Malware Detection

Malware Detection

- It comes in many different flavors
- **Extremely complex**

- We will only scratch the surface of the surface
- Even more than all the other topics

Malware Detection
≈ Classification (I)

- Main performance index: **Accuracy** (FP/FN)
- **Many other** crucial characteristics:
  - **Coverage**
    - **What** can be analyzed
      - Files / Processes Memory
      - URLs / Web pages / Network traffic
      - ...
    - With which **depth**
- ...

Malware Detection ≈ Classification (II)

- **Accuracy** (FP/FN)
- **Coverage**
  - What can be analyzed
  - With which depth
- **Scenario**
  - Live system or analysis platform?
- **Explanation**
  - Why is it (not) considered malware?
- **Novelty**
  - Can it detect only (variants of) previously known malware?
- …

Scenario 1: AV / EDR

- **AV** ("antivirus")
- ...also called **EDR** (Endpoint Detection and Response)

- **Live system**
  - Prevention
  - Containment
- Proceeds **automatically**

Scenario 2: Analysis Platform

- **Inject file F in analysis platform**
  - Most often a cloud service
- **Automated** assessment
  1. Score
  2. Description of the score (**IoC** and other)

- Static (no execution)
- Dynamic (execution within VM)
  - No input / Predefined automated inputs
  - + Operator-driven inputs

Scenario 3: Incident Response (I)

- **We know an attack is ongoing within our organization**

- Which malware?
- or only legitimate tools ("**living off the land**")?

- Which systems are in control of adversaries?
- How to contain / restore?
- How initial access was executed?
- How persistence was executed?

Scenario 3: Incident Response (II)

- We know an attack is ongoing within our organization

- Human experts
- Strong and highly specific skills

- Costly and Time-consuming

Scenario 4: Forensics (I)

- **Is this system / device clean or infected?**
- If infected:
  - Which malware?
  - How initial access / persistence?
  - How to restore it?

- Many possible combinations of
  - Automation
  - Resources
  - Human skills

Scenario 4: Forensics (II)

- Rule of thumb for "sophisticated" malware

- IF you **don't** know whether it is infected
- THEN detection is **very hard / hardly possible**
  // just too many things to analyze

- IF you know there is some malware to be found
- THEN detection is more likely

Common scenario (oversimplified) (I)

Specialized organization:

1. **Identifies** a new piece of malware (or a new variant of a known "family")
   - Proprietary automated technology
   - Operator-driven analysis

Common scenario (oversimplified) (II)

Specialized organization:

1. **Identifies** a new piece of malware
2. **Develops** and **distributes** information for its identification
   - "Signatures" of its **static** content and **dynamic** behavior:
     - File hashes
     - File names
     - Contacted IPs / Domains
     - ...

↓

- Indicators of Compromise (**IoC**) that suggest its **presence** on a system

Common scenario (oversimplified) (III)

Specialized organization:

1. Identifies a new piece of malware
   (or a new variant of a known "family")
2. Develops and distributes IoC

"Every defender" incorporates IoC in its systems

- AV / EDR
- Analysis platforms
- ...

(Oversimplified) Remark

- Detecting a "novel" malware is very hard
- Even for skilled operators with plenty of time and resources

- Most real detections are of malware that "someone" has **previously** discovered and described "somehow"

