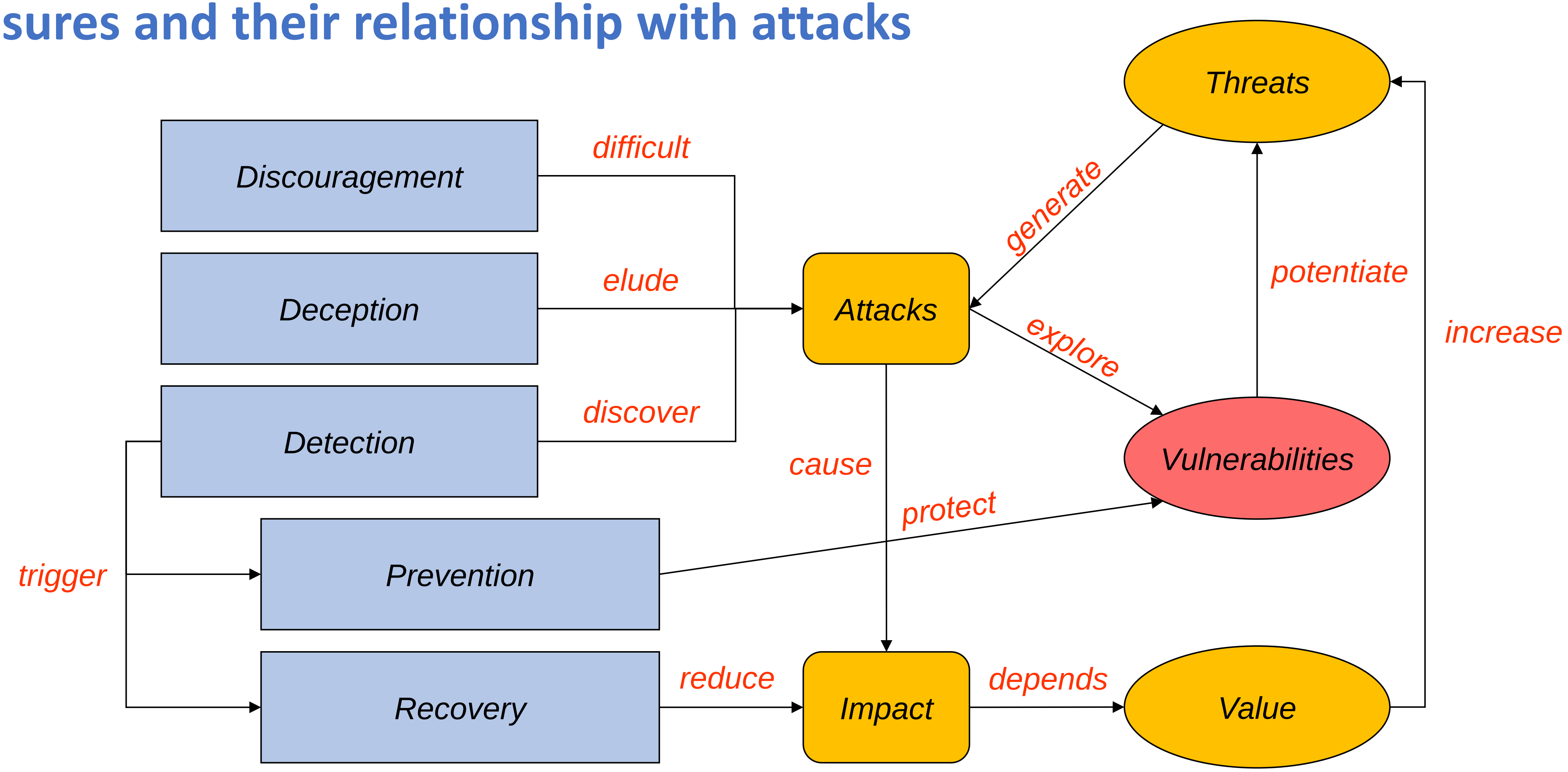
Threats and Vulnerabilities

SIO

deti universidade de aveiro
departamento de eletrónica,
telecomunicações e informática

Information Security

Measures and their relationship with attacks



Measures (and some tools)

- **Discouragement**
  - Punishment
    - Legal restrictions
    - Forensic evidences
  - Security barriers
    - Firewalls
    - Autentication
    - Secure communication
    - Sandboxing
- **Detection**
  - Intrusion detection system
    - e.g. Seek, Bro, Suricata
  - Auditing
  - Forensic break-in analysis

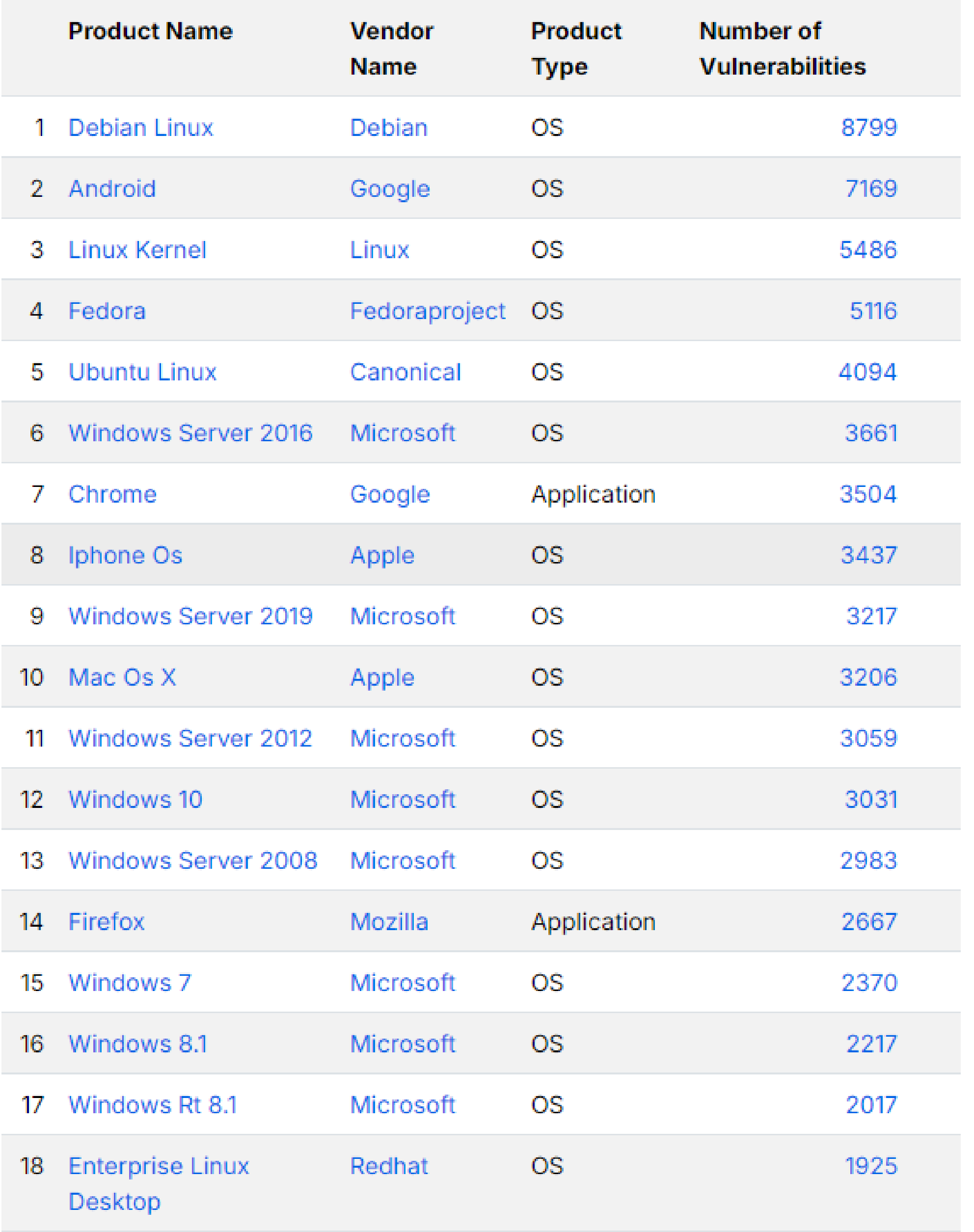
- **Discouragement**
  - Honeypots / honeynets
  - Forensic follow-up
- **Prevention**
  - Restrictive policies
    - e.g. least privilege principle
  - Vulnerability scanning
    - e.g. OpenVAS, metasploit
  - Vulnerability patching
    - e.g. regular updates
- **Recovery**
  - Backups
  - Redundant systems
  - Forensic recovery

