CSCI 466: Networks

Network Forensics

Reese Pearsall

Fall 2024

Announcements

PA 4 Posted
- Due 11/24

Wireshark Lab 4 Posted
- Due 11/20

- No Class on Monday (Veterans Day)

PA4

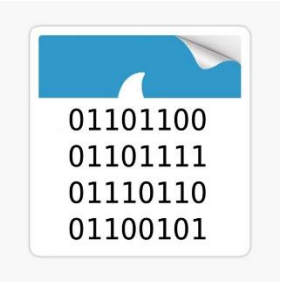
Network Forensics is a branch of Digital Forensics

Digital Forensics – Collection, analysis and interpretation of digital evidence.

- Can help support or refute a theory of how an offense occurred or that address critical elements of the offense such as intent or an alibi
- Digital Evidence plays a crucial part in many modern-day investigations

Network Forensics = digital evidence is coming from traffic of a computer network

Digital Evidence can be collected through combinations of software or hardware tools



You will usually be working with PCAP files

Goals of Network Forensics

Answer important questions such as:

- When did the incident happen? What is the timeline?
- What is the root cause of the incident?
- Who attacked us?
- Why did they attack us?
- What is the scope of the damage?

Reflection

- Did staff and organizations perform as expected?
- What will our organization do next time?
- What corrective actions need to happen?

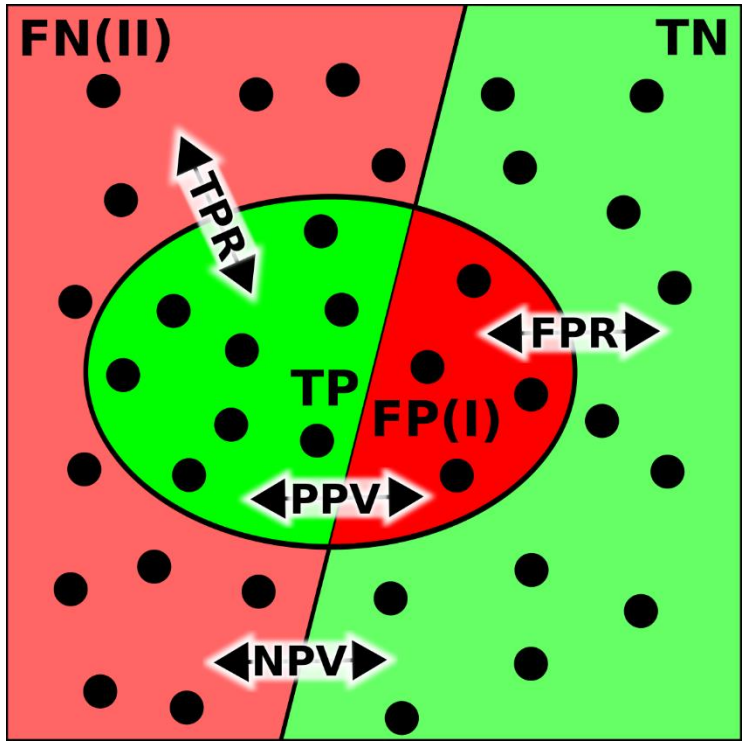
Investigation Errors

True Positive – The detection system correctly identifies malicious activity

False Positive – The detection system incorrectly flags legitimate activity as a threat (false alarm)

True Negative – The detection system correctly identifies normal, benign traffic

False Negative – The detection system fails to detect actual malicious traffic, thinking it is just benign traffic



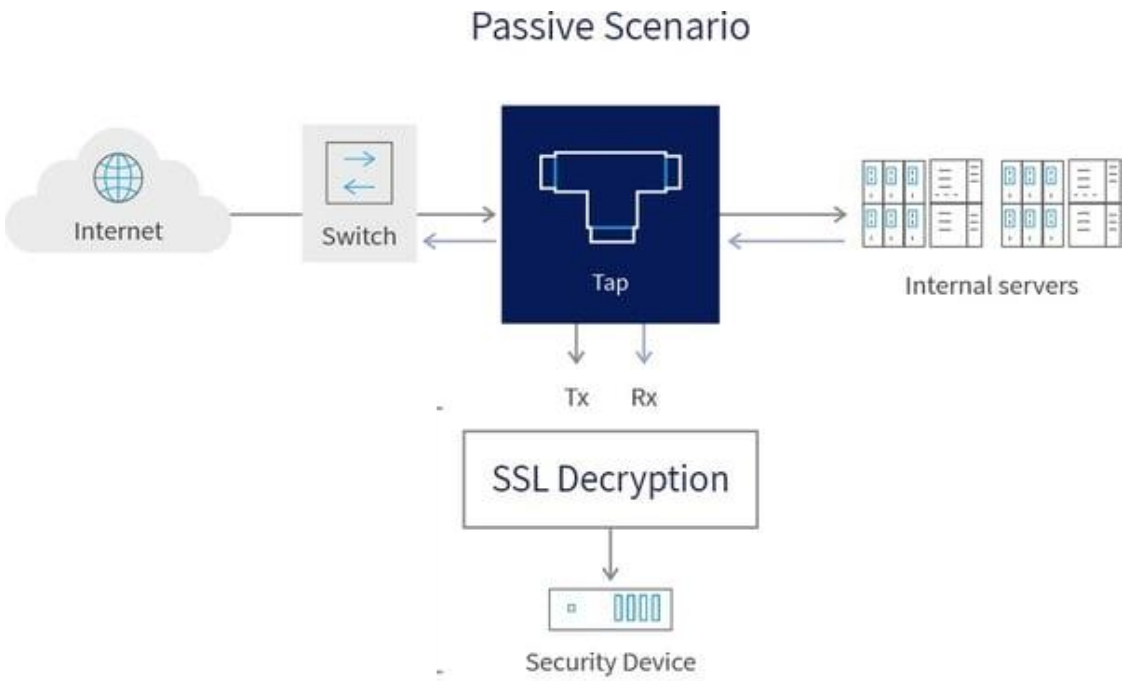
False Negatives are the scariest, and we want to minimize the number of false negatives for an IDS