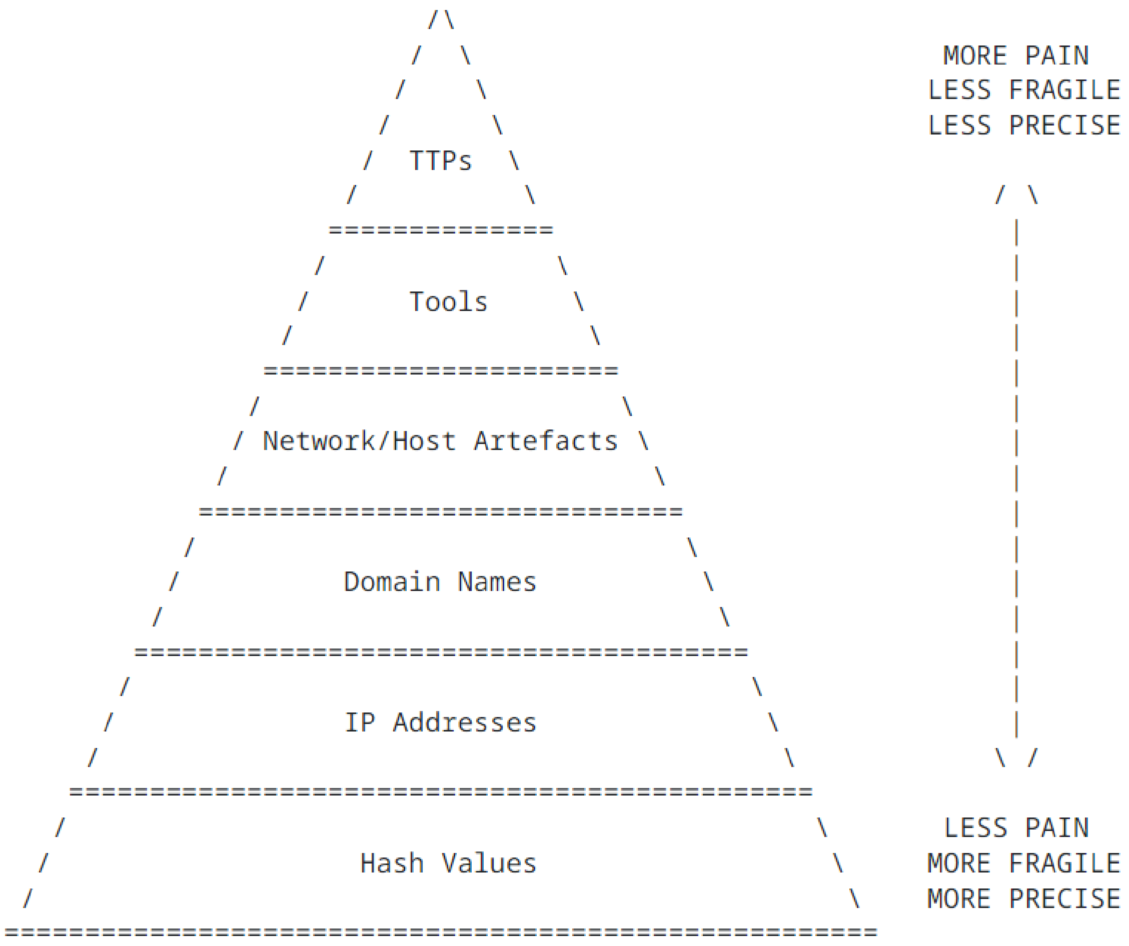
Important

- Download locations
- Download protocols
- File names
- File contents (hashes)

- There may be **many** differences even in the **same** campaign!

- IoC might cover only a **subset** of a given campaign
- IoC might become **obsolete**

IoC & "Pyramid of Pain"



```
                          /\
                         /  \                             MORE PAIN
                        /    \                           LESS FRAGILE
                       /      \                          LESS PRECISE
                      /  TTPs  \
                     /          \                             / \
                    ==============                             |
                   /              \                            |
                  /      Tools     \                           |
                 /                  \                          |
                ======================                         |
               /                      \                        |
              / Network/Host Artefacts \                       |
             /                          \                      |
            ==============================                     |
           /                              \                    |
          /          Domain Names          \                   |
         /                                  \                  |
        ======================================                 |
       /                                      \                |
      /              IP Addresses              \               |
     /                                          \             \ /
    ==============================================
   /                                              \       LESS PAIN
  /                   Hash Values                  \     MORE FRAGILE
 /                                                  \    MORE PRECISE
======================================================
```

Detection more difficult and less precise...but Attacker **cannot** change easily *(change with more pain)*

Detection easy and precise ...but Attacker **can change easily** *(change with less pain)*

Threat Intelligence (in a nutshell)

Malware Campaign

- Attacks to **different** organizations often exhibit **many similarities**
  - Tactics, Techniques, Procedures (**TTP**)
  - Type of targeted organizations
  - Objectives
  - IoC
  - ...
- **Campaign**: grouping of "attacks with many similarities" in a specific time period
- **Attributed** to a specific **threat actor** (or **group**)
- Naming and definitions of campaigns and threat actors **not uniform**

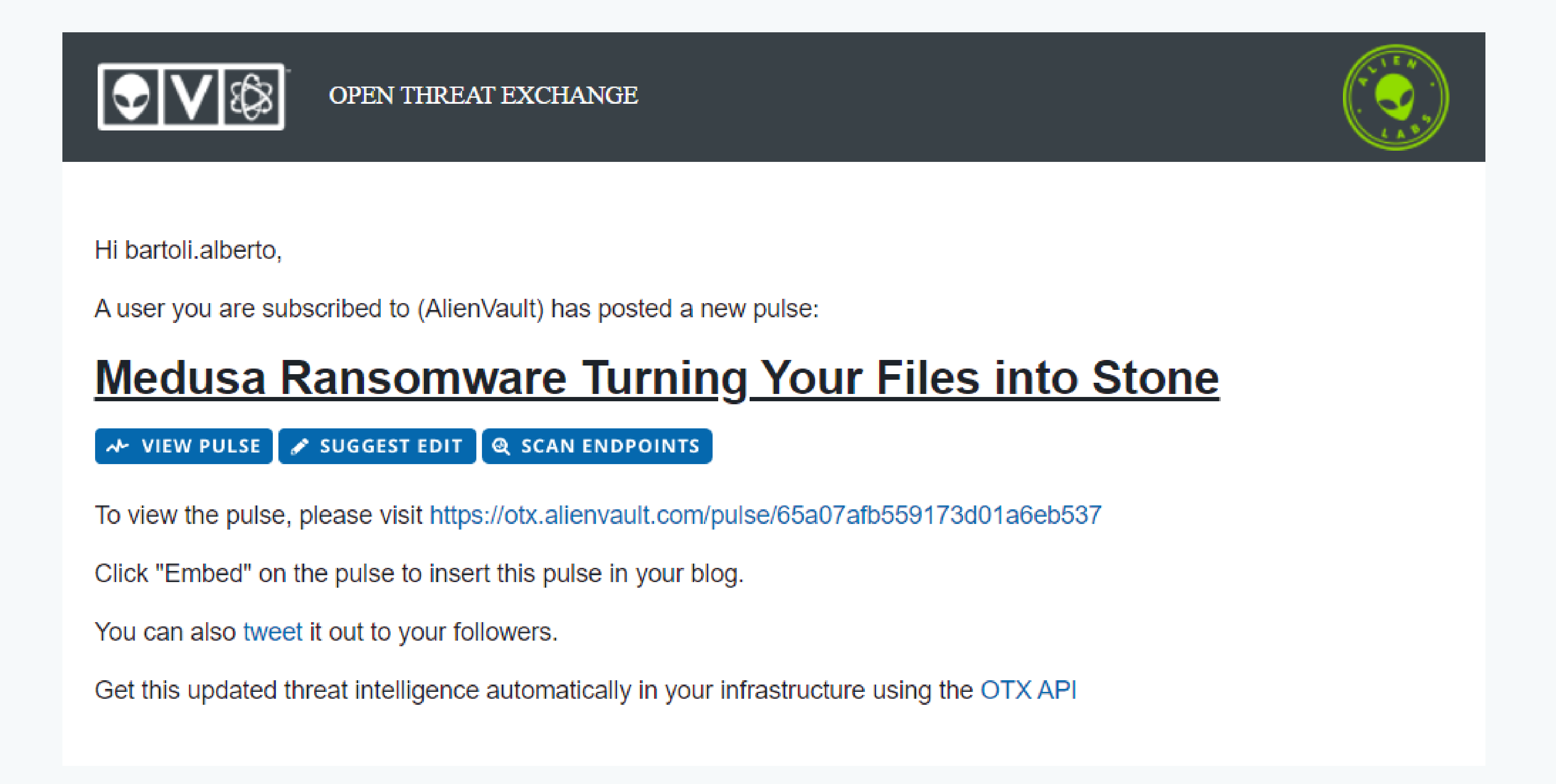
Threat Intelligence (in a nutshell)