Threats and Attacks

- Threat Actors **explore Vulnerabilities**
  - They will trigger and action, send a crafted payload, to disrupt CIA and existing policies

- Threat Actors also conduct Attacks **without** clear **Software Vulnerabilities**
  - **Targeting people, processes and resources**
  - Out of the scope of Information Security, but relevant to the security of Organizations

- The number vulnerabilities depends on Value and Security Posture
  - More popular software will have higher number of vulnerabilities
  - Also software with more higher maturity (more tests)



	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	Debian Linux	Debian	OS	8799
2	Android	Google	OS	7169
3	Linux Kernel	Linux	OS	5486
4	Fedora	Fedoraproject	OS	5116
5	Ubuntu Linux	Canonical	OS	4094
6	Windows Server 2016	Microsoft	OS	3661
7	Chrome	Google	Application	3504
8	Iphone Os	Apple	OS	3437
9	Windows Server 2019	Microsoft	OS	3217
10	Mac Os X	Apple	OS	3206
11	Windows Server 2012	Microsoft	OS	3059
12	Windows 10	Microsoft	OS	3031
13	Windows Server 2008	Microsoft	OS	2983
14	Firefox	Mozilla	Application	2667
15	Windows 7	Microsoft	OS	2370
16	Windows 8.1	Microsoft	OS	2217
17	Windows Rt 8.1	Microsoft	OS	2017
18	Enterprise Linux Desktop	Redhat	OS	1925

https://www.cvedetails.com/top-50-products.php?year=0

Common Attacks and Threats

Only some... more here: https://owasp.org/www-community/attacks/

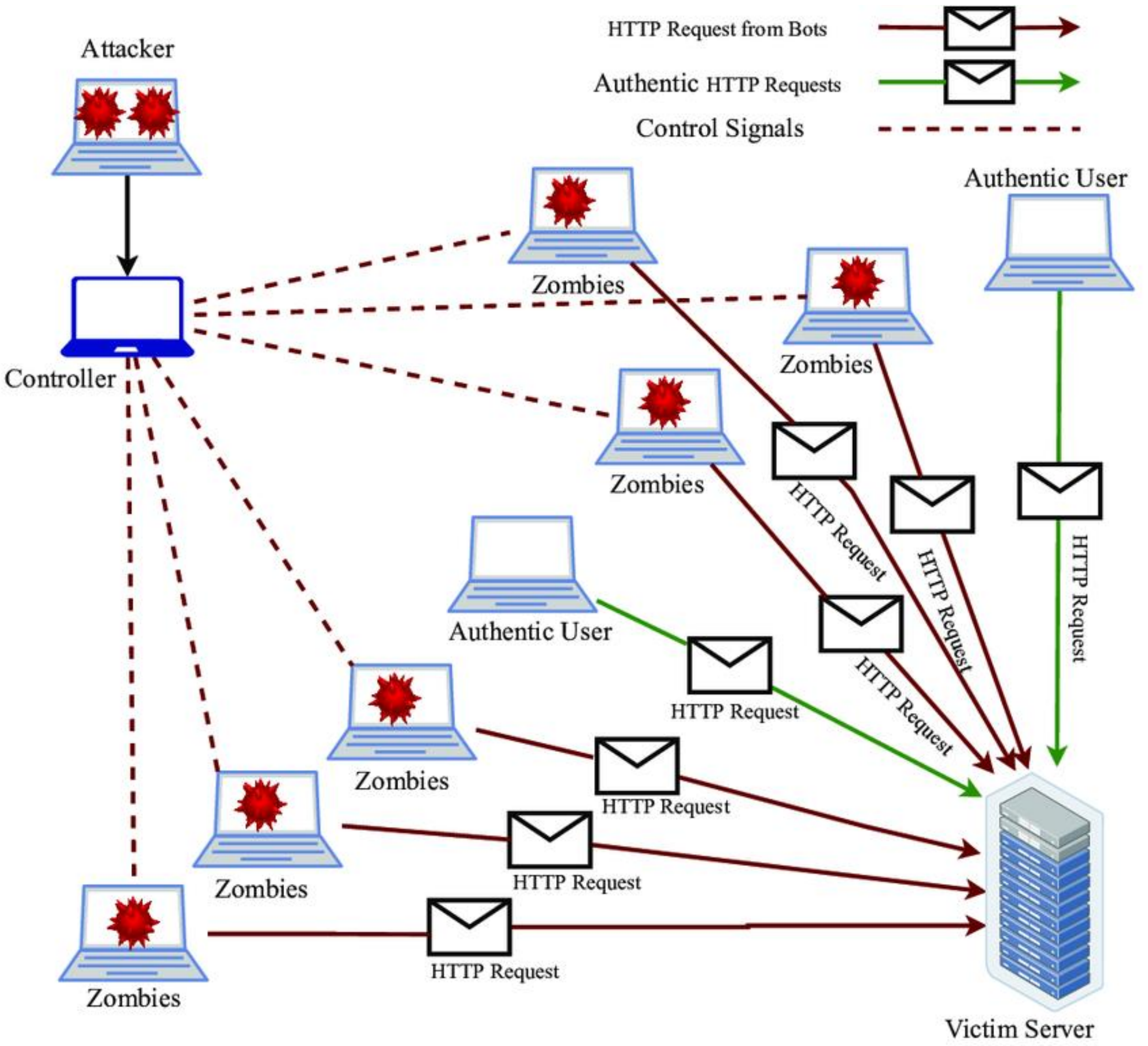
- Denial Of Service
- MiTM
- Phishing
- Ransomware
- Password
- Injection
- Malware
- Insider Threats

Denial of Service (DoS)

- Attacker overwhelms the resources of a system to the point where it is unable to reply to legitimate service requests.
  - Overwhelms **server providing the service**
  - Overwhelms dependent services such as the Authentication or Database servers
  - Frequently executed as a DDoS – Distributed DoS
  - Explores **software/system vulnerabilities**

- Impact: Clients are unable to access a service
  - Financial, brand and operational damage (e.g. Denial of Wallet)
  - Popular in relevant moments (exams, elections, public events)
  - Popular due to the low cost and low complexity

Denial of Service (DoS)



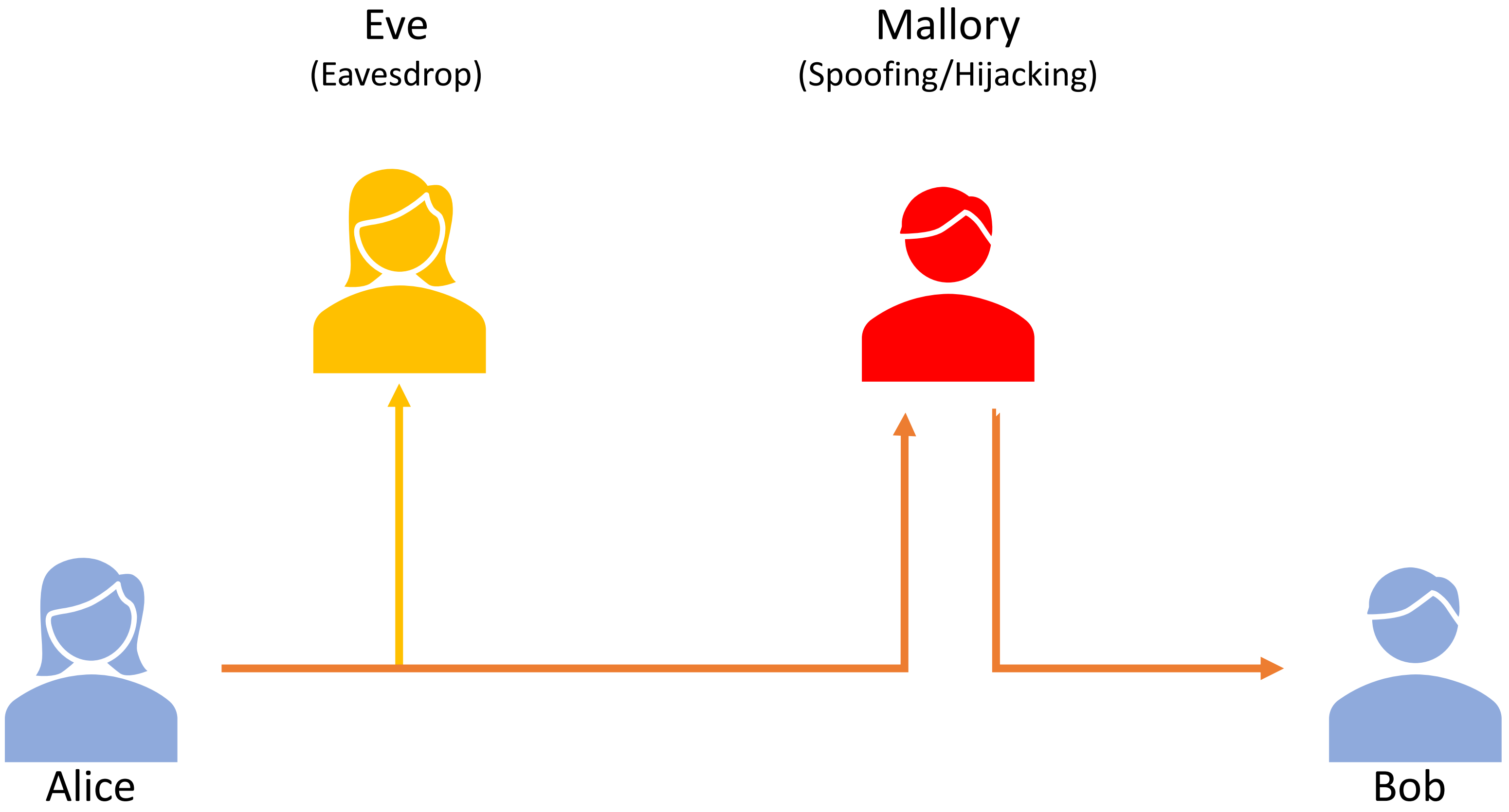
Rustam, Furqan & Mushtaq, Muhammad & Hamza, Ameer & Farooq, Shoaib & Jurcut, Anca & Ashraf, Imran. (2022). Denial of Service Attack Classification Using Machine Learning with Multi-Features. Electronics. 11. 3817. 10.3390/electronics11223817.

