Detecting and Disrupting Compromised Devices based on Their Communication Patterns to Legitimate Web Services

Hen Tzaban

Akamai Technologies
Network Security

BotConf 2022

Who Am I

Hen Tzaban

Senior Data Scientist Lead
Akamai Enterprise Security Research
htzaban@akamai.com

Fields of interest: User behavior analysis, Anomaly detection, and Network traffic

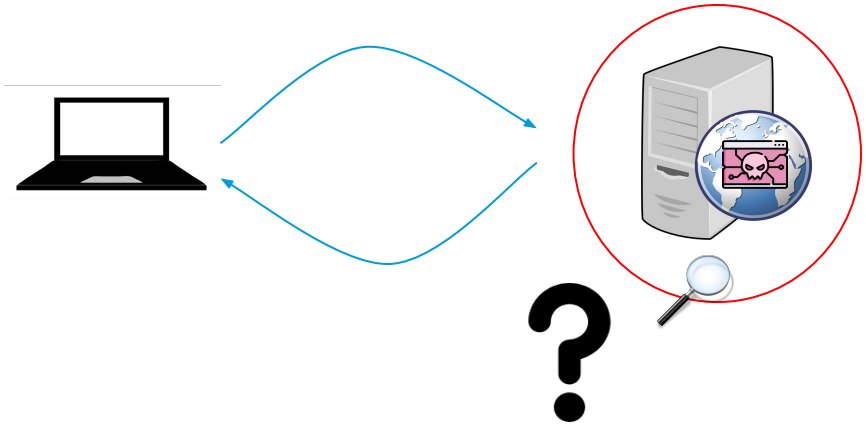
Agenda

- **Introduction**
  - Enterprise protection shift from blacklisting domains to monitoring behavior to detect bots that are compromising the enterprise.
- **Framework Example**
  - Technical background- PSD (Power Spectral Density) and Neural Networks models
  - Presenting framework for detecting infected devices according to their DNS traffic patterns
- **Analysis**
  - Real-world detections
  - Disruption - Enforcement Upon Detection
  - Takeaways

Past - IOC hunting

On Akamai, our products protects more than 400 enterprises worldwide that are concerned with automated bot-ish behavior and unwanted activity.

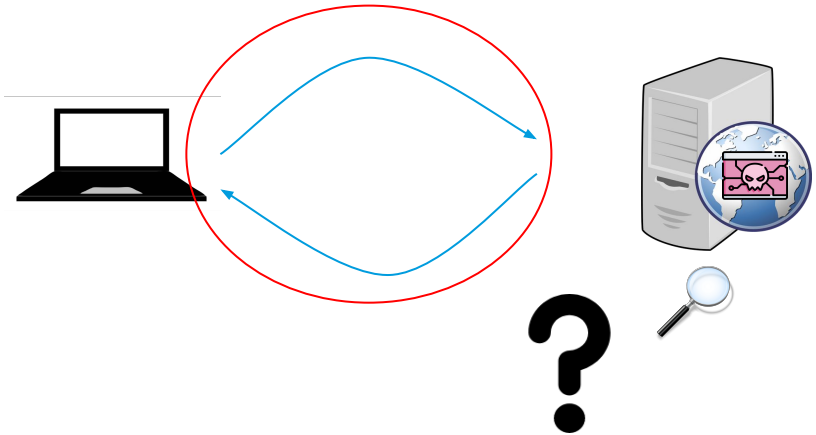
The Goal: Find indication of compromise of a domain/URL in order to increase our DNS/HTTP proxy blocklist



Shift

On Akamai, our products protects more than 400 enterprises worldwide that are concerned with automated bot-ish behavior and unwanted activity.

The Goal: Find indication of compromise of a device/user by tracking devices/users behavior in order to alert suspicious activity



Why is that shift is so important in security?

Some well known APT groups as well as cyber criminals leverage legitimate web services such as GitHub, Twitter, Google Storage and many more, in order to achieve their attack goals and breach an enterprise.

HammerToss*:

- A malware that uses a variety of techniques to commands execution
- It undermines the detection of the malware by adding layers of obfuscation and mimicking the behavior of legitimate devices.
- HAMMERTOSS uses Twitter, GitHub, and cloud storage services to send commands and extract sensitive data from compromised enterprise networks.