- **"Information"** about **potential cyber threats** and **risks**

- Gathered through the analysis of various sources, including:
  - **Malware analysis**
  - **Vulnerability assessments**
  - **Monitoring of threat actors activities**
  - …

- Propagated through free / paid services

Example: Email Alert



Hi bartoli.alberto,

A user you are subscribed to (AlienVault) has posted a new pulse:

Medusa Ransomware Turning Your Files into Stone

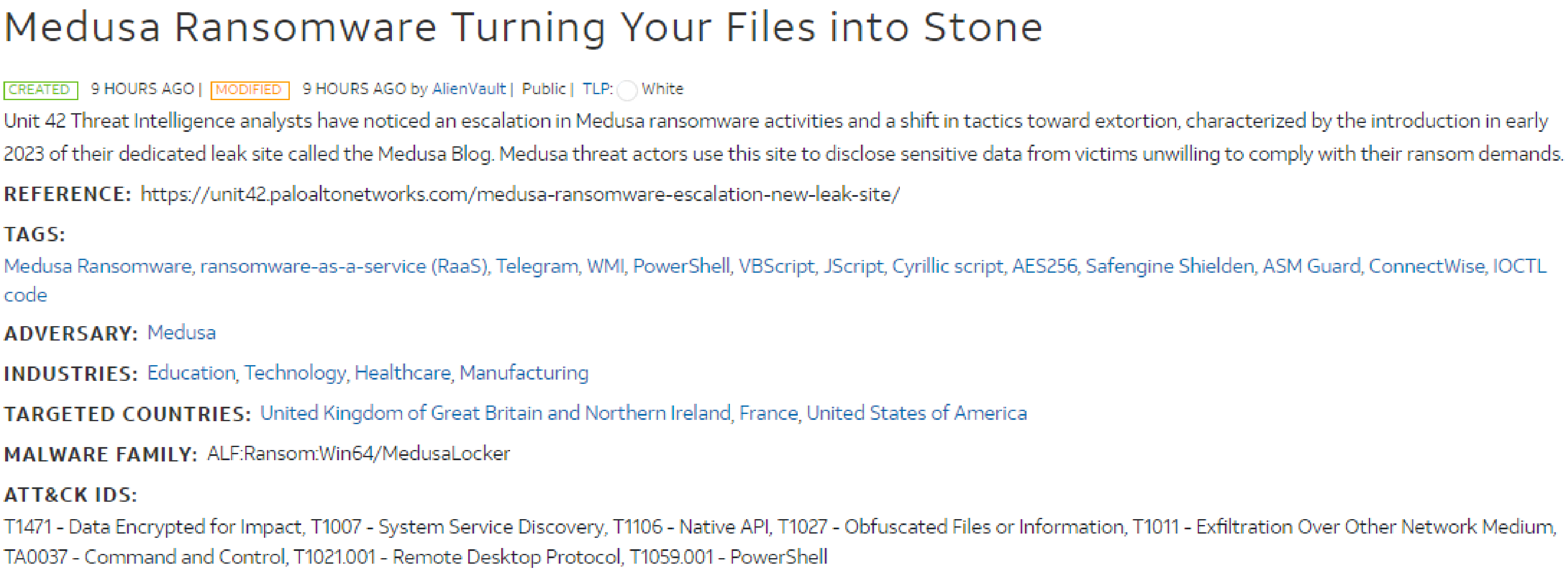
To view the pulse, please visit https://otx.alienvault.com/pulse/65a07afb559173d01a6eb537

Click "Embed" on the pulse to insert this pulse in your blog.

You can also tweet it out to your followers.

Get this updated threat intelligence automatically in your infrastructure using the OTX API

Example: Threat Description



Medusa Ransomware Turning Your Files into Stone

CREATED 9 HOURS AGO | MODIFIED 9 HOURS AGO by AlienVault | Public | TLP: ○ White

Unit 42 Threat Intelligence analysts have noticed an escalation in Medusa ransomware activities and a shift in tactics toward extortion, characterized by the introduction in early 2023 of their dedicated leak site called the Medusa Blog. Medusa threat actors use this site to disclose sensitive data from victims unwilling to comply with their ransom demands.