MiTM – Man in The Middle Attacks

- Attacker puts themselves in the **middle of two communicating parties**
  - Eavesdropping: attacker passivelly listens to traffic
  - Spoofing: attacker fakes responses to questions (e.g. DNS Spoofing)
  - Hijacking: attacker activelly mangles the communication
    - May steal data, inject packets or divert the communication
  - Using social engineering, misconfigurations or vulnerabilities

- Impact: CIA Triad is compromised
  - Communications not confidential
  - Communications payloads are manipulared/changed
  - Sessions are blocked or data is ommitted

MiTM – Man in The Middle Attacks



https://en.wikipedia.org/wiki/Alice_and_Bob

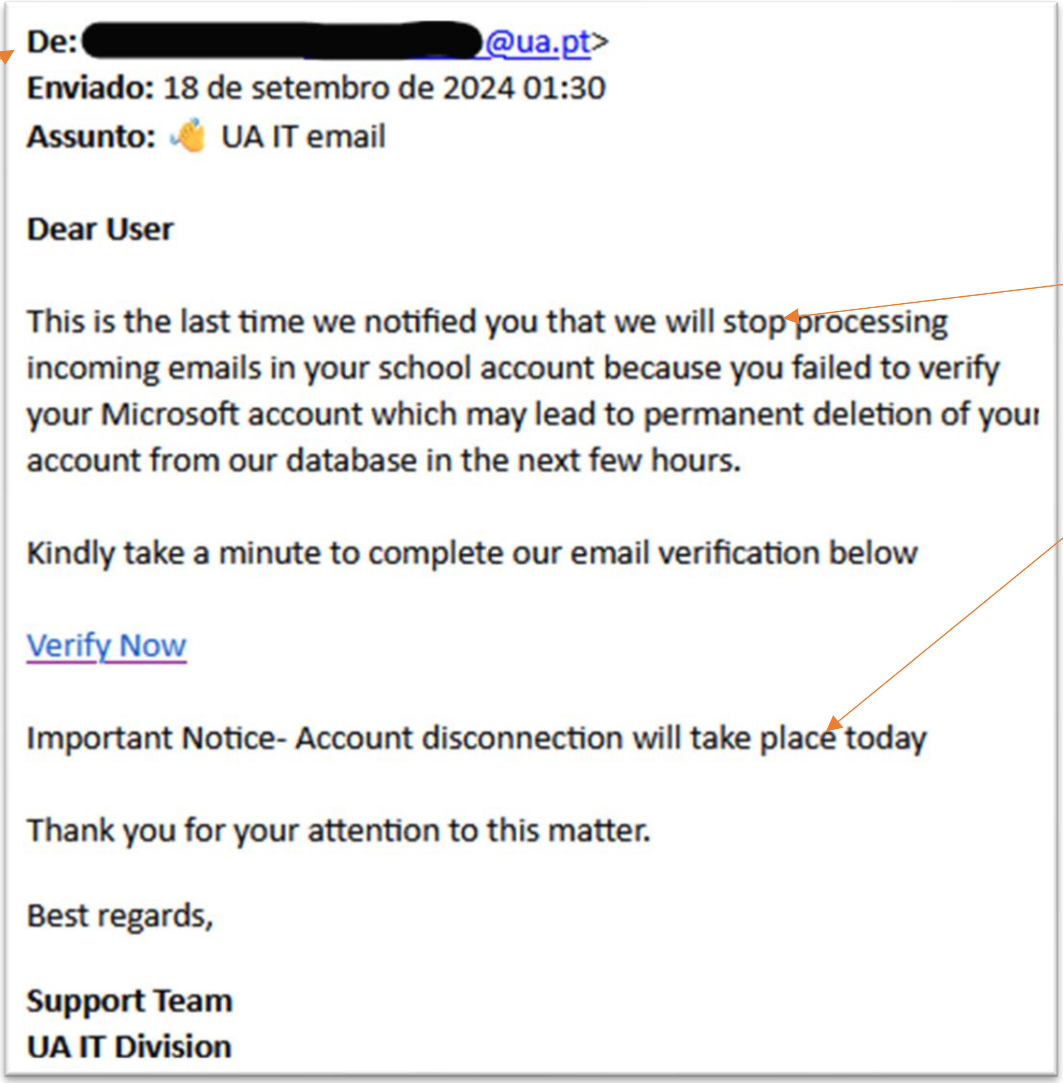
Phishing Attack

- Attacker uses fraudulent messages to trick victims
  - Objective: provide information, exposing, download malware, pay for something
  - Social Engineering attack exploring human vulnerabilities
  - Messages resort to urgency, fear, curiosity, authority, greed
  - Subtypes:
    - **Spear Phishing**: crafted to trick a specific person
    - **Whaling**: targets as executives, and high-net-worth individuals
    - **Smishing**: Uses SMS
    - **Vishing**: Uses phone calls

- Impact: Financial loss, damage to public image, compromise of other systems

Phishing Attack

Authority and trust



De: [redacted]@ua.pt>
Enviado: 18 de setembro de 2024 01:30
Assunto: 👋 UA IT email

Dear User

This is the last time we notified you that we will stop processing incoming emails in your school account because you failed to verify your Microsoft account which may lead to permanent deletion of your account from our database in the next few hours.

Kindly take a minute to complete our email verification below

Verify Now

Important Notice- Account disconnection will take place today

Thank you for your attention to this matter.