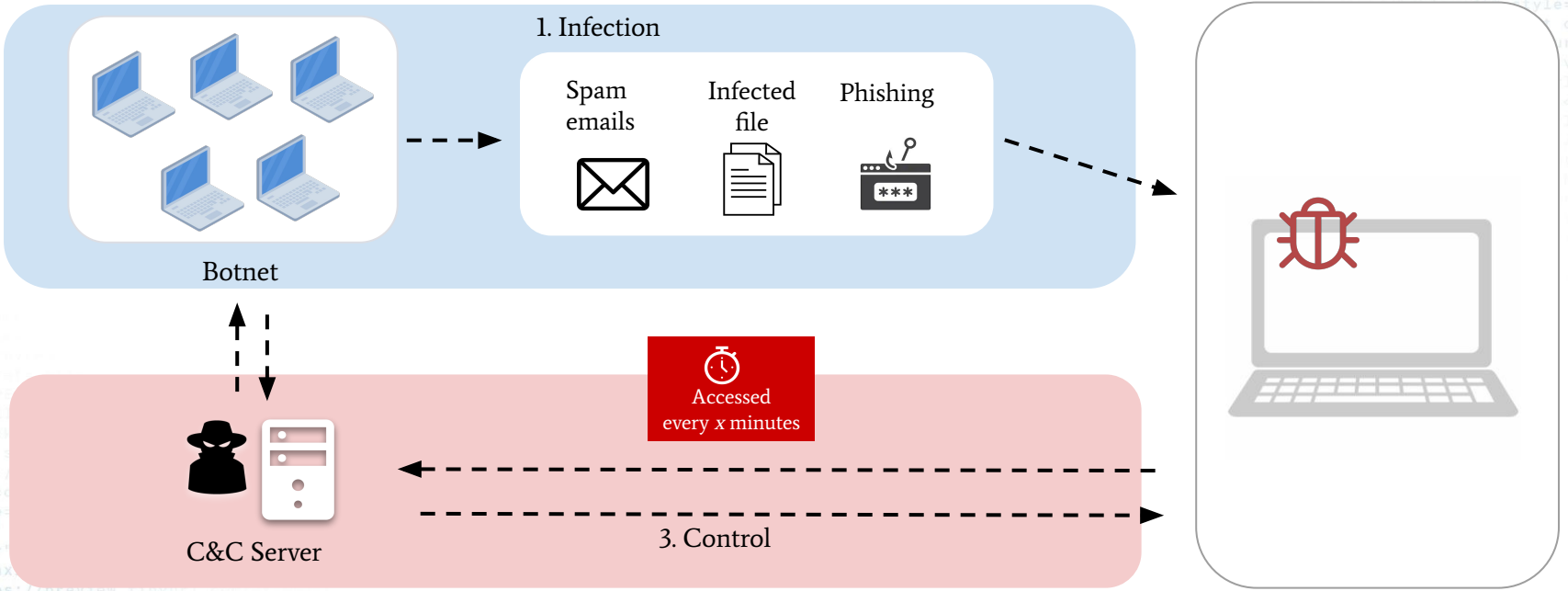
* HAMMERTOSS: Stealthy Tactics Define a Russian Cyber Threat Group, FIREEYE THREAT INTELLIGENCE

Framework Example

- Technical background- PSD (Power Spectral Density) and Neural Networks models
- Presenting framework for detecting infected devices according to their DNS traffic patterns