REFERENCE: https://unit42.paloaltonetworks.com/medusa-ransomware-escalation-new-leak-site/

TAGS:

Medusa Ransomware, ransomware-as-a-service (RaaS), Telegram, WMI, PowerShell, VBScript, JScript, Cyrillic script, AES256, Safengine Shielden, ASM Guard, ConnectWise, IOCTL code

ADVERSARY: Medusa

INDUSTRIES: Education, Technology, Healthcare, Manufacturing

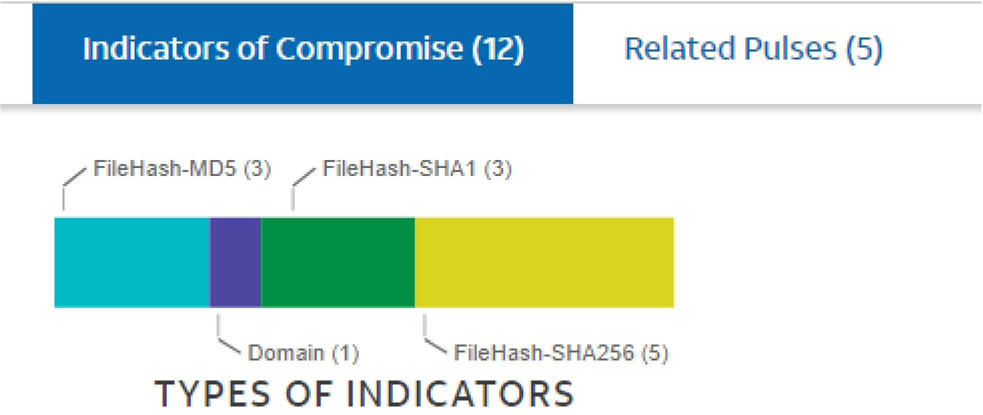
TARGETED COUNTRIES: United Kingdom of Great Britain and Northern Ireland, France, United States of America

MALWARE FAMILY: ALF:Ransom:Win64/MedusaLocker

ATT&CK IDS:

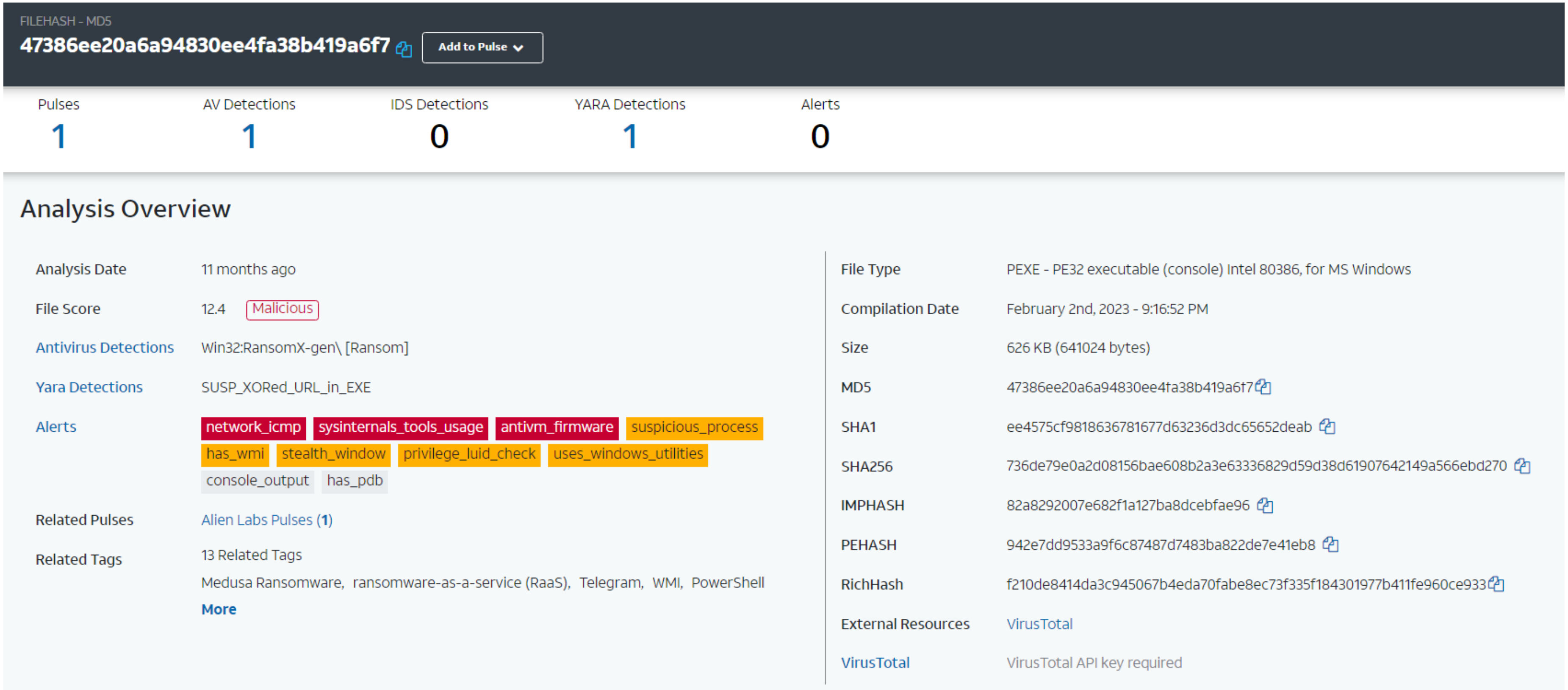
T1471 - Data Encrypted for Impact, T1007 - System Service Discovery, T1106 - Native API, T1027 - Obfuscated Files or Information, T1011 - Exfiltration Over Other Network Medium, TA0037 - Command and Control, T1021.001 - Remote Desktop Protocol, T1059.001 - PowerShell