Best regards,

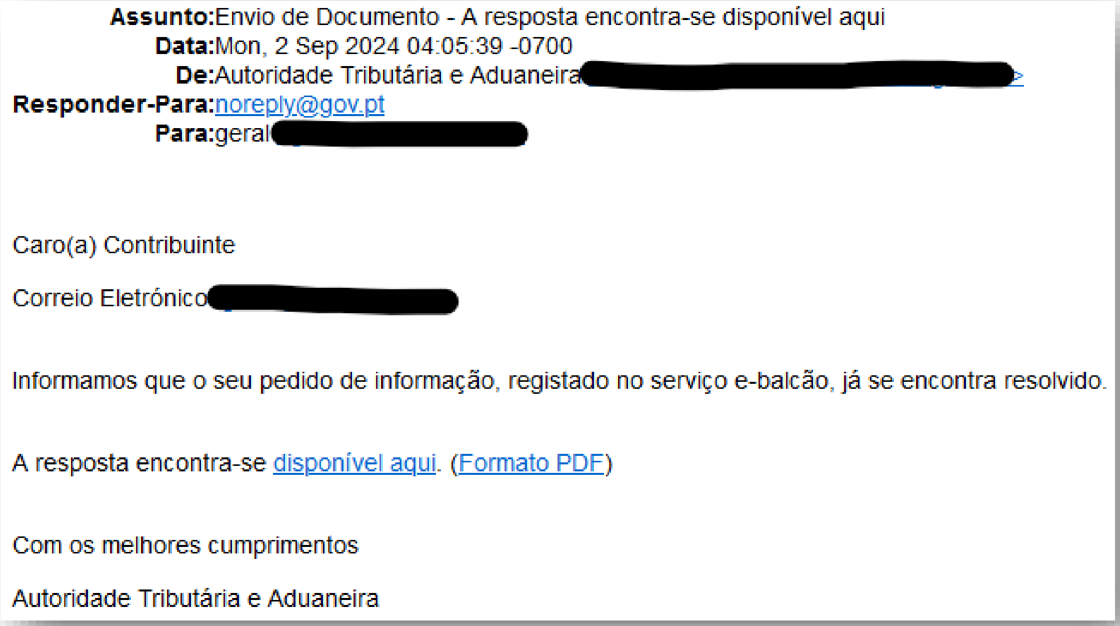
Support Team
UA IT Division

Urgency and fear

Malware

- Infect systems with malicious software
  - Using social engineering or **software vulnerabilities**
  - Variations:
    - Virus: Require some host to exist (binary file, document)
    - Worm: Isolated program that can run without others
    - Trojan: Disguised of another application (popular with keygens/cracks)

- Impact: Financial loss, information loss, compromise of other systems, participation in attacks



Assunto: Envio de Documento - A resposta encontra-se disponível aqui
Data: Mon, 2 Sep 2024 04:05:39 -0700
De: Autoridade Tributária e Aduaneira [redacted]
Responder-Para:noreply@gov.pt
Para:geral [redacted]

Caro(a) Contribuinte

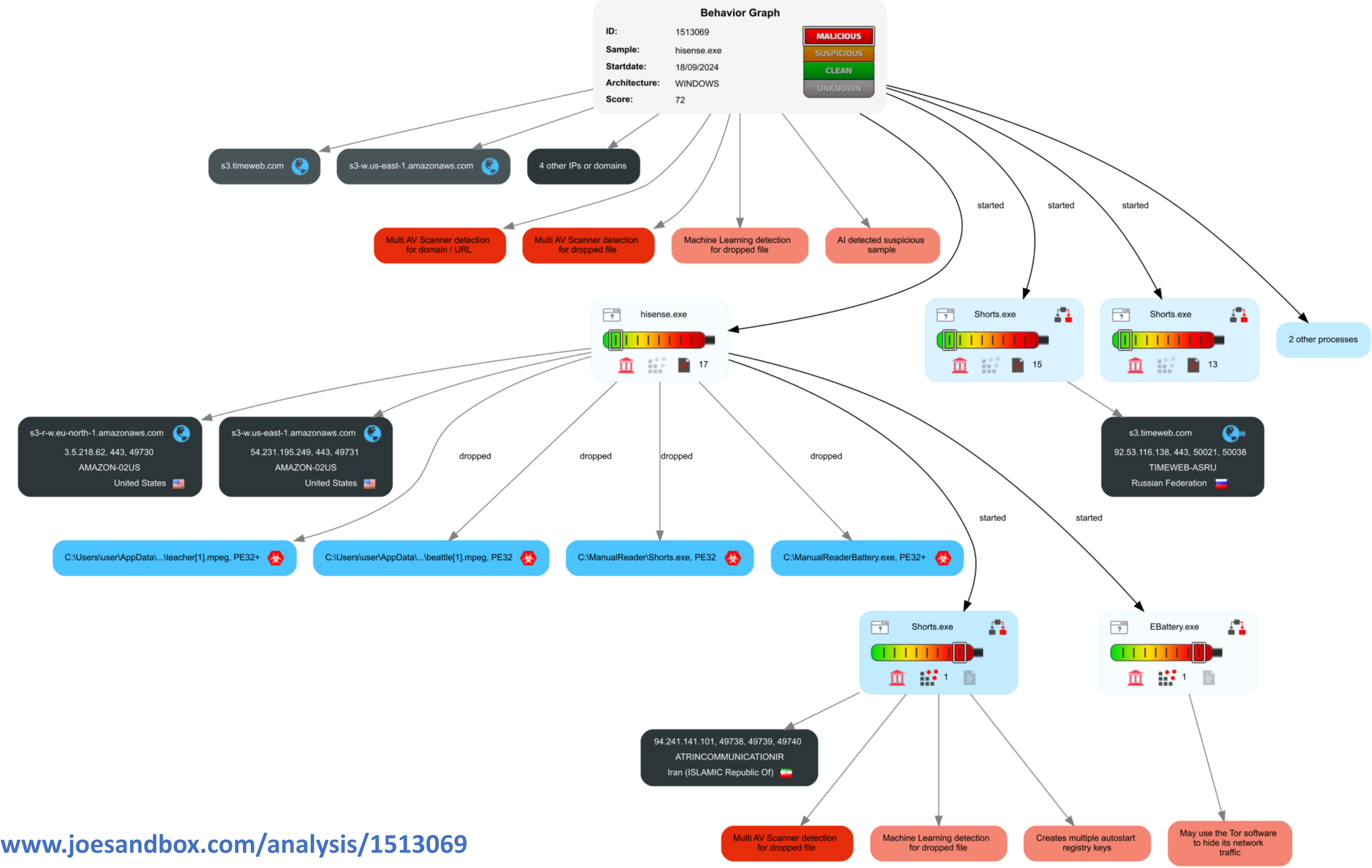
Correio Eletrónico [redacted]

Informamos que o seu pedido de informação, registado no serviço e-balcão, já se encontra resolvido.

A resposta encontra-se disponível aqui. (Formato PDF)

Com os melhores cumprimentos

Autoridade Tributária e Aduaneira



Behavior Graph

ID: 1513069

Sample: hisense.exe

Startdate: 18/09/2024

Architecture: WINDOWS

Score: 72

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN
s3.timeweb.com
s3-w.us-east-1.amazonaws.com
4 other IPs or domains
Multi AV Scanner detection for domain / URL
Multi AV Scanner detection for dropped file
Machine Learning detection for dropped file
AI detected suspicious sample
started
started
started
hisense.exe
17
Shorts.exe
15
Shorts.exe
13
2 other processes
s3-r-w.eu-north-1.amazonaws.com
3.5.218.62, 443, 49730
AMAZON-02US
United States
s3-w.us-east-1.amazonaws.com
54.231.195.249, 443, 49731
AMAZON-02US
United States
dropped
dropped
dropped
dropped
s3.timeweb.com
92.53.116.138, 443, 50021, 50038
TIMEWEB-ASRU
Russian Federation
started
started
C:\Users\user\AppData\...\teacher[1].mpeg, PE32+
C:\Users\user\AppData\...\beattle[1].mpeg, PE32
C:\ManualReader\Shorts.exe, PE32
C:\ManualReaderBattery.exe, PE32+
Shorts.exe
1
EBattery.exe
1
94.241.141.101, 49738, 49739, 49740
ATRINCOMMUNICATIONIR
Iran (ISLAMIC Republic Of)
Multi AV Scanner detection for dropped file
Machine Learning detection for dropped file
Creates multiple autostart registry keys
May use the Tor software to hide its network traffic