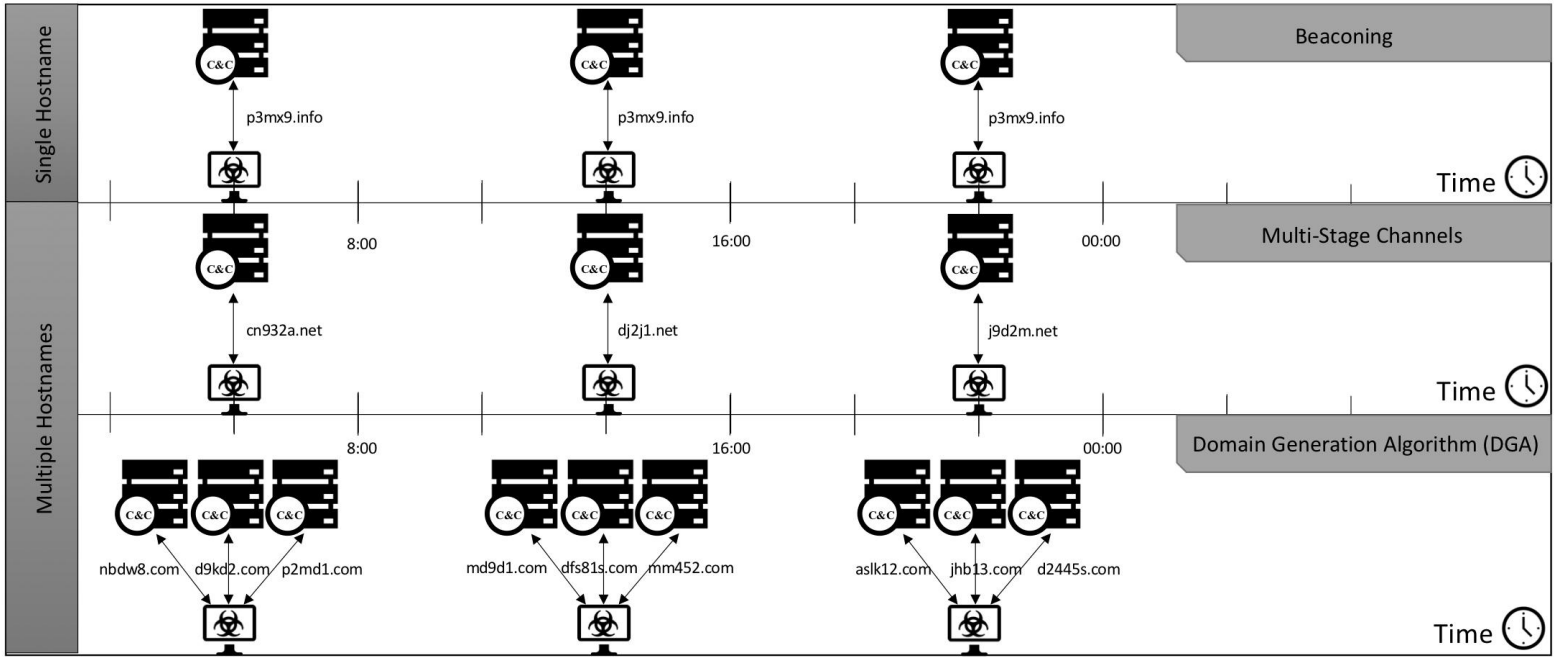
* ‘MORTON: Detection of Malicious Routines in Large-Scale DNS Traffic’, ESORICS’21