Challenges with Network Forensics

- Capturing network traffic for analysis is becoming less and less feasible due to data transmission and storage limitations
- Takes a long time to sift through thousands of packets

- 100 MBPS x 7 days per week = 7.56 TB
- 10 GBPS x 7 days per week = 756 TB

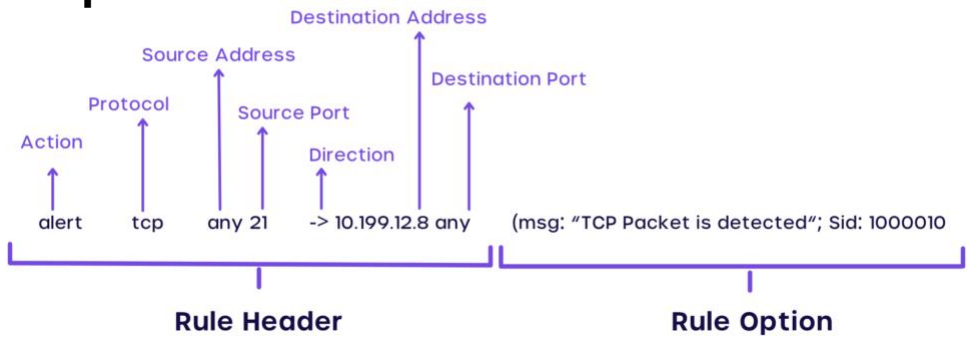
Think about keeping track of this for all machines at your organization…



- May have to decrypt in-line/MITM traffic
- Difficult to capture in a cloud network

SNORT

A set of rules to detect suspicious/malicious traffic



If we satisfy a rule, an alert can be generated or that packet can be logged

Alerts for malicious IP addresses, typical malware behavior, log unusual ports

This rule would generate an alert for web traffic that is not using the secure version of HTTP

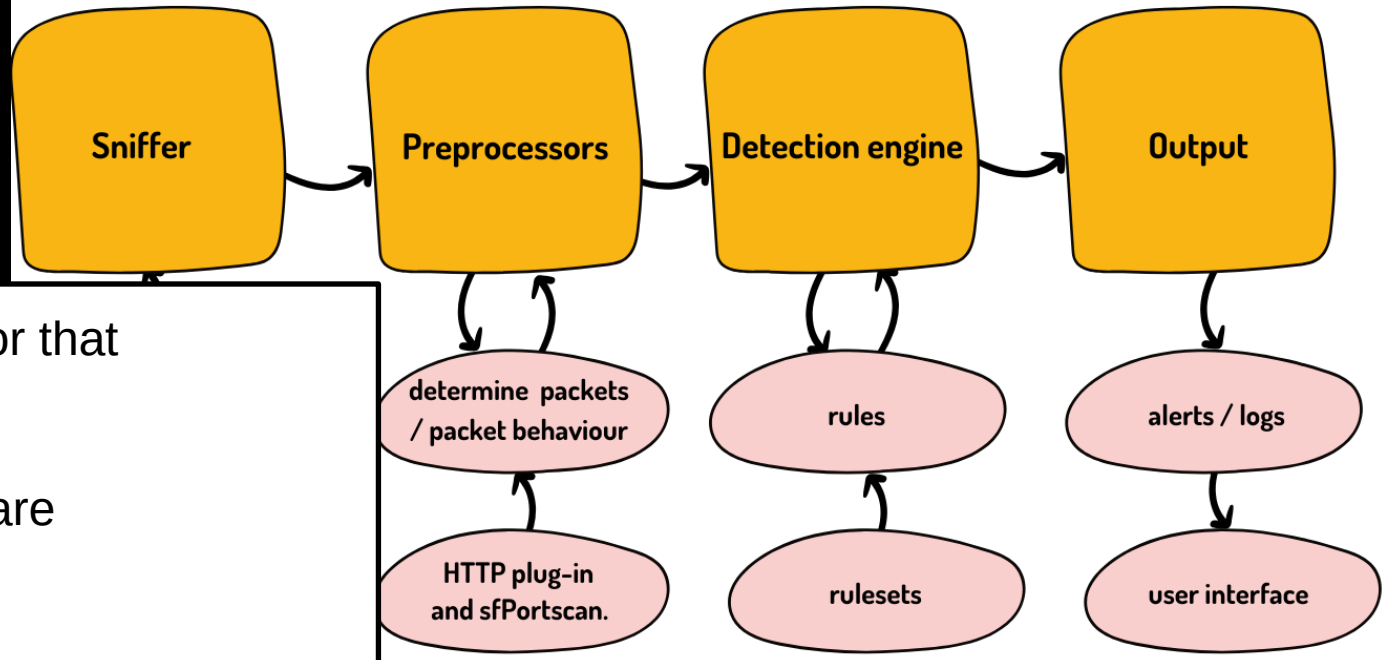
```
alert tcp any any → any 80 (msg:"Sus web traffic"; flags: S; sid: 100;)
```

The core component that collects and identifies packet structures from network traffic.