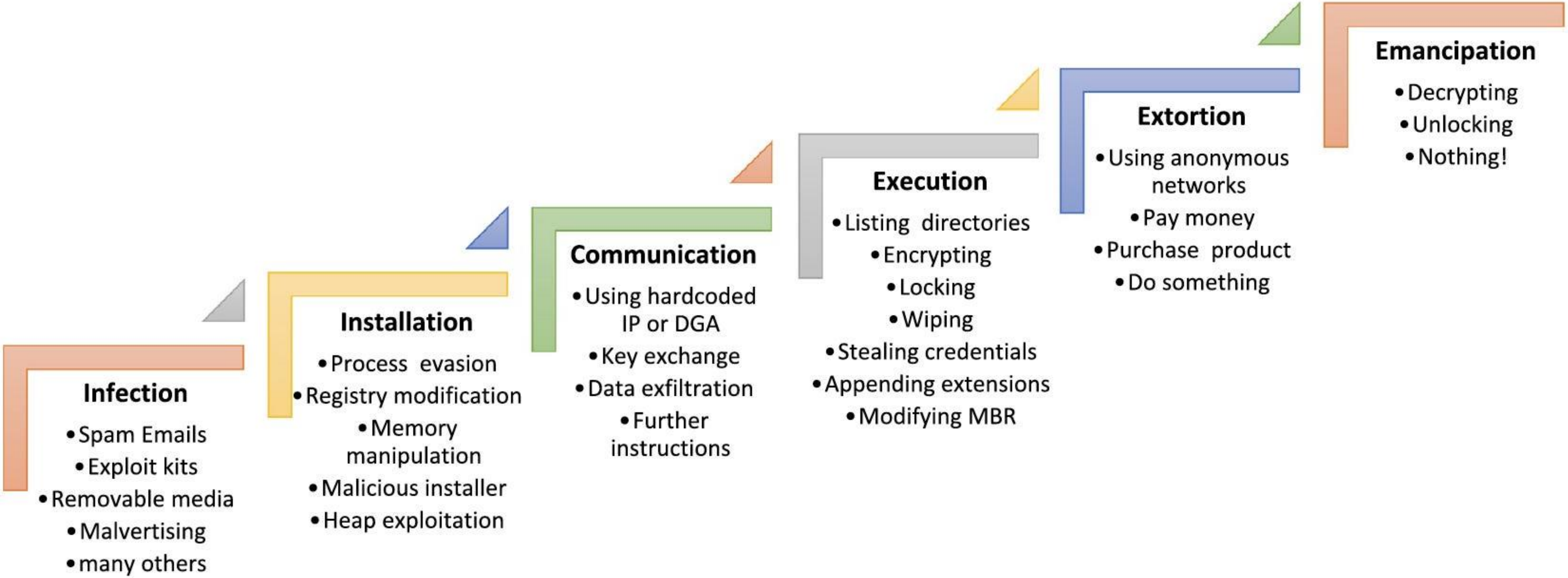
https://www.joesandbox.com/analysis/1513069

Ransomware

- Malware that blocks access to system until a ransom is paid
  - **Cryptoviral Extortion -** Encrypts user data and requests a ransom to release a key
  - Explores social engineering or **software vulnerabilities**
    - Social engineering such as phishing
    - Software vulnerabilities allow fast propagation across systems
  - Facilitated in systems with no defenses or perimeter defenses

- Impact: Denial of Resources, Data loss, Severe disruption
  - Considered as extremely dangerous as operations may be disrupted for a long time
  - Recovery will require Off Site Backups
    - Sometimes Backups with a WORM (Write Once, Read Many) strategy

Ransomware



Infection

- Spam Emails
- Exploit kits
- Removable media
- Malvertising
- many others

Installation

- Process evasion
- Registry modification
- Memory manipulation
- Malicious installer
- Heap exploitation

Communication

- Using hardcoded IP or DGA
- Key exchange
- Data exfiltration
- Further instructions

Execution

- Listing directories
- Encrypting
- Locking
- Wiping
- Stealing credentials
- Appending extensions
- Modifying MBR

Extortion

- Using anonymous networks
- Pay money
- Purchase product
- Do something

Emancipation

- Decrypting
- Unlocking
- Nothing!

Masoudeh Keshavarzi, Hamid Reza Ghaffary, I2CE3: A dedicated and separated attack chain for ransomware offenses as the most infamous cyber extortion, Computer Science Review, Volume 36, 2020, 100233, ISSN 1574-0137

Password

- Attacks targeting the discovery of passwords
  - Explore social behavior (password reuse) and **software vulnerabilities**
  - Note: Leaked passwords are compiled and distributed (see rockyou.txt)
  - Types:
    - Brute force: login attempts testing all possibilities
    - Dictionary attack: testing common words
    - Stuffing: testing leaked passwords
    - Spraying: testing the same user across multiple services
    - Keylogging: intercepting keys using malware
    - Rainbow table attack: optimized brute force of hashed passwords

- Impact: financial loss, system compromise, information loss, impersonation

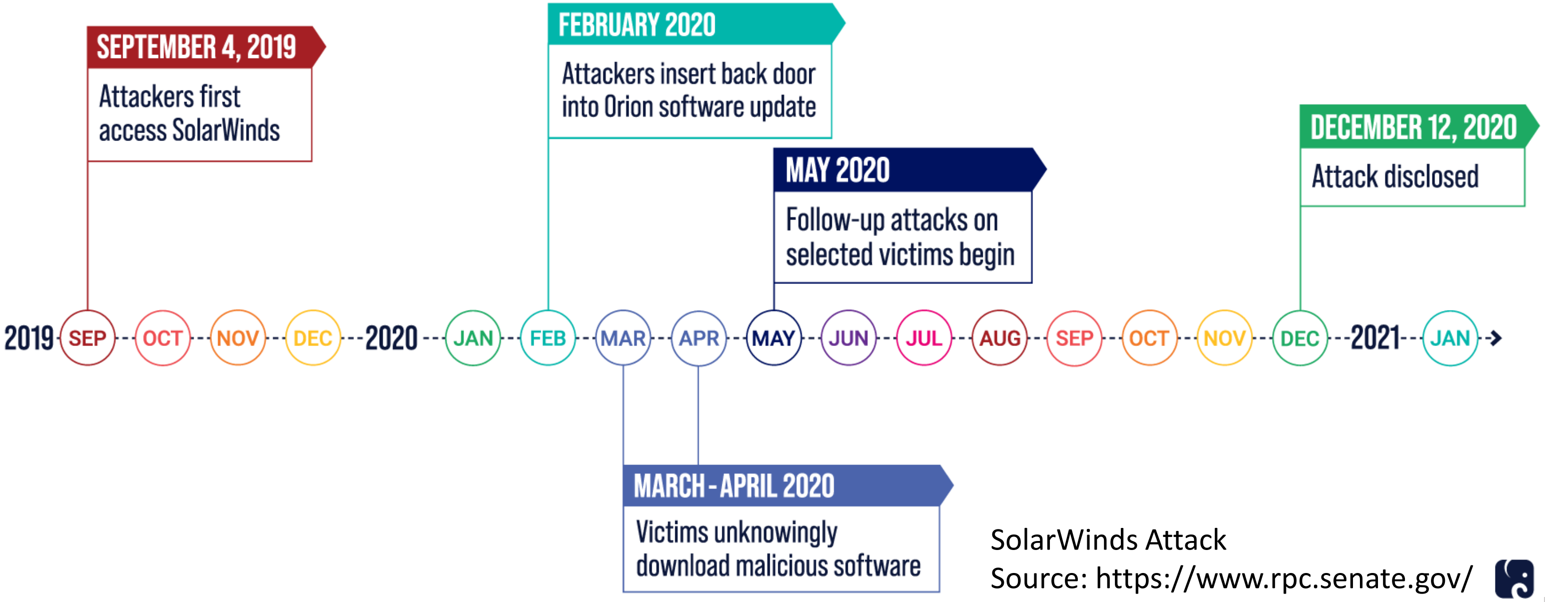
1. 123456
2. admin
3. 12345678
4. 123456789
5. 1234
6. 12345
7. password
8. 123
9. Aa123456
10. 1234567890
11. UNKNOWN
12. 1234567
13. 123123
14. 111111
15. Password
16. 12345678910
17. 000000
18. Admin123
19. ********
20. user

Most common passwords

Insider and Supplier Threats

- An insider that uses their authorized access or understanding of an organization to harm that organization
  - **Collaborators**: disgruntled, subverted or simply malicious
  - **Suppliers** or **contractors:** create a variant named: Supply Chain Attacks
  - Explore weaknesses in a Perimeter Defense Model
    - Insiders have wide access to resources (without monitoring?)
  - Can be used to escalate attack to **other organizations**
    - Compromising a software company will potentially compromise their clients

- Impact: Brand, Information, Total disruption



SEPTEMBER 4, 2019

Attackers first access SolarWinds

FEBRUARY 2020

Attackers insert back door into Orion software update

MARCH - APRIL 2020

Victims unknowingly download malicious software

MAY 2020

Follow-up attacks on selected victims begin

DECEMBER 12, 2020

Attack disclosed

SolarWinds Attack
Source: https://www.rpc.senate.gov/

Injection

- Exploration of a vulnerability allowing Injection of code into a program or query
  - Code is later executed in server or other clients
    - Code is an SQL statement, Javascript/python/bash/powershell/html/css code, Binary instructions…
  - Targets Databases, Web applications, binary applications…
  - Due to improper handling of untrusted data with is accepted and later used

- Impact: data loss, total system compromise
  - Specific technique: Remote Code Injection – System run new malicious code provided by the attacker