Goal: Identify Compromised devices in Enterprise Networks

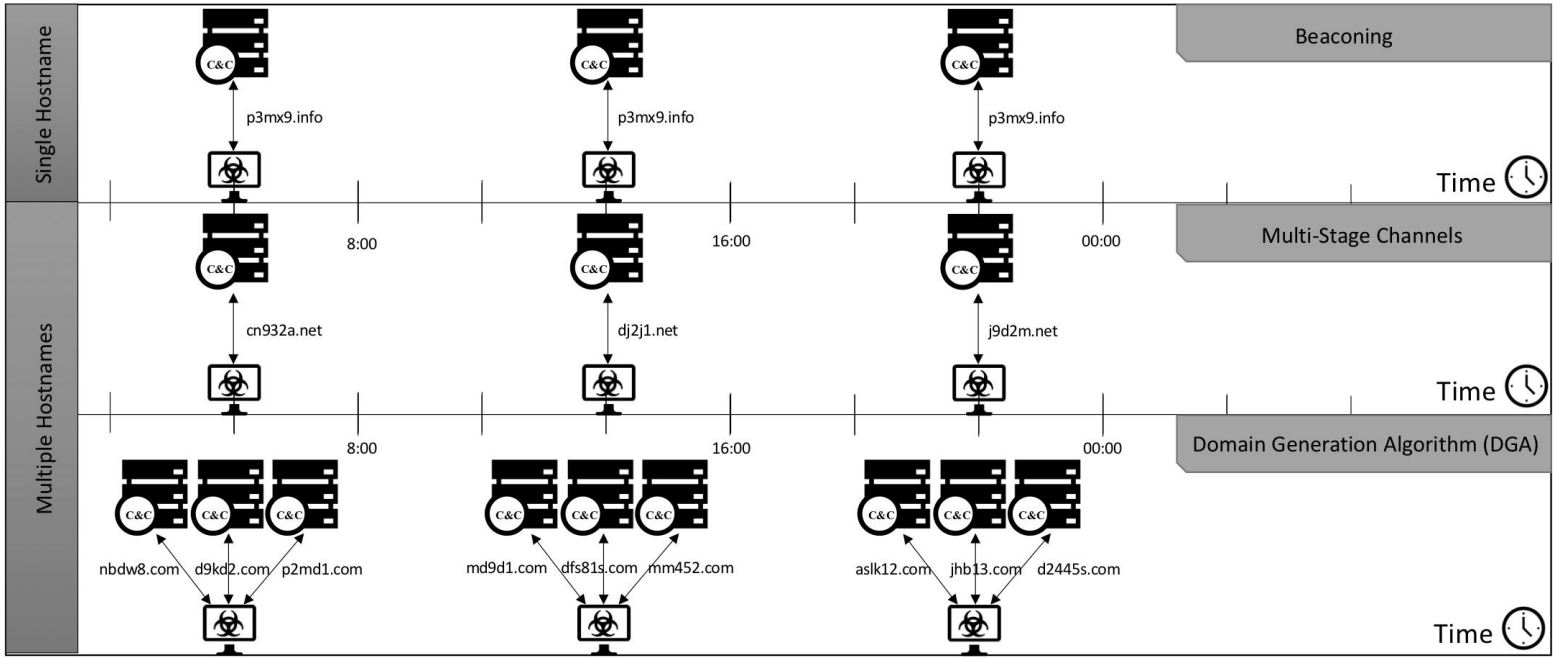


Technique: Detect Devices That Engage In Routine Malicious Bot Communication

Threat Model: Types of Routine Malicious Communication



Threat Model: Types of Routine Malicious Communication



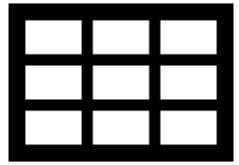
Emotet
Trickbot
…

HammerToss
Zusy
..

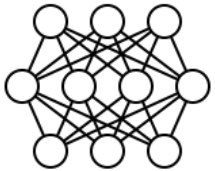
bdsklvd.com
dasfsdvd.com
….

Technical background: PSD + DL

- Represent each enterprise device behavior:
  - Create an informative representation of each enterprise device (embedding) using a PSD (Power Spectral Density)



- Use Neural network for fast and accurate classification
  - Train using simulated bots communication

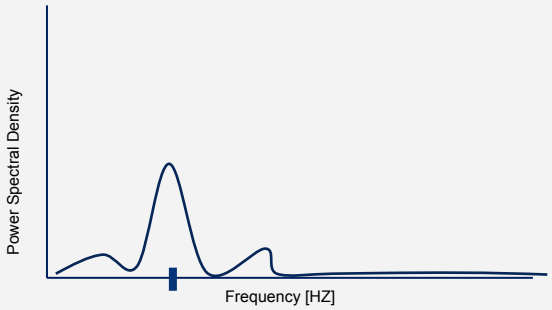


Power Spectral Density (PSD)

- **Power Spectral Density** (PSD) is leveraged from a signal processing field
- Transform from the time domain into the frequency domain
- The higher spectral density of individual frequency is, the more tendency to repeat with this period the time series has.

UserID	Query name	Query timestamp
1234	boot.dev.pubstack.io.	13214564687
1234	boot.dev.pubstack.io.	13214564689
…		

Any network traffic



Signal

$$(f_0, f_1, .., f_N)$$

DFT

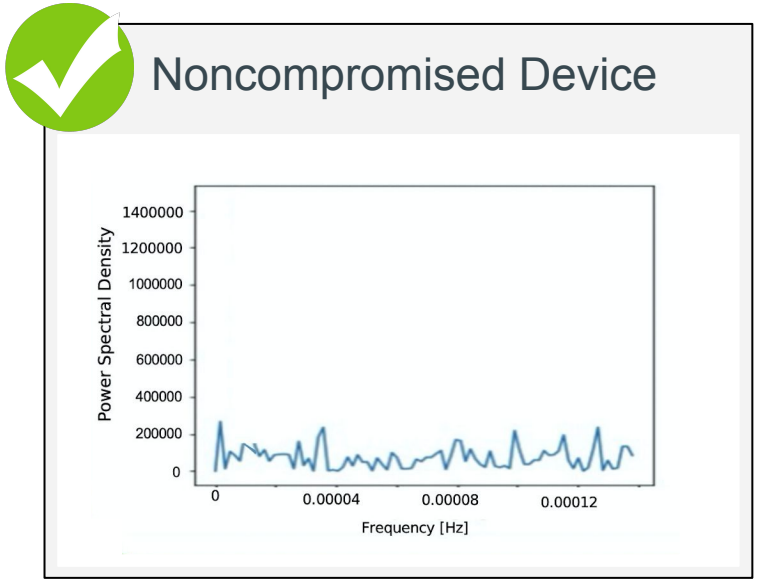
$$DFT(T,k) = \sum_{n=0}^{N-1} t_n e^{-i2\pi \frac{kn}{N}}, k = 0, 1, .., N-1$$