Example: IoC



Indicators of Compromise (12)
Related Pulses (5)
FileHash-MD5 (3)
FileHash-SHA1 (3)
Domain (1)
FileHash-SHA256 (5)
TYPES OF INDICATORS

Example IoC: FileHash



FILEHASH - MD5

47386ee20a6a94830ee4fa38b419a6f7

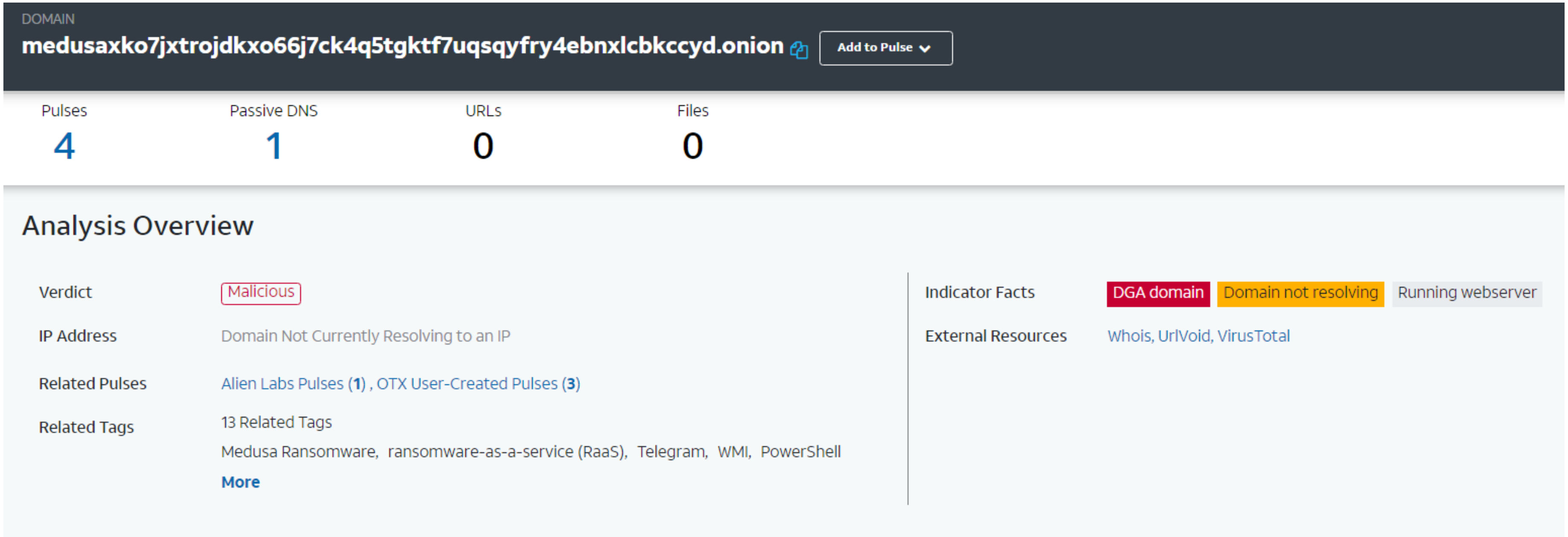
Pulses	AV Detections	IDS Detections	YARA Detections	Alerts
1	1	0	1	0

Analysis Overview

Analysis Date	11 months ago
File Score	12.4 Malicious
Antivirus Detections	Win32:RansomX-gen\ [Ransom]
Yara Detections	SUSP_XORed_URL_in_EXE
Alerts	network_icmp sysinternals_tools_usage antivm_firmware suspicious_process has_wmi stealth_window privilege_luid_check uses_windows_utilities console_output has_pdb
Related Pulses	Alien Labs Pulses (1)
Related Tags	13 Related Tags Medusa Ransomware, ransomware-as-a-service (RaaS), Telegram, WMI, PowerShell More

File Type	PEXE - PE32 executable (console) Intel 80386, for MS Windows
Compilation Date	February 2nd, 2023 - 9:16:52 PM
Size	626 KB (641024 bytes)
MD5	47386ee20a6a94830ee4fa38b419a6f7
SHA1	ee4575cf9818636781677d63236d3dc65652deab
SHA256	736de79e0a2d08156bae608b2a3e63336829d59d38d61907642149a566ebd270
IMPHASH	82a8292007e682f1a127ba8dcebfae96
PEHASH	942e7dd9533a9f6c87487d7483ba822de7e41eb8
RichHash	f210de8414da3c945067b4eda70fabe8ec73f335f184301977b411fe960ce933
External Resources	VirusTotal
VirusTotal	VirusTotal API key required

Example IoC: Domain



DOMAIN

medusaxko7jxtrojdkxo66j7ck4q5tgktf7uqsqyfry4ebnxlcbkccyd.onion

Pulses	Passive DNS	URLs	Files
4	1	0	0

Analysis Overview

Verdict	Malicious
IP Address	Domain Not Currently Resolving to an IP
Related Pulses	Alien Labs Pulses (1) , OTX User-Created Pulses (3)
Related Tags	13 Related Tags Medusa Ransomware, ransomware-as-a-service (RaaS), Telegram, WMI, PowerShell More
Indicator Facts	DGA domain Domain not resolving Running webserver
External Resources	Whois, UrlVoid, VirusTotal

