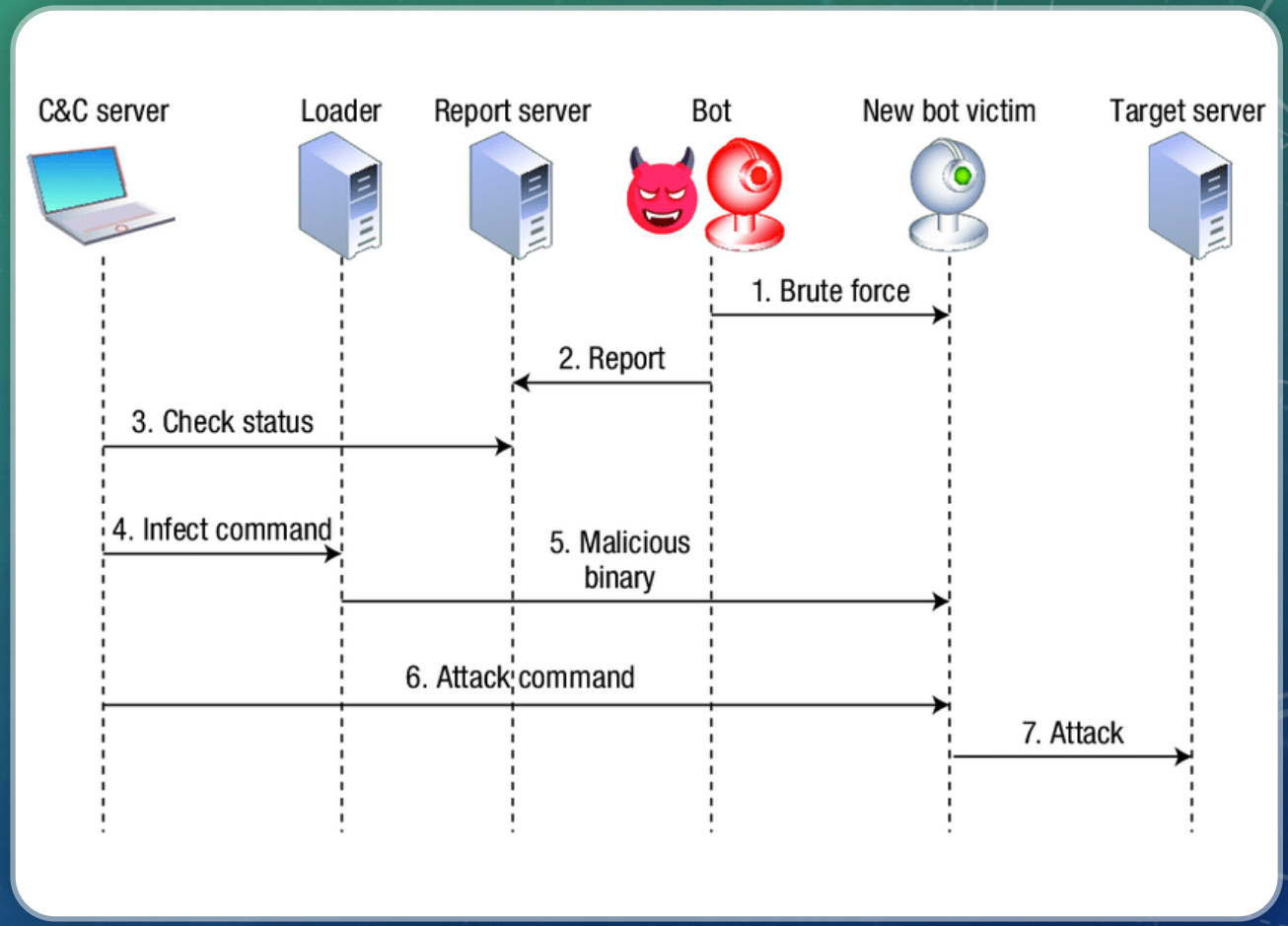
MIRAI STEP 5 - INFECTION

- Loader machine logs into target device
- Instructs device to download and execute specific binary for the device
  - Done through wget or ftp
- As soon as the malware is executed:
  - Block Telnet
  - Block SSH
  - Kills other infections
- Now communicates back to C&C to receive commands
  - Hardcoded domain in the binary
  - cnc.changeme.com