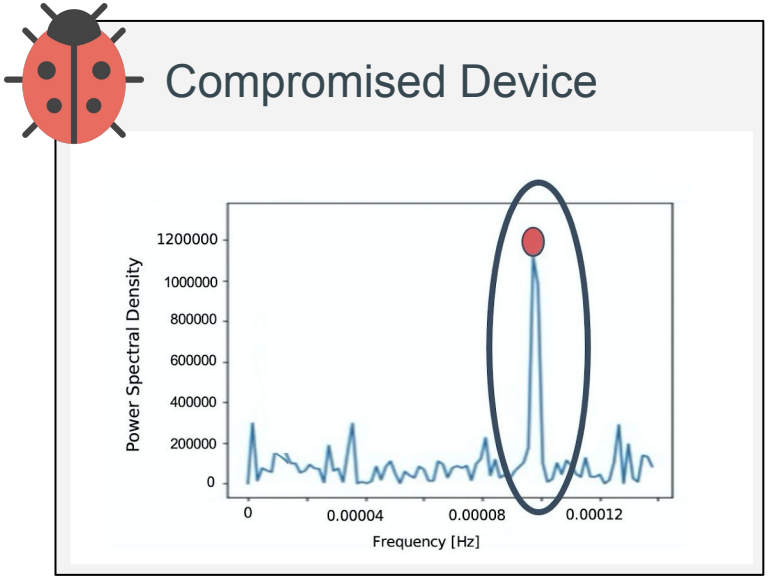
PSD

$$P(f_k) = \|DFT(f_k)\|^2, k = 0, 1, ..., \left\lceil \frac{N-1}{2} \right\rceil$$

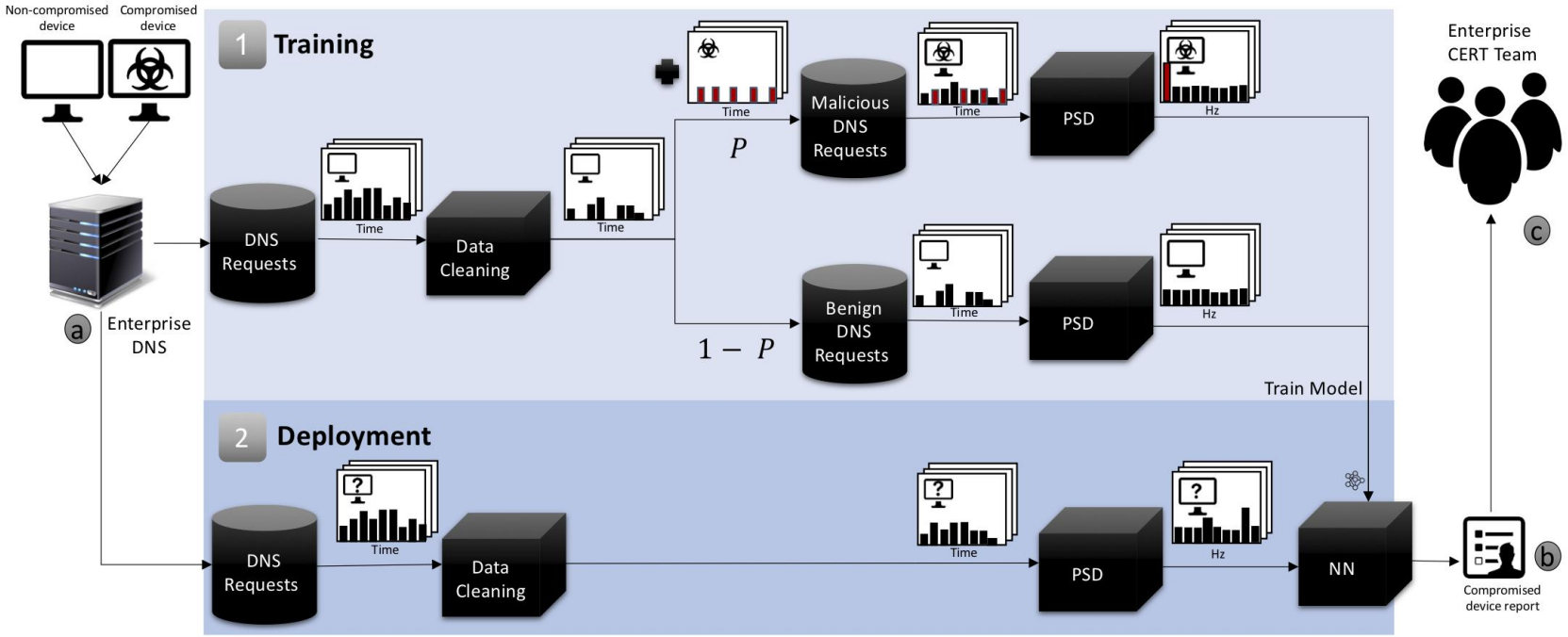
$$PSD(T) = (F_0, F_1, ..., F_{\frac{N-1}{2}-1})$$