YARA

Yet **A**nother **R**ecursive **A**cronym

- A "tool" for **identifying** and **classifying** malware samples
- Each **rule** describes a malware. It consists of a set of strings and a boolean expression which determine its logic.
- It can describe:
  - **Static** properties (e.g., to be searched in a file)
  - **Dynamic** properties (e.g., to be searched in network messages / system calls)
- An engine can scan a file/log against a set of rules

STIX / TAXII

Structured **T**hreat **I**nformation E**x**pression

- **Language** and **serialization** protocol for describing and exchanging cyber threat intelligence
  - IoC
  - Techniques, Tactics, Procedurs of a threat actor
  - YARA rules
  - ...

Trusted **A**utomated E**x**change of **I**ntelligence **I**nformation

- Application layer protocol for the **communication** of cyber threat information in a simple and scalable manner

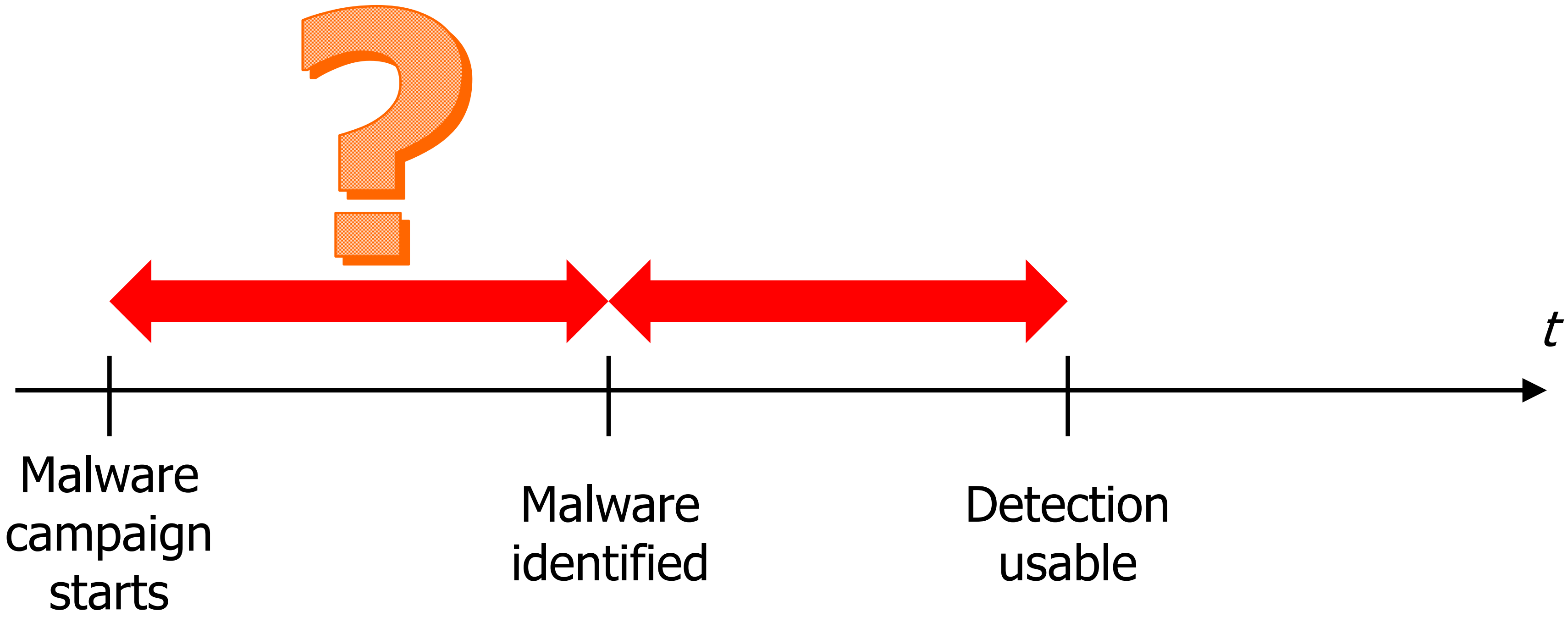
Threat Intelligence: Remark

- **Crucial** component of a comprehensive cybersecurity strategy

- Useful for:
  - Identification
  - Prevention
  - Mitigation
  - …

Some Practical Issues in Malware Detection

Crucial practical issues (I)