MIRAI STEP 6 & 7 - ACTION

- Botmaster instructs bots to attack a target via the C&C server
- The bots attack the target via some protocol:
  - Generic Routing Encapsulation (GRE)
  - TCP
  - HTTP flooding
  - …



MIRAI FOOTPRINTS

- Almost all stages of infection leave a footprint...
  - Sequential testing of specific credential on specific ports
  - Sending reports that generate distinctive patterns
  - Downloading a specific type of binary
  - Exchanging keep-alive message
  - Receiving commands in a specific structure
  - Very predictable attack traffic

FRITZFROG (2020) INTRO

- First reported this P2P botnet in January 2020 by Guardicore

- Aggressive
  - Actively breaching SSH servers and brute forcing logings
- Hard to detect
  - Fileless
  - Generic executable names: `ifconfig`, `nginx`
  - Communication encrypted with AES, Diffie Hellman key exchange
- Efficient and Up-to-date
  - Novel P2P implementation
  - Well decentralized
  - Exchange databases of targets and breached machines constantly
- Distributed Monero mining

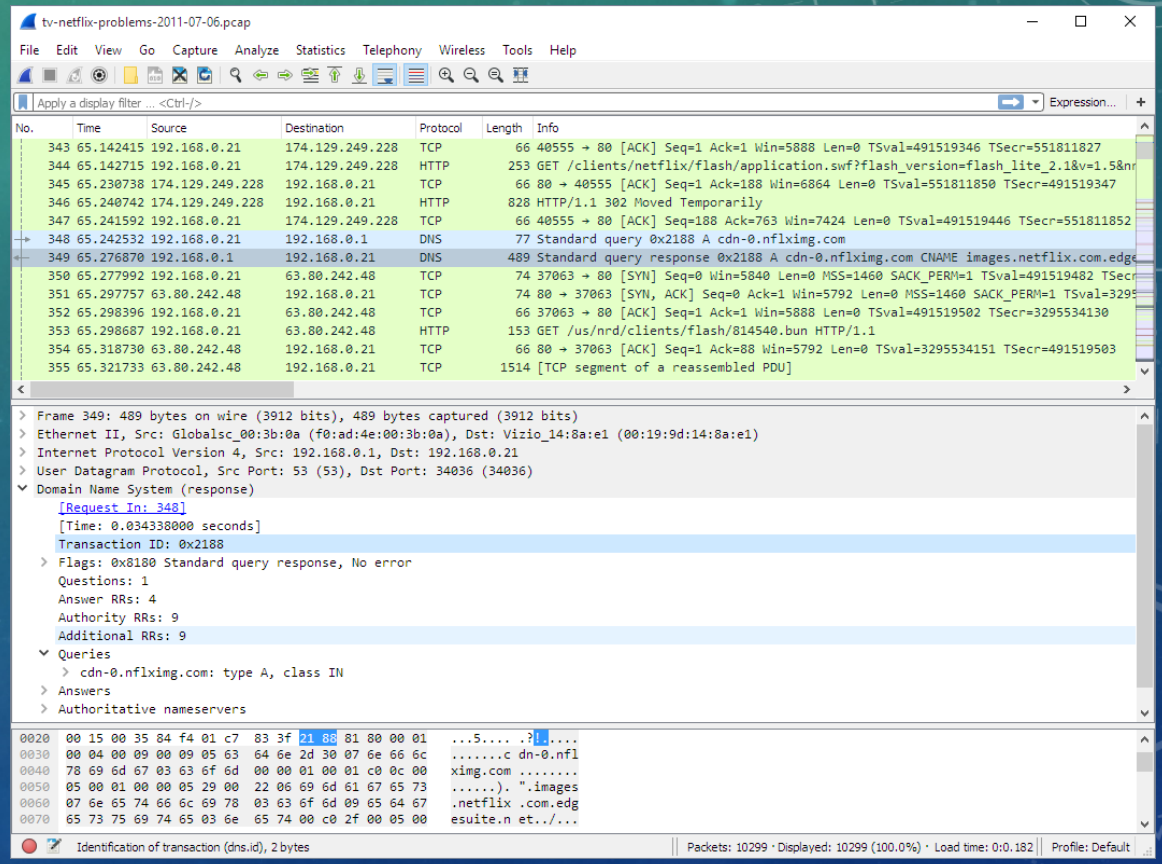
FRITZFROG DETECTION & MITIGATION

- Guardicore script:
  - https://github.com/guardicore/labs_campaigns/blob/master/FritzFrog/detect_fritzfrog.sh
- Fileless processes named:
  - nginx
  - ifconfig
  - libexec
  - php-fpm
- Port 1234 is listening
- SSH Key:
  - ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDJYZIsncBTFc ...
- List of IP addresses:
  - Known to be sources
  - Known machines in the network