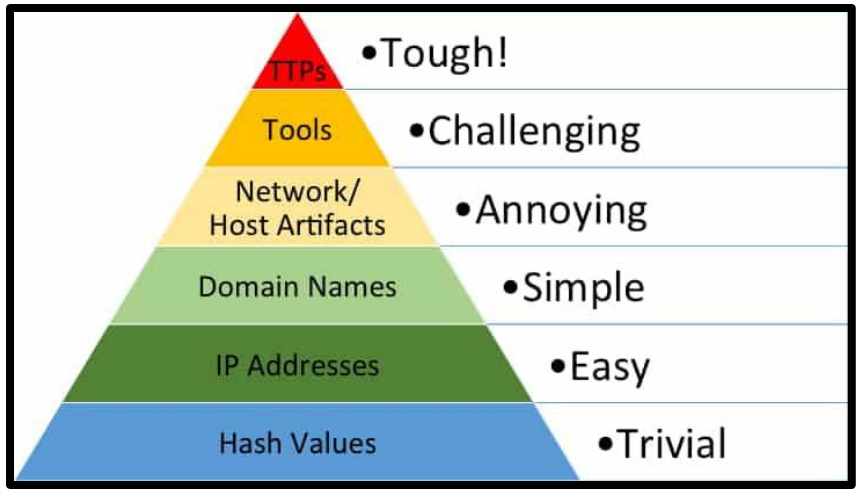
These analyze and modify packets to determine their type or behavior before passing them to the detection engine.

This compares packet data against a predefined ruleset to identify potential threats. Packets that match the rules are forwarded to the output.

Logs and triggers alerts based on detected threats. Logs can be saved in various formats and locations, and user interfaces like Snorby or ACID help manage and view this data.



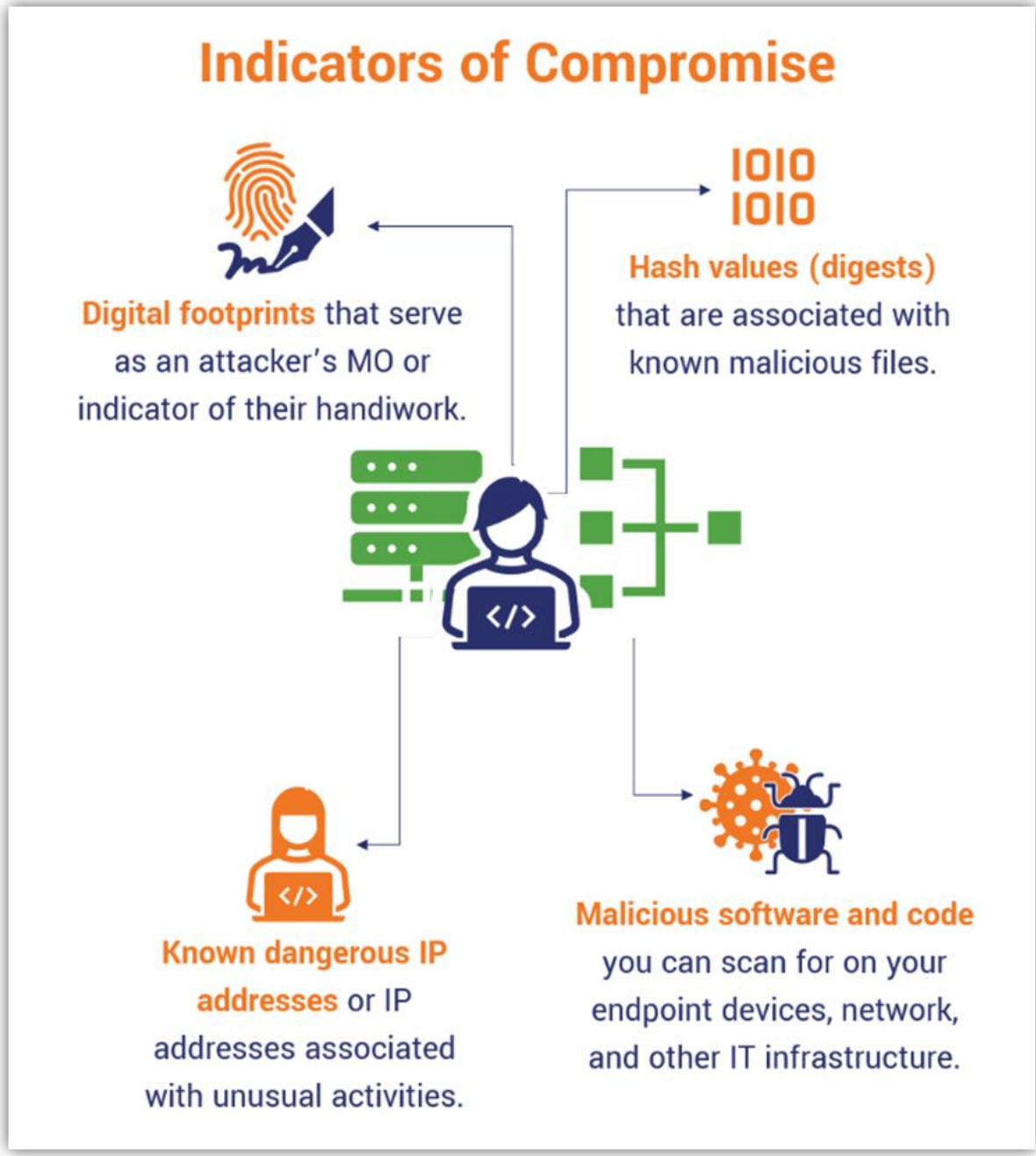
Indicators of Compromise (IOC)