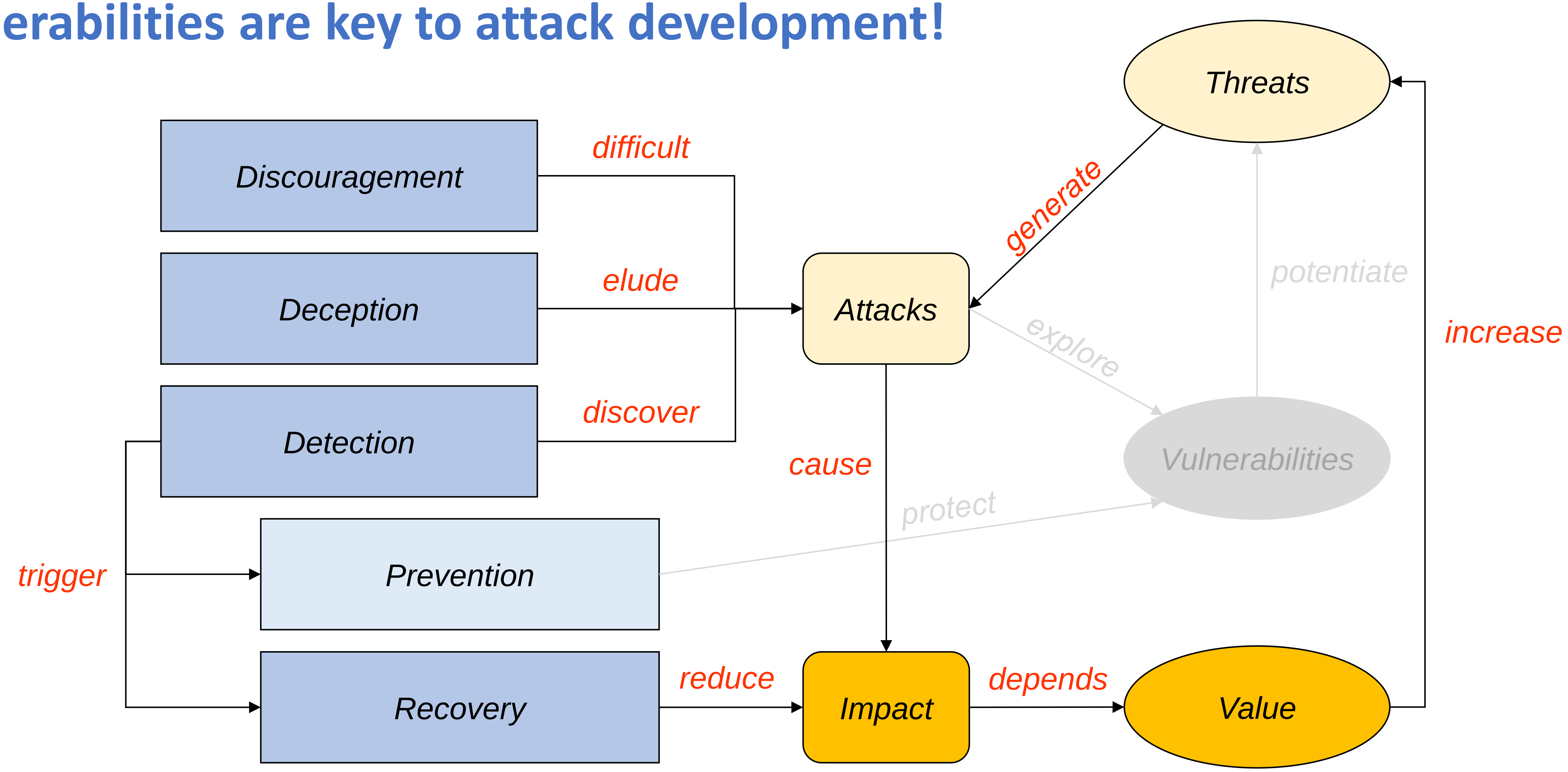
```
Query:  SELECT * FROM users WHERE username = “%u” AND pass=“%p”
Arguments: u=admin and p=qwerty
Result: SELECT * FROM users WHERE username = “admin” AND pass= “qwerty”

But if: u=admin and p=“ or 1=1 --
Result: SELECT * FROM users WHERE username = “admin” AND pass= ““ or 1=1 --”
```

Always true

Comment.
Ignores what follows

Information Security

Vulnerabilities are key to attack development!



Vulnerability tracking

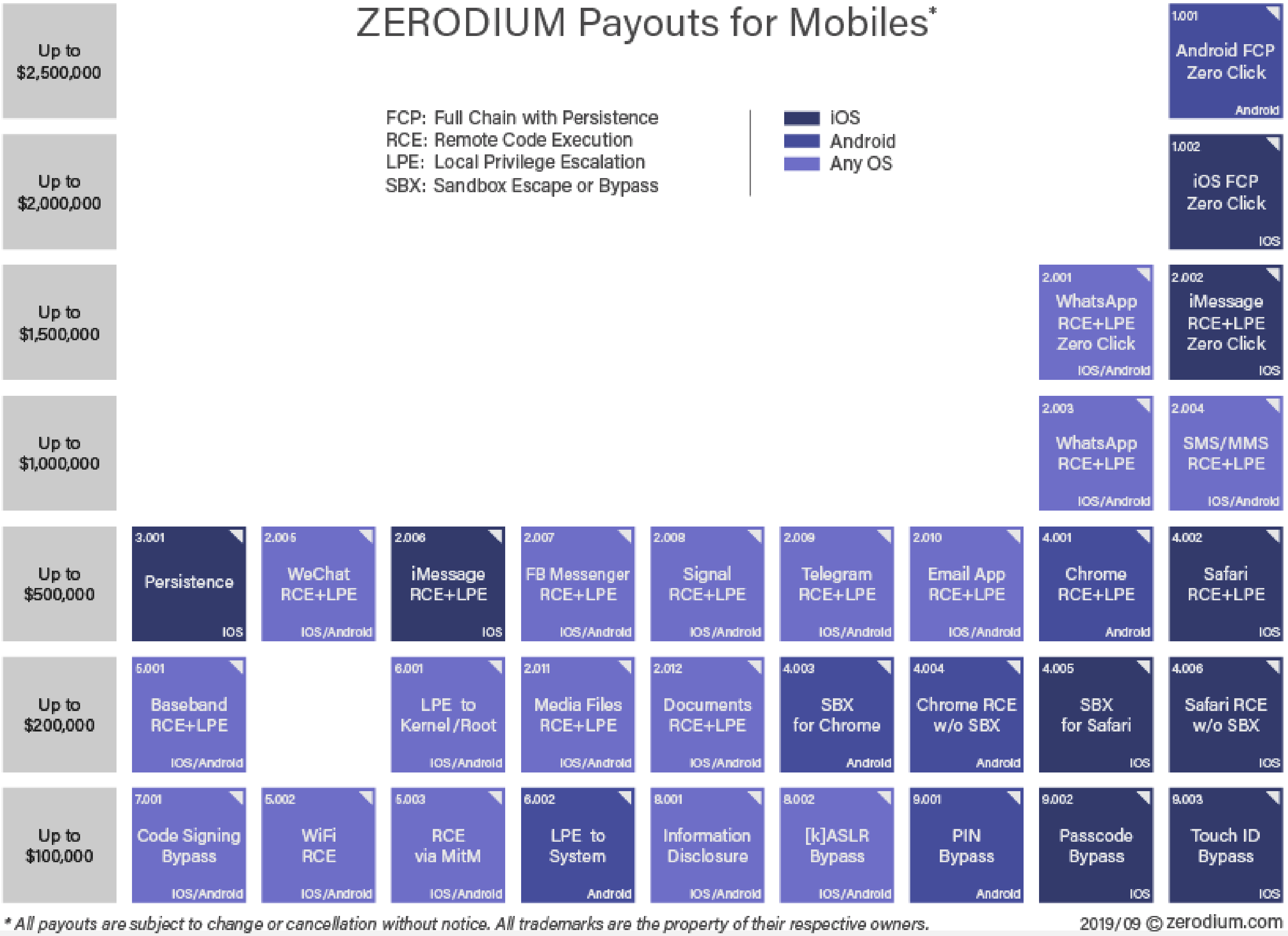
- During the development cycle, vulnerabilities are handled as bugs
  - May have been handled by a security team or not
  - May have a **security classification**, **priority** and **time to be handled**

- When software is available, vulnerabilities are **also tracked at a wider scale**
  - For every system and software publicly available