- Immediate device quarantine
- Kill any of the fileless processes
- Block all traffic on ports:
  - 1234 (used for P2P communication)
  - 5555 (cryptominer)
- Block all traffic to xmrpool.eu
- Clear SSH keys
- Change passwords

BOTNET DETECTION – POTENTIAL INDICATORS OF COMPROMISE

- Anomaly-based
  - Network-based
    - NetFlow analyzer
  - Host-based
- Signature-based
  - Ntop + Snort
- DNS-based
  - Wireshark + Capinfos
- Mining-based
  - Botminer



WHEN CAN THE GOOD GUYS DO?

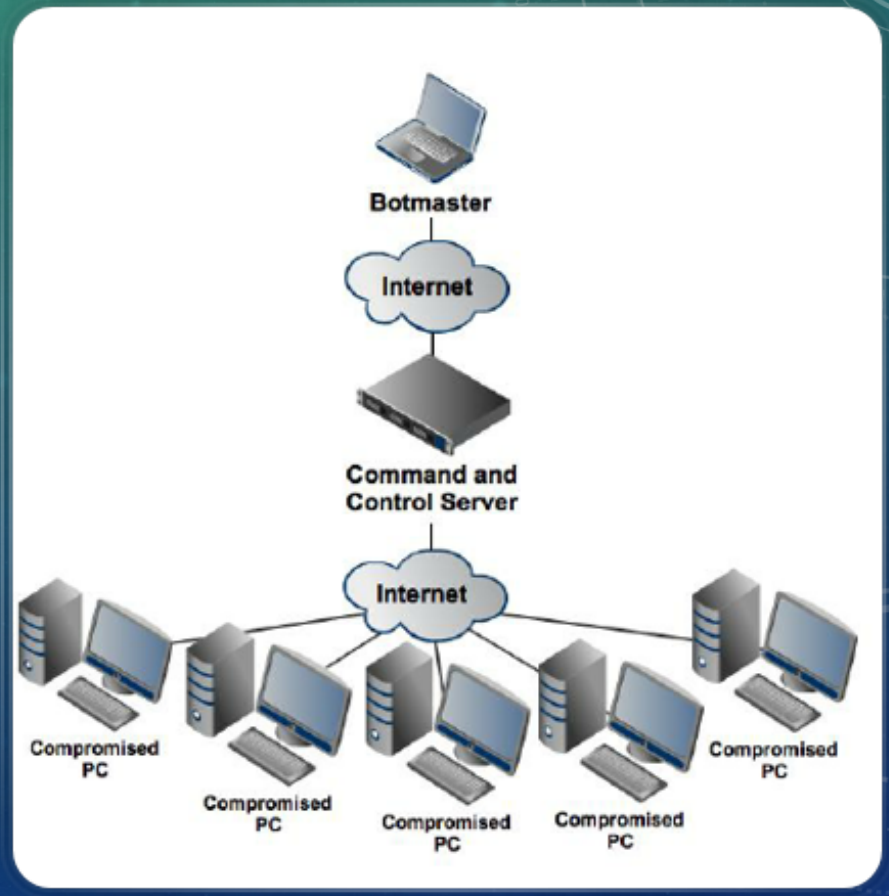
- Index poisoning
- Honey pot
- C&C takedown

INDEX POISONING -P2P

- Originally devised to prevent "illegal distribution of content" in P2P networks
- Insert massive numbers of false records into the index system
    - A peer receives the false record and may not be able to find the resource
- If the offence can introduce enough false records they can "poison" the system by overwhelming the system to retrieve information from nodes they own, or non-existant nodes
- Why does it work?
    - A lack of central coordination for what's real
- Does it always work?
    - No, there's already mitigations – authenticate the record injection