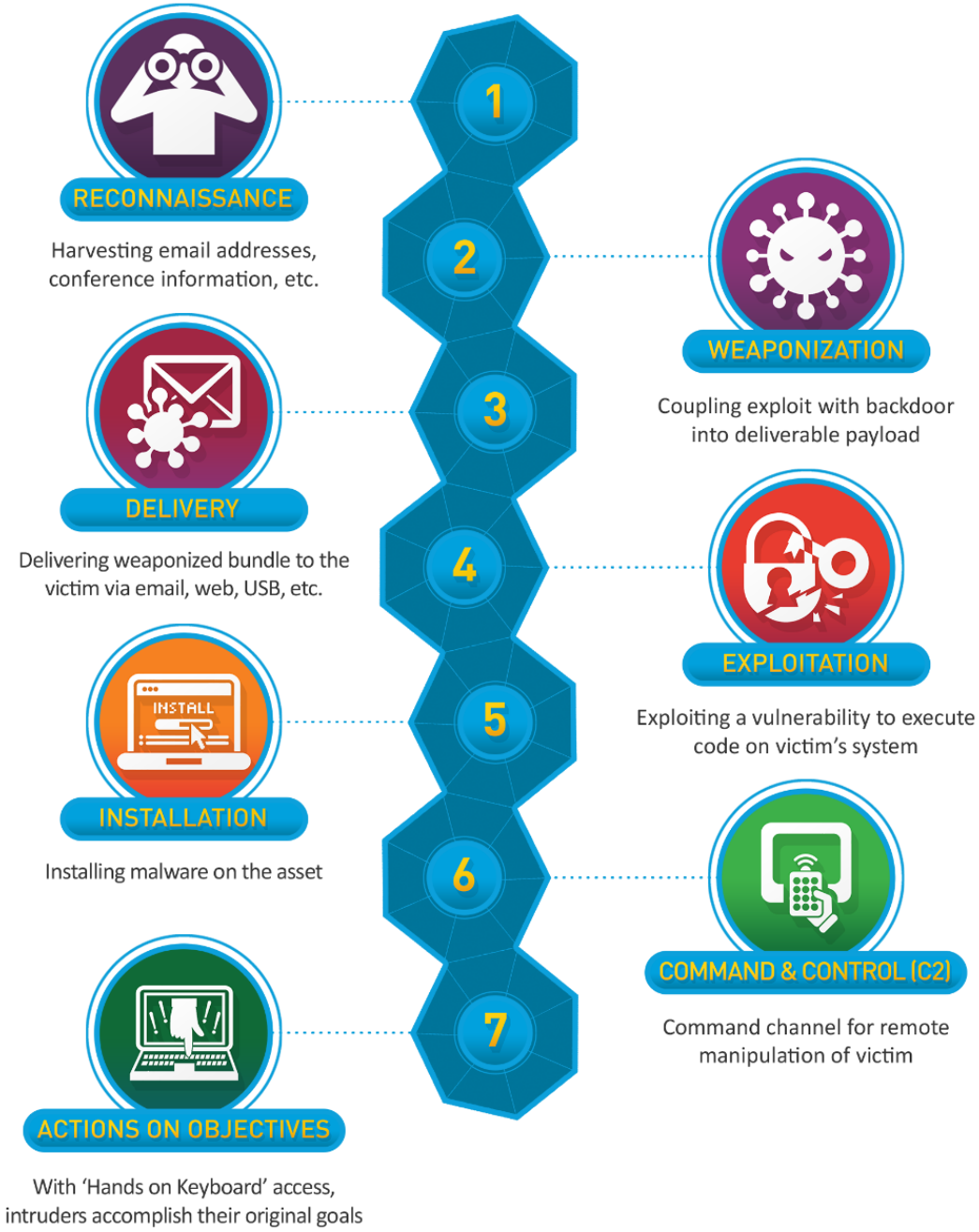


The **Pyramid of Pain** describes a list of Indicators of Compromise that can be used to detect a threat