Some Intuition regarding PSD





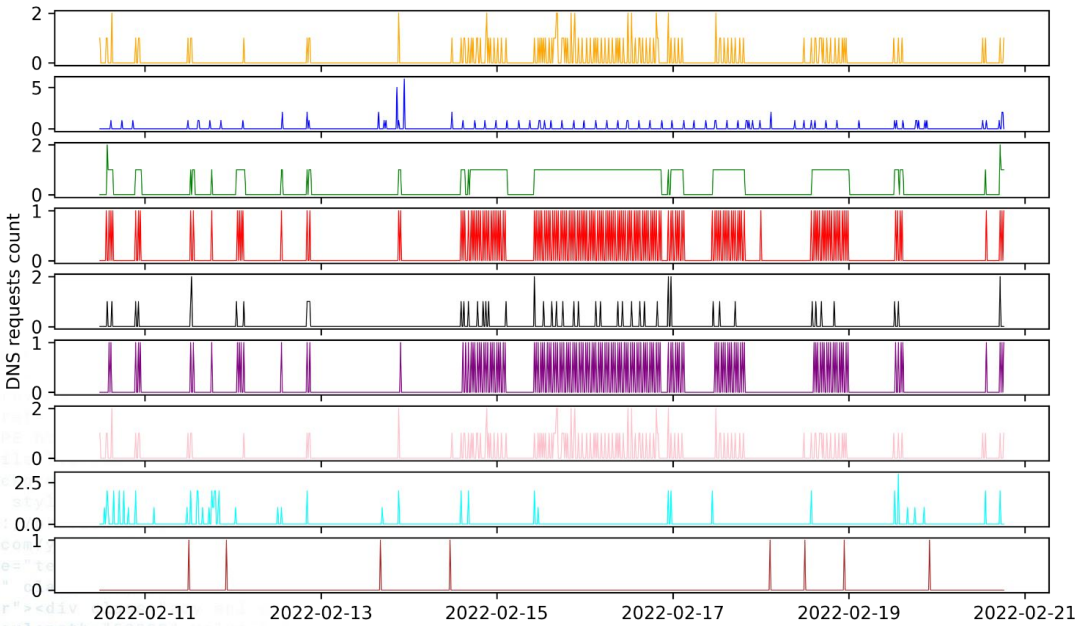
System Overview



Analysis

- Real-world detections in DNS traffic
- Disruption - Enforcement Upon Detection
- Takeaways