- Public tracking helps…
  - focusing the discussion around the **same issue**
    - Ex: a dependency that is used in multiple applications or distributions
  - defenders to easily **test their systems**, enhancing the security
  - (attackers to easily know what vulnerability can be used to a given system)

Vulnerability tracking

There is even a market



ZERODIUM Payouts for Mobiles*

FCP: Full Chain with Persistence
RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass

■ iOS
■ Android
■ Any OS

Up to $2,500,000									1.001 Android FCP Zero Click Android
Up to $2,000,000									1.002 iOS FCP Zero Click iOS
Up to $1,500,000								2.001 WhatsApp RCE+LPE Zero Click iOS/Android	2.002 iMessage RCE+LPE Zero Click iOS
Up to $1,000,000								2.003 WhatsApp RCE+LPE iOS/Android	2.004 SMS/MMS RCE+LPE iOS/Android
Up to $500,000	3.001 Persistence iOS	2.005 WeChat RCE+LPE iOS/Android	2.006 iMessage RCE+LPE iOS	2.007 FB Messenger RCE+LPE iOS/Android	2.008 Signal RCE+LPE iOS/Android	2.009 Telegram RCE+LPE iOS/Android	2.010 Email App RCE+LPE iOS/Android	4.001 Chrome RCE+LPE Android	4.002 Safari RCE+LPE iOS
Up to $200,000	5.001 Baseband RCE+LPE iOS/Android		6.001 LPE to Kernel/Root iOS/Android	2.011 Media Files RCE+LPE iOS/Android	2.012 Documents RCE+LPE iOS/Android	4.003 SBX for Chrome Android	4.004 Chrome RCE w/o SBX Android	4.005 SBX for Safari iOS	4.006 Safari RCE w/o SBX iOS
Up to $100,000	7.001 Code Signing Bypass iOS/Android	5.002 WiFi RCE iOS/Android	5.003 RCE via MitM iOS/Android	6.002 LPE to System Android	8.001 Information Disclosure iOS/Android	8.002 [k]ASLR Bypass iOS/Android	9.001 PIN Bypass Android	9.002 Passcode Bypass iOS	9.003 Touch ID Bypass iOS

** All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.*

2019/09 © zerodium.com

CVE - Common Vulnerabilities and Exposures

What it is

- Dictionary of **publicly known information security <u>vulnerabilities</u> and <u>exposures</u>**
  - For vulnerability management
  - For patch management
  - For vulnerability alerting
  - For intrusion detection

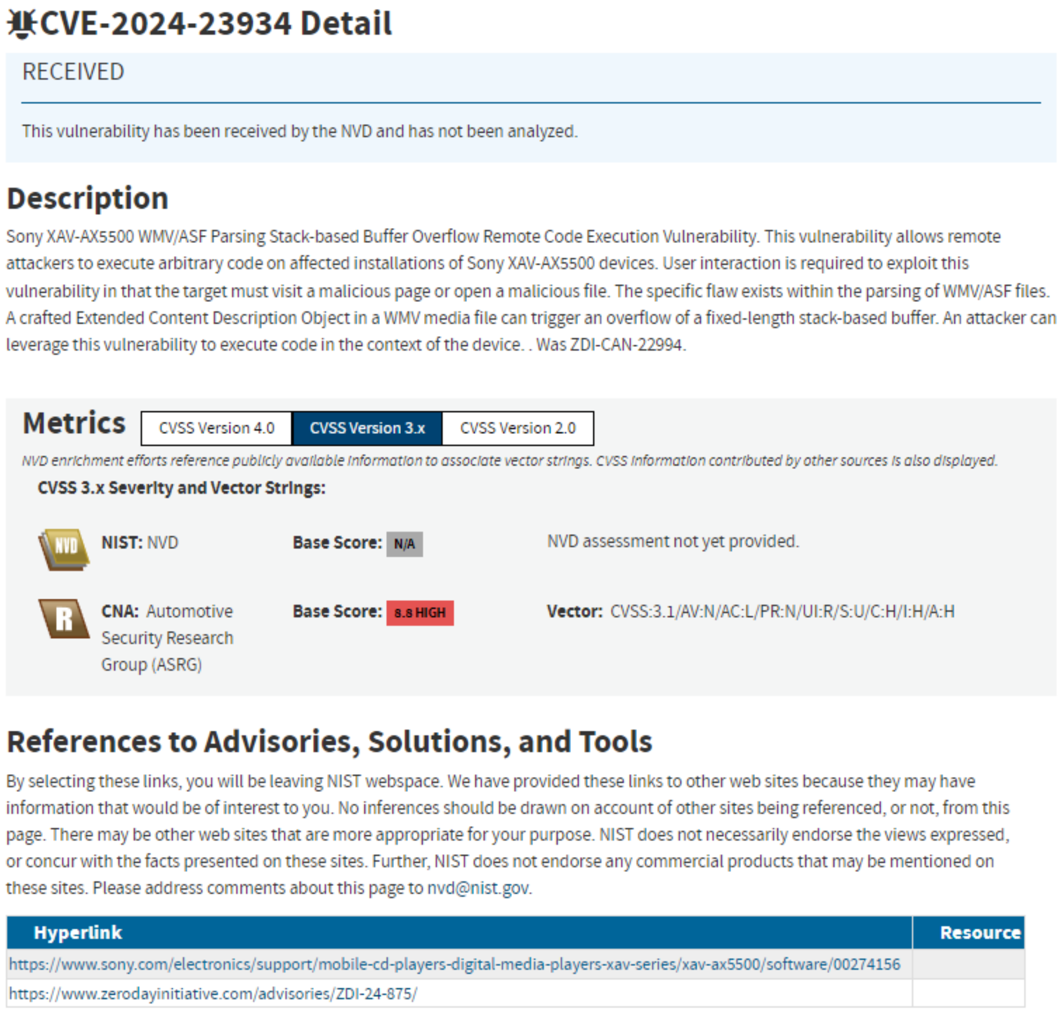
- Uses **common identifiers** for the same issue in given application (e.g: CVE-2024-1234)
  - Enable data exchange between security products
  - Provide a baseline index point for evaluating coverage of tools and services.
  - Details about a vulnerability can be kept private
  - Part of responsible disclosure: until owner provides a fix

CVE Identifiers

…aka CVE names, CVE numbers, CVE-IDs, CVEs

- Unique, common identifiers for publicly known information security vulnerabilities
  - Have "candidate" or "entry" status
  - Candidate: under review for inclusion in the list
  - Entry: accepted to the CVE List

- Format
  - CVE identifier number (CVE-Year-Order)
  - Status (Candidate or Entry)
  - Brief description of the vulnerability or exposure
  - References to extra information



CVE-2024-23934 Detail

RECEIVED

This vulnerability has been received by the NVD and has not been analyzed.

Description

Sony XAV-AX5500 WMV/ASF Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Sony XAV-AX5500 devices. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of WMV/ASF files. A crafted Extended Content Description Object in a WMV media file can trigger an overflow of a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the device. . Was ZDI-CAN-22994.

Metrics

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

NIST: NVD	**Base Score:** N/A	NVD assessment not yet provided.
CNA: Automotive Security Research Group (ASRG)	**Base Score:** 8.8 HIGH	**Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
https://www.sony.com/electronics/support/mobile-cd-players-digital-media-players-xav-series/xav-ax5500/software/00274156	
https://www.zerodayinitiative.com/advisories/ZDI-24-875/	

Definition: Vulnerability

A mistake in software that can be directly used by an attacker to gain access to a system or network

- A mistake is a vulnerability **if it allows an attacker to use it to violate a reasonable security policy for that system**
  - This excludes entirely "open" security policies in which all users are trusted, or where there is no consideration of risk to the system