Stuff on lower part of pyramid- easy to detect, easy for attacker to change

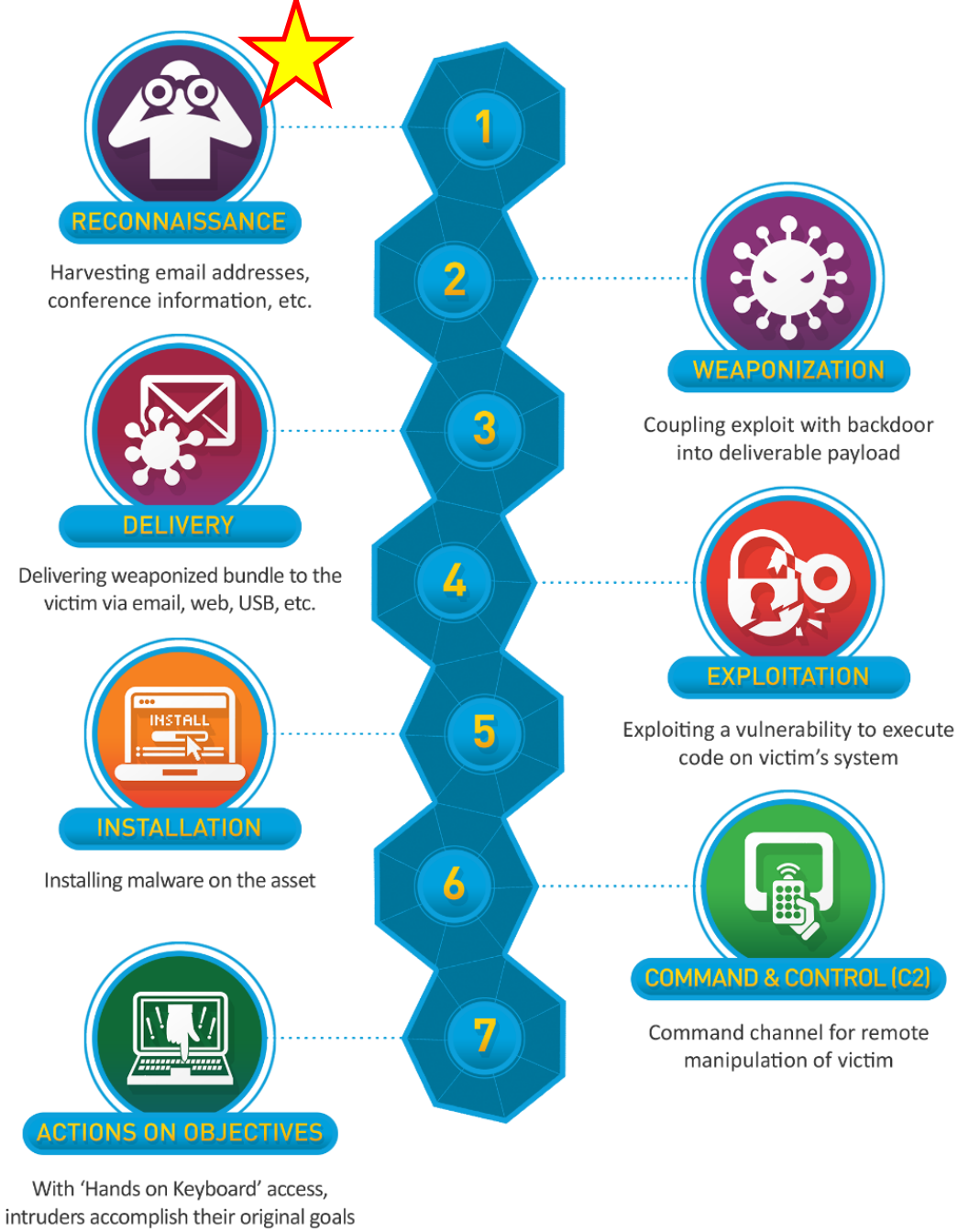
Stuff on higher part of pyramid- harder to detect, harder for an attacker to change





The **Cyber Kill Chain** describes the typical steps a malicious actor carries out to conduct a cyber attack

In network forensic investigations, we can see evidence of these steps occurring!



The **Cyber Kill Chain** describes the typical steps a malicious actor carries out to conduct a cyber attack

Step 1. Reconnaissance

Gather information about their target to understand potential vulnerabilities and points of entry

- Open Source Intelligence (OSINT)
  - look at public web pages, social media profiles, forums
- Network Scanning
  - Use **`nmap`** to discover open ports and/or services
- Gather information for phishing
  - Email lists, credentials, etc
- WHOIS Lookup, DNS Record lookup

The **Cyber Kill Chain** describes the typical steps a malicious actor carries out to conduct a cyber attack

Step 2. Weaponization

Create a tailored payload for your attack

- Malicious Emails
  - Phishing email, malicious macro file (.docx, .xlsx), zip file
- Trojan Software
  - Hide malicious payload in benign-looking software
- Language-specific payload for targeted vulnerability
- Malicious USB Drives

The **Cyber Kill Chain** describes the typical steps a malicious actor carries out to conduct a cyber attack

Step 3. Delivery

Transmit payload to target victim

- Phishing Email(s)
- Send data to open port(s)
- Send malicious USB

The **Cyber Kill Chain** describes the typical steps a malicious actor carries out to conduct a cyber attack

Step 4. Exploitation

Payload is triggered, and vulnerability is exploited

- Victim opens malicious files
- Victim opens malicious ZIP
- Server accepts attacker's payload
- Victim plugs in USB device

The **Cyber Kill Chain** describes the typical steps a malicious actor carries out to conduct a cyber attack

Step 5. Installation

Find way to install malware to cause damage or gain persistence

- Remote Access Trojans (RATs)
  - Allows attack remote control over victim's system
- Keyloggers
  - Discover passwords or credentials
- Backdoor
  - Can be used to re-enter system later on
- **Lateral Movement**
  - Try to spread to other devices on a network

The **Cyber Kill Chain** describes the typical steps a malicious actor carries out to conduct a cyber attack

Step 6. Command and Control

It is very common for attackers to "phone home" to a **command and control (C2)** server to be able to compromise the system remotely

- HTTPS/HTTP
- DNS Tunneling
- Peer-to-Peer for Botnets

The **Cyber Kill Chain** describes the typical steps a malicious actor carries out to conduct a cyber attack

Step 7. Actions on Objectives

Malware is installed, attacker can remotely access a system, now do something evil

Data **exfiltration** – unauthorized transfer of data from a device or network

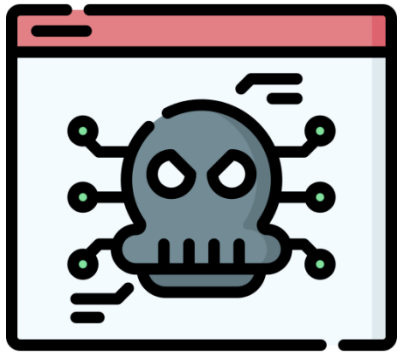
Delete Information

Ransomware

Deface website

Common Malware Behavior

- Downloading malware/malware dropper through HTTP
- Communicate with a C2 server
  - Cobalt Strike
  - Metasploit
  - Covenant
- Unusual Outbound Traffic
- Malware Beaconing
- Suspicious DNS Queries to attacker domains
- Spike in connections to other devices (lateral movement)
- Failed login attempts/authentication