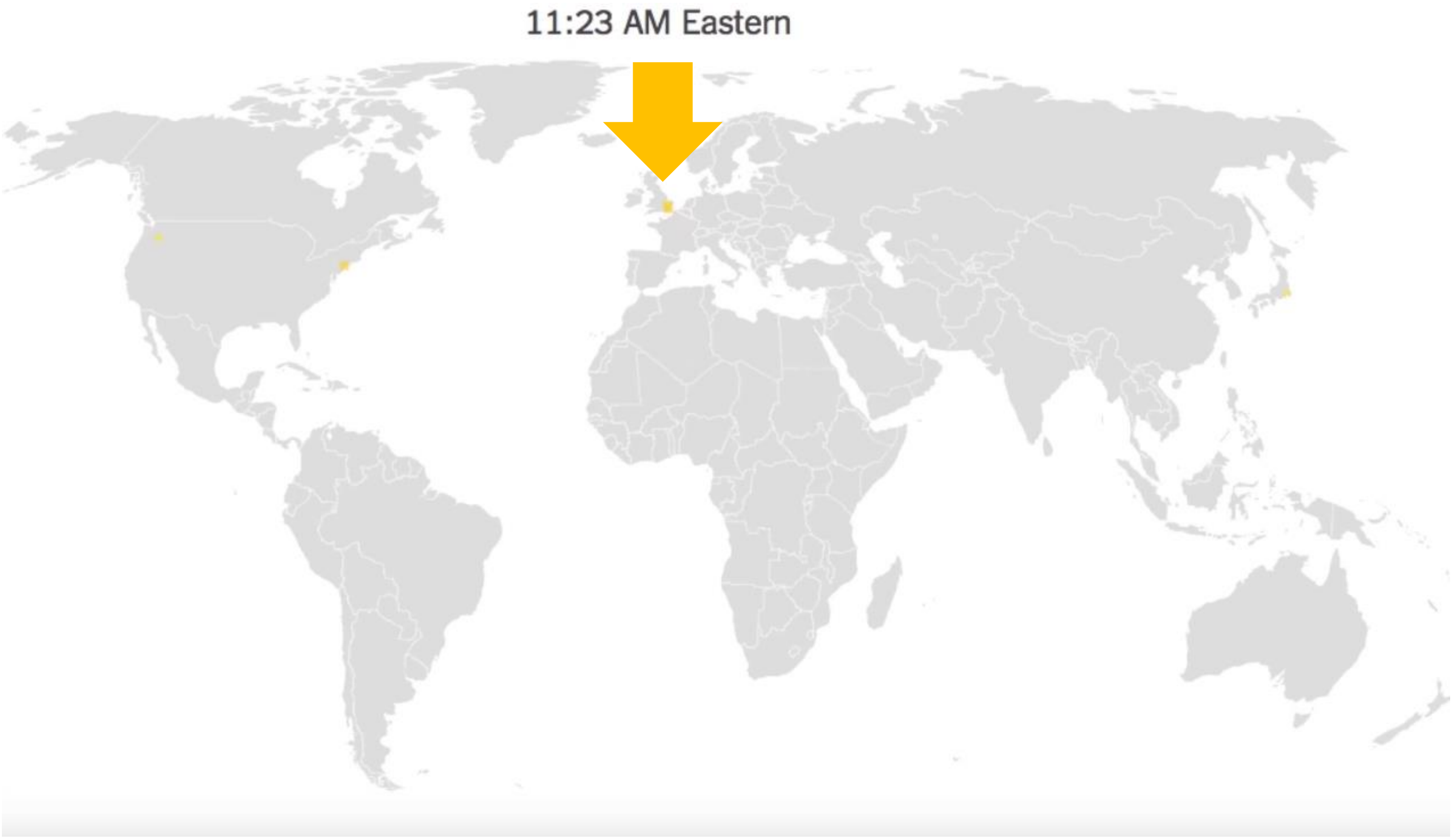


Malware campaign starts

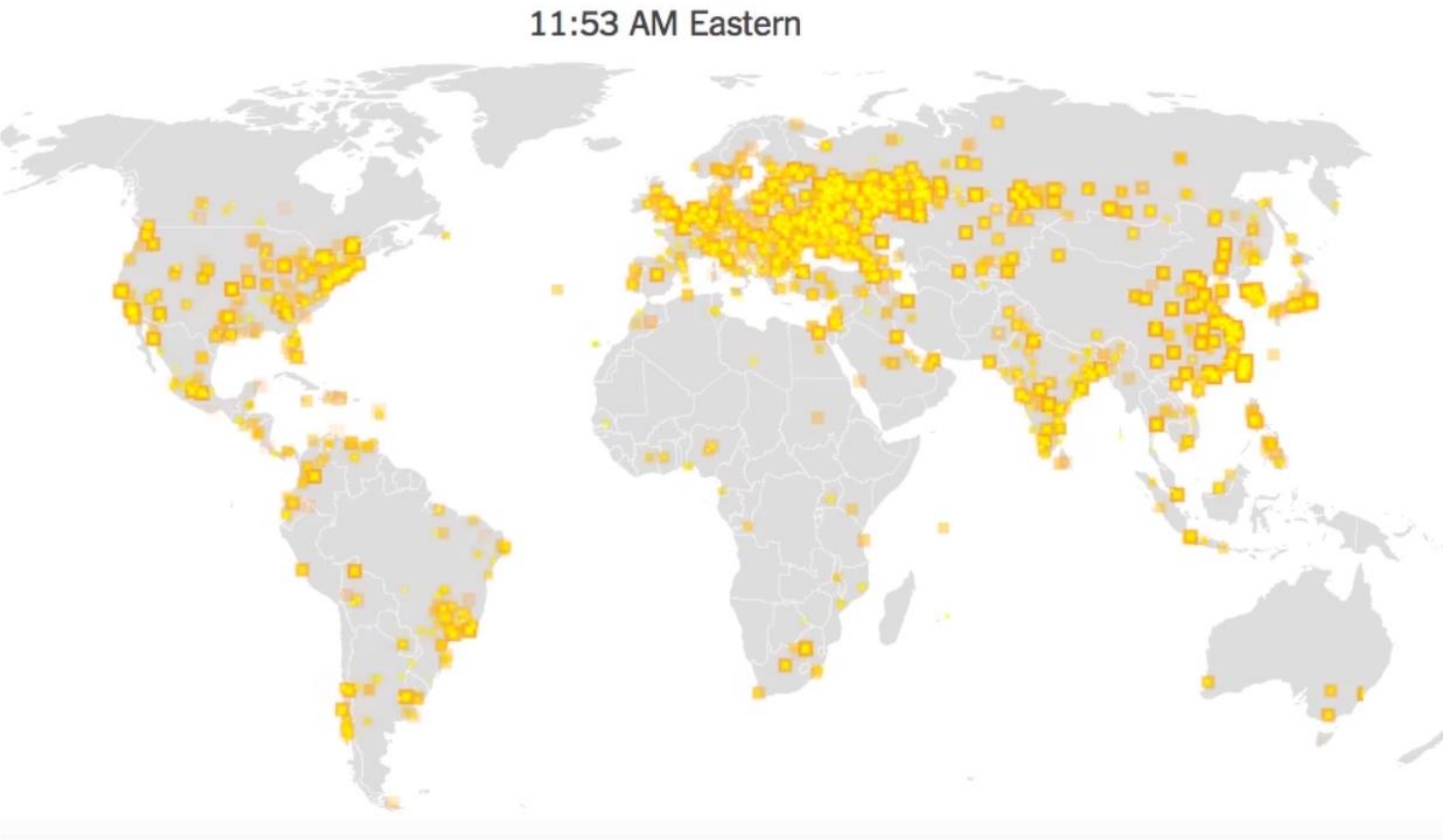
Malware identified

Detection usable

Wannacry (May 2017): Time 0



Wannacry (May 2017): 30 minutes



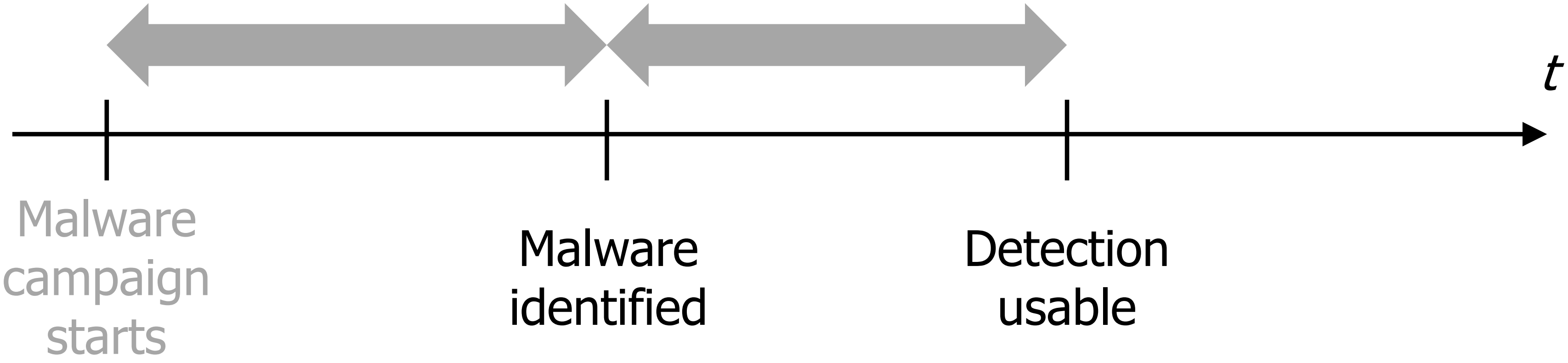
An event at UniTS (March 2018)

- **9AM** Attack campaign via mail
  - Propagation through attachment
  - Inbox scan
  - Send email with same Subject to the same people
- Not detected by 3 AV (org boundary, email, endpoint)

- **+3 hours** Notification to AV-boundary

- **+12 hours** AV-endpoint updated
- **+24 hours** AV-boundary updated
- **+31 hours** AV-email not yet updated
- C

Crucial practical issues (II)



Really?

Really?

- How effective are detection rules?
  - FP / FN?
  - Prevention or IoC?

A quick look at AVs (antiviruses)

A quick look at AVs (antiviruses)

- **What** they scan?
- **When** they scan?
- What can they **detect**?

- Many, many other important issues
  - How do they scan?
  - How do they protect themselves?
  - How do they react to a detected threat?
  - How and how frequently are they updated?
  - ...
- Proprietary and "heterogenous" technology

What

- **File system**
  - Newly-created and/or modified
- **Process**
  - Children of loaders, Injections
- **Memory**
  - Fileless malware
- **Browser**
  - HTTP traffic, loaded content
- **Network**
  - Not very common

When

- **Real-time**
  - Continuos inspection of process-O.S. interactions
- **Trigger-based**
  - Upon specific actions (e.g., when a file is about to be run)

- **On-demand**
- **Scheduled**

- **Delayed**
  - Additional checks on artifacts clean with "not high confidence"
  - When the system is idle / Cloud service

Detection (I)

- **Signatures**
  - **Patterns in content** of file / memory / network traffic
    - Video in companion website
      - Write pattern in text file → Detected as malware (!)
      - Cut text file in two pieces → Piece with pattern still detected as malware
  - Evasion techniques:
    - Polymorphism:
      Every instance looks different, while retaining its functionality
    - Obfuscation:
      XOR/RC4 with unique key, Base64 encoding, ...
    - Scan performed before deobfuscation does not detect
    - Trying to deobfuscate everything may not be feasible

Detection (II)

- **Behavior**
  - Patterns of **process / memory manipulation** and **syscall invocations**

  - DLL injection by reflection
    - DLL loaded by skipping system calls normally used to this purpose
  - Process hollowing
    - Clone legitimate process and then replace its code
  - ...

- Usually low recall