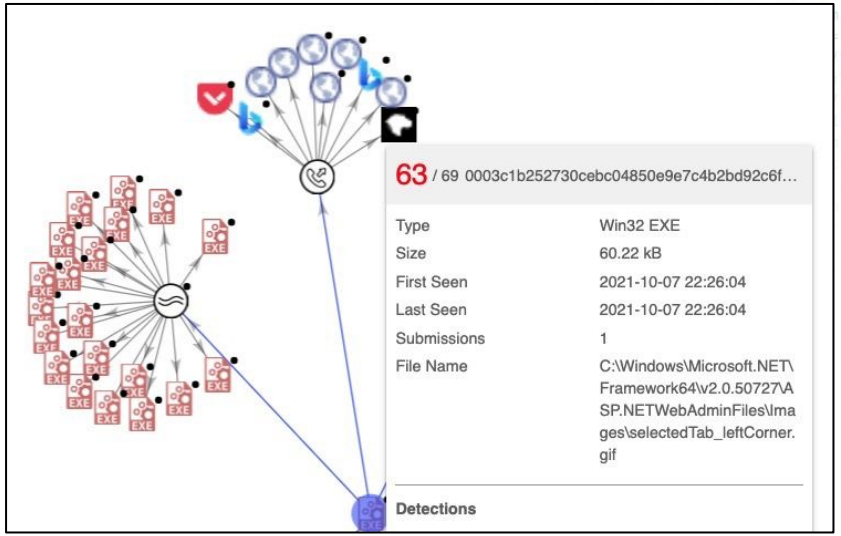
Fsysna Trojan



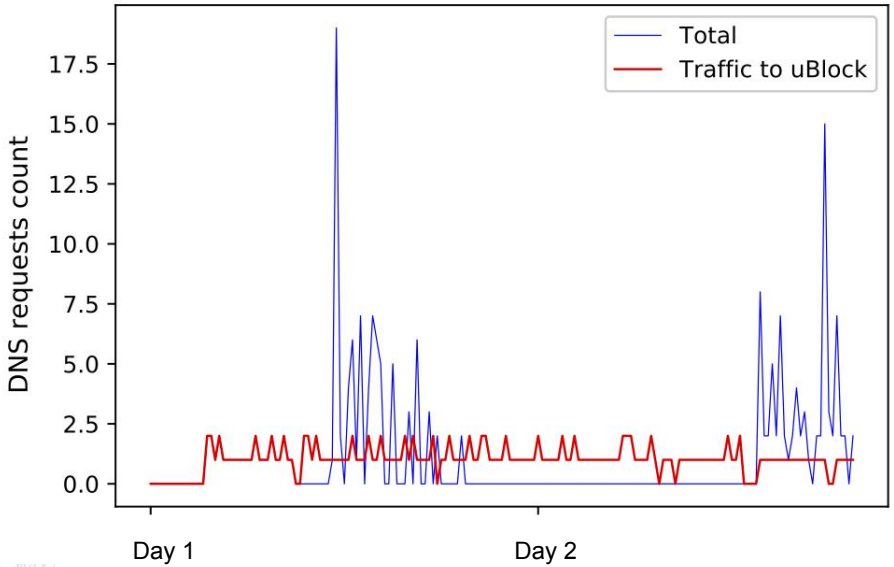
All the accessed domains by the file are legitimate! But the network behavior deviates from the normal patterns

Fsysna Trojan

- First observed in early 2019, Fsysna is an advanced trojan that an attacker remotely controls the victim PC.
- Infection is distributed through small-scale spam campaign
- Maintains a C2 connection to control the payloads and sending sensitive information
- Performs activities without the user's knowledge. For example: capturing keyboard input, collecting system information, downloading/uploading files, dropping other malware into the infected system, performing denial-of-service (DoS) attacks, and running/terminating processes.



uBlock: Malicious add-on



- Malicious add-on for the Chrome browser that is disguised as an ad blocker
- It's code that was cloned to mimic a legitimate ad blocker
- Includes a malicious backdoor for cookie stuffing which is a technique used to commit ad fraud.
- Sends a heartbeat (beacon) to its servers periodically

Enforcement Upon Detection

Monitoring:

1. Monitor the entire activity of the user.
2. Monitor all the relevant sessions.

Security check:

3. Trust pending on security check - Trigger an AV check before allowing further access to any enterprise service

Blocking:

4. Revoke trust for specific apps - Prevent a user from accessing sensitive applications (e.g., financial applications)
5. Block all the relevant sessions.
6. Block the entire activity of the user.

Takeaways

- We have shown use cases this system detected that no blocklist or signature match was able to detect. Therefore, If you want to defend against sophisticated attacks, as a network defender, don’t only use block lists and signatures and start doing behavior based defense systems (and don’t leave it to the SOC to handle!)
- Building a personal optimized system leveraging your massive network logs, with specific use-cases to look for, is beneficial to protect from insider attacks.
- Maintain an holistic approach to view both internal and external web services as suspicious; it doesn’t matter who is hosting it, if your enterprise uses it, it could be a part of a data breach attack!