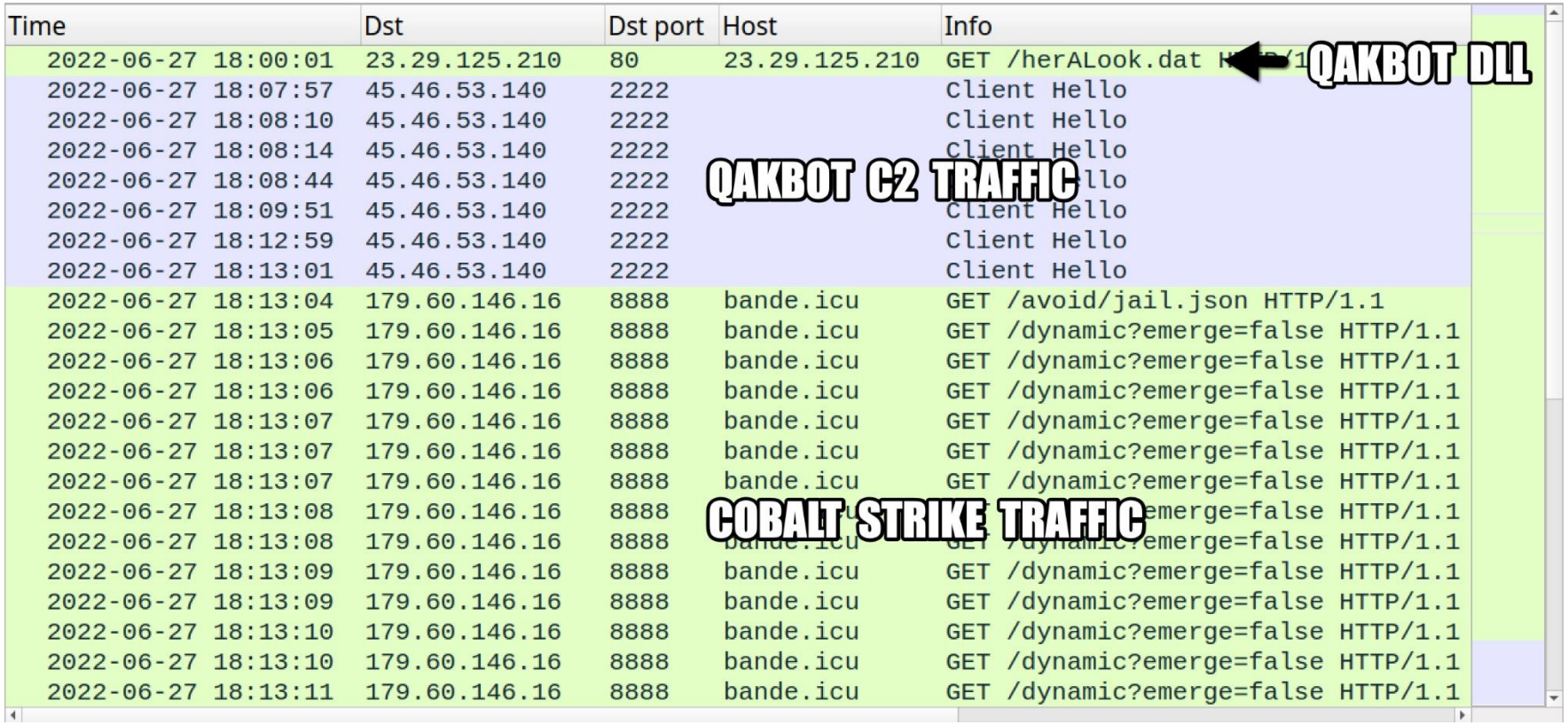
Cobalt Strike C2 Server Threat Hunting

- Use of default SSL certificates
- Increased usage of port 443, 80, 8443 with foreign IP address
- Check default responses for HTTP 404 and DNS Queries

Malware File Types to Check for

- `.exe` files - Windows executable files
- `.dll` files - Dynamic Linked Libraries
- `.msi` files – Windows installers
- `.bat` files – Windows command line script
- `.vbs` scripts – Visual Basic Scripts
- `.js` scripts – Javascript file
- `.docx` files – Microsoft Word Document (can contain macros)
- `.xlsx` files – Microsoft Excel Spreadsheet (can contain macros)
- `.zip` files – Compressed Archive Files (may have scripts when unzipped)
- `.pdf` files – Can contain suspicious links, or a PDF reader vulnerability