C&C TAKEDOWN

- If we can cut the communication, then the bots are dead
- Using some detection technique, we can find the command and control server
- Multiple methods to shut-down the control
  - Block the IP on the network
  - Take the server down
  - Domain takedowns
  - If you're creative, DDOS the C&C server 😅
- How does it work?
  - If the bots cannot communicate, they cannot perform actions
- Does it always work?
  - No, depending on how the C2 is architected it may be innefective without mass coordination
  - May be multiple C2 servers
  - If domain based, can move the C2 servers around easily

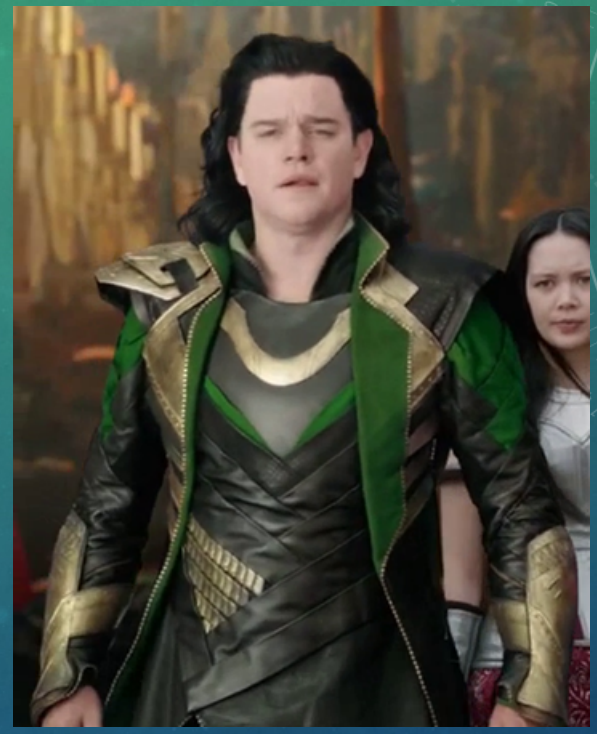


HONEY POTS

- A computer or system intended to mimic likely targets
- Used to detect attacks or deflect them from targets
  - Don't look for attacks, bait them with a target!
- How does it work?
  - Setup a system that looks like a real target
    - Don't run security updates
    - Leave ports open
    - Leave services on
    - Weak passwords
  - Tricks bots into infecting the device

- Once the device is infected:
  - The owner of the system can monitor traffic
  - Track changes on the VM
  - Decompile binaries and see how it works
- Does it always work?
  - No, techniques have been published to detect honeypots and avoid them
    - Honeypot Hunter (2004)

DEMO



- https://github.com/Bitwise-01/Loki
- https://github.com/malwaredllc/byob

byob

SOURCES & SOME INTERESTING READINGS

- IEEE:
  - DDoS in the IoT: Mirai and Other Botnets
  - The Mirai botnet and the IoT Zombie Armies
  - Analysis of Mirai malicious software
  - On Security Threats of Botnets to Cyber Systems
  - Botnet and P2P Botnet Detection Strategies: A Review
- University of Central Florida:
  - Peer-to-Peer Botnets
  - http://www.eecs.ucf.edu/~czou/research/P2PBotnets-bookChapter.pdf
- Mirai source code:
  - https://github.com/jgamblin/Mirai-Source-Code
- https://www.paloaltonetworks.com/cyberpedia/what-is-botnet
- https://www.crowdstrike.com/epp-101/botnets/
- https://www.kaspersky.com/resource-center/threats/botnet-attacks
- Usenix:
  - Understanding the Mirai Botnet
- https://www.sentinelone.com/blog/what-is-a-botnet-and-why-are-they-dangerous/
- https://www.securitymagazine.com/articles/93898-tackling-the-challenges-of-detecting-p2p-botnets
- https://www.imperva.com/blog/malware-analysis-mirai-ddos-botnet/
- https://www.f-secure.com/v-descs/articles/botnet.shtml
- Guardicore:
  - https://www.youtube.com/watch?v=RUO9sSZde84
  - https://www.guardicore.com/2020/08/fritzfrog-p2p-botnet-infects-ssh-servers/
  - https://github.com/guardicore/labs_campaigns/tree/master/FritzFrog