Wireshark

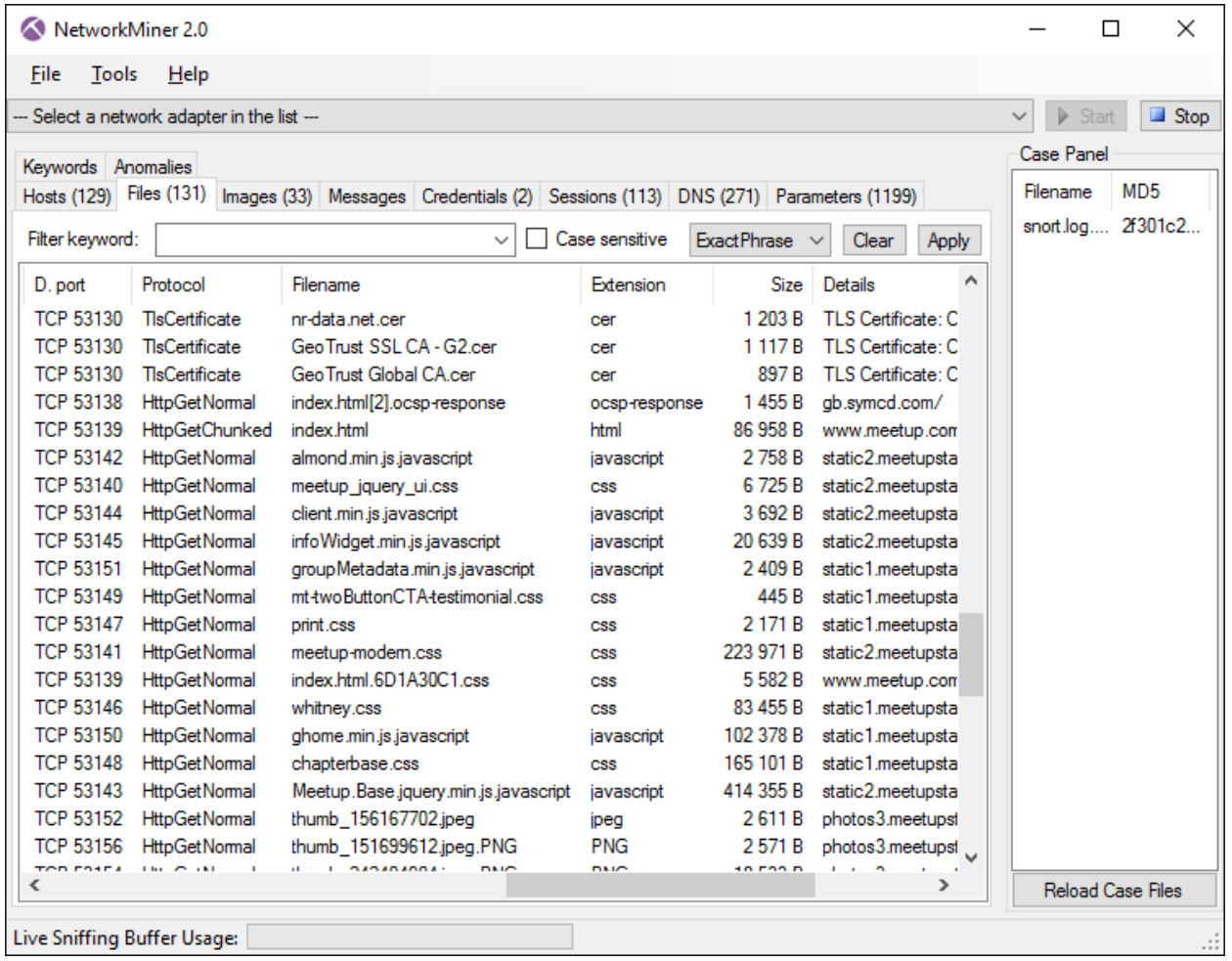


Time	Dst	Dst port	Host	Info
2022-06-27 18:00:01	23.29.125.210	80	23.29.125.210	GET /herALook.dat H[illegible]/1
2022-06-27 18:07:57	45.46.53.140	2222		Client Hello
2022-06-27 18:08:10	45.46.53.140	2222		Client Hello
2022-06-27 18:08:14	45.46.53.140	2222		Client Hello
2022-06-27 18:08:44	45.46.53.140	2222		Client Hello
2022-06-27 18:09:51	45.46.53.140	2222		Client Hello
2022-06-27 18:12:59	45.46.53.140	2222		Client Hello
2022-06-27 18:13:01	45.46.53.140	2222		Client Hello
2022-06-27 18:13:04	179.60.146.16	8888	bande.icu	GET /avoid/jail.json HTTP/1.1
2022-06-27 18:13:05	179.60.146.16	8888	bande.icu	GET /dynamic?emerge=false HTTP/1.1
2022-06-27 18:13:06	179.60.146.16	8888	bande.icu	GET /dynamic?emerge=false HTTP/1.1
2022-06-27 18:13:06	179.60.146.16	8888	bande.icu	GET /dynamic?emerge=false HTTP/1.1
2022-06-27 18:13:07	179.60.146.16	8888	bande.icu	GET /dynamic?emerge=false HTTP/1.1
2022-06-27 18:13:07	179.60.146.16	8888	bande.icu	GET /dynamic?emerge=false HTTP/1.1
2022-06-27 18:13:07	179.60.146.16	8888	bande.icu	GET /dynamic?emerge=false HTTP/1.1
2022-06-27 18:13:08	179.60.146.16	8888	bande.icu	GET /dynamic?emerge=false HTTP/1.1
2022-06-27 18:13:08	179.60.146.16	8888	bande.icu	GET /dynamic?emerge=false HTTP/1.1
2022-06-27 18:13:09	179.60.146.16	8888	bande.icu	GET /dynamic?emerge=false HTTP/1.1
2022-06-27 18:13:09	179.60.146.16	8888	bande.icu	GET /dynamic?emerge=false HTTP/1.1
2022-06-27 18:13:10	179.60.146.16	8888	bande.icu	GET /dynamic?emerge=false HTTP/1.1
2022-06-27 18:13:10	179.60.146.16	8888	bande.icu	GET /dynamic?emerge=false HTTP/1.1
2022-06-27 18:13:11	179.60.146.16	8888	bande.icu	GET /dynamic?emerge=false HTTP/1.1

We can use Wireshark to identify **specific** malicious packets, and find the exact moment where the infection started

C2 server information, Victim information, other relevant evidence

NetworkMiner

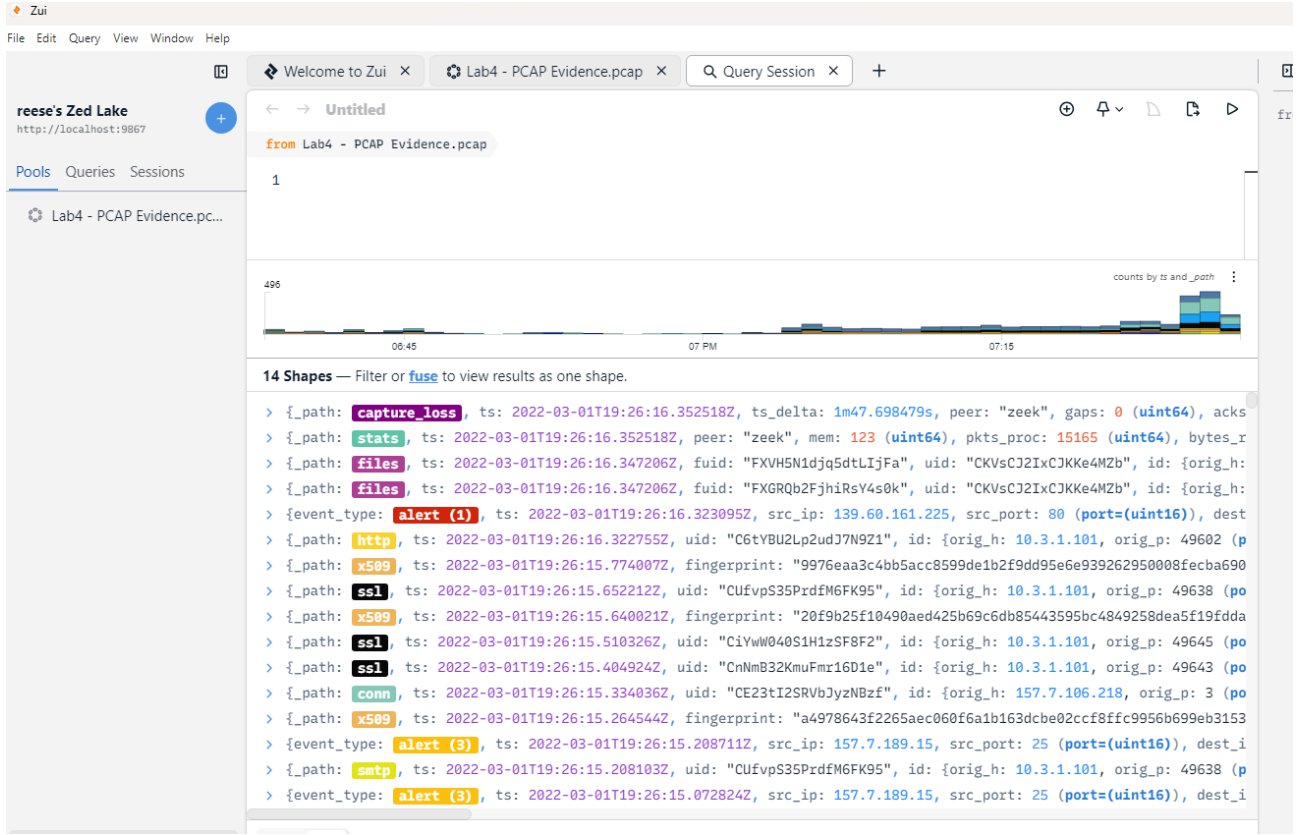


NetworkMiner is a automated flow analysis tool that will identify all hosts, downloaded files, emails, logins from a pcap file and attempt to reassemble them for analysis

Very powerful tool that can provide many helpful insights during an investigation

NetworkMiner should always be run in a sandbox environment (VM) that is disconnected from the network

Zui



Zui (formerly known as **brim**) is a automated flow analysis tool that will identify any suspicious packets, emails, certificates, files from a pcap file and create a *timeline*

Won't assemble the files, so it will be safer to use

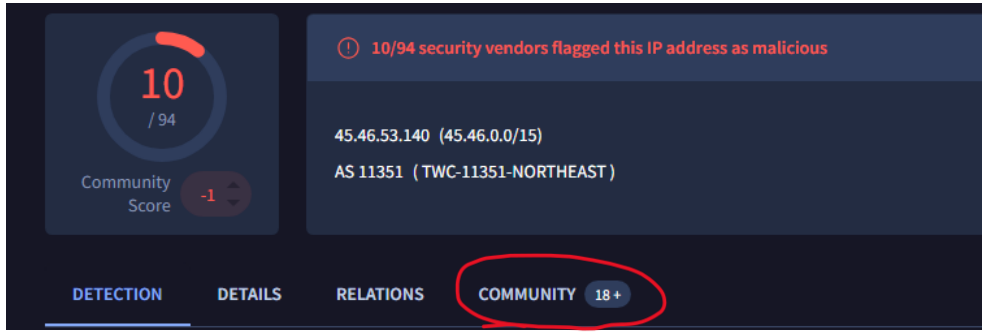
Can help identify potential IOCs

VirusTotal

VirusTotal is a massive database of known malware signatures and malicious fingerprints

We can provide signatures from our investigation to see if they have been flagged as malicious in the past

- File Hashes
- IP Addresses
- Domain Names



The community tab will provide more context around the malicious signatures

Example Timeline