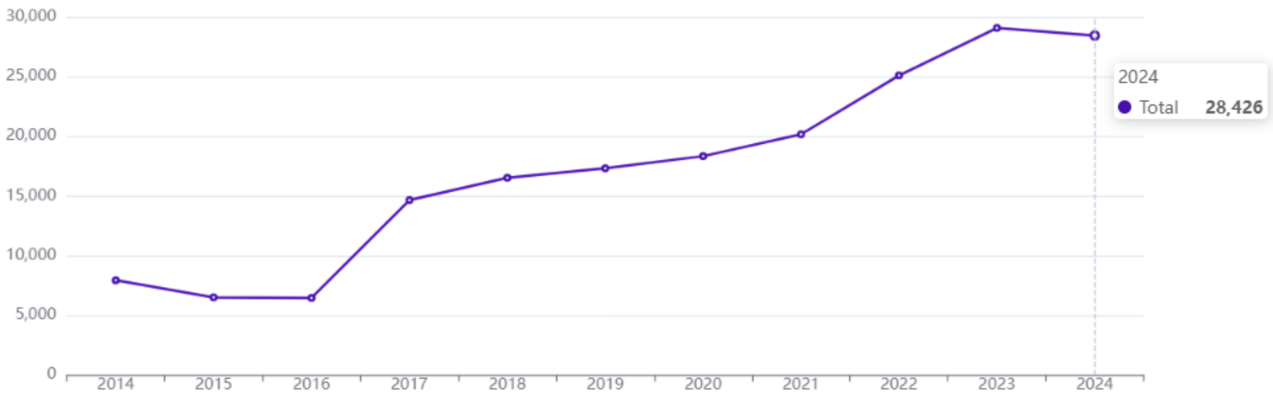
- A CVE vulnerability is a state in a computing system (or set of systems) that either:
  - Allows an attacker to execute commands as another user
  - Allows an attacker to access data that is contrary to the specified access restrictions for that data
  - Allows an attacker to pose as another entity
  - Allows an attacker to conduct a denial of service

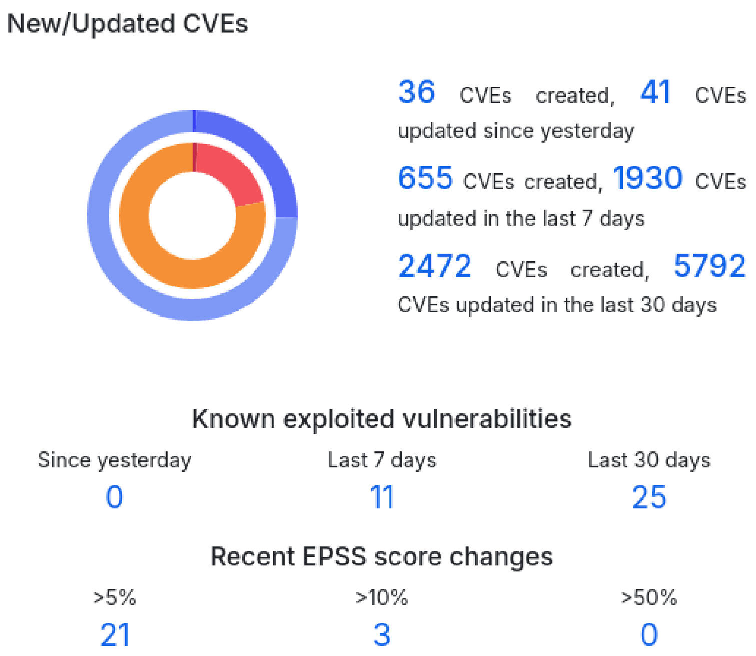
Definition: Exposure

A configuration issue or a mistake in software allowing access to information or capabilities used as a stepping-stone into a system or network

- A configuration issue or a mistake is an exposure **if it does not <u>directly</u> allow compromise**
  - But could be an important component of a successful attack, and is a violation of a reasonable security policy
- An exposure describes a state in a computing system (or set of systems) that is not a vulnerability, but either:
  - Allows an attacker to conduct information gathering activities
  - Allows an attacker to hide activities
  - Includes a capability that behaves as expected, but can be easily compromised
  - Is a primary point of entry that an attacker may attempt to use to gain access to the system or data
  - Is considered a problem by some reasonable security policy

CVE number statistics (from cvedetails.com)





New/Updated CVEs

36 CVEs created, 41 CVEs updated since yesterday

655 CVEs created, 1930 CVEs updated in the last 7 days

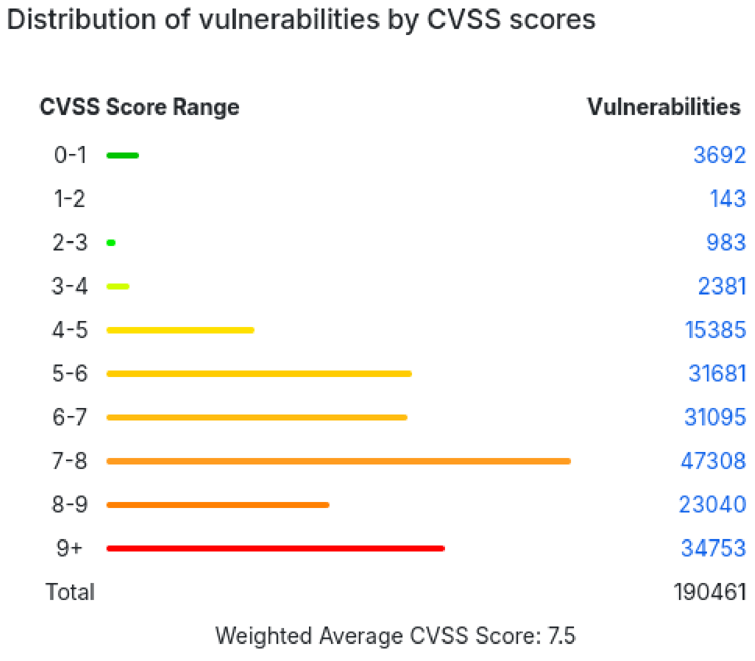
2472 CVEs created, 5792 CVEs updated in the last 30 days

Known exploited vulnerabilities

Since yesterday	Last 7 days	Last 30 days
0	11	25

Recent EPSS score changes

>5%	>10%	>50%
21	3	0



Distribution of vulnerabilities by CVSS scores

CVSS Score Range	Vulnerabilities
0-1	3692
1-2	143
2-3	983
3-4	2381
4-5	15385
5-6	31681
6-7	31095
7-8	47308
8-9	23040
9+	34753
Total	190461

Weighted Average CVSS Score: 7.5

Vulnerabilities and Software

- The number of vulnerabilities **always increases**
  - Even if it is solved for a given software, it is still present in older (non updated) versions
    - May be relevant in systems **without updates** or due to **downgrade attacks**

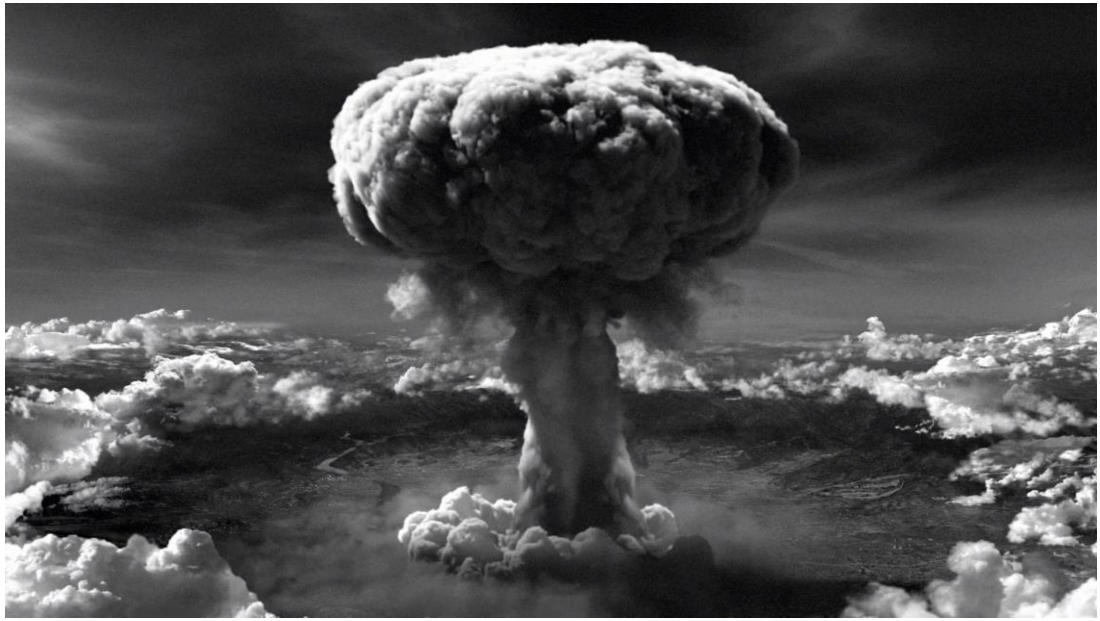
- Vulnerabilities are a **common aspect of software**
  - **They are not only bugs, as there is an impact!**
  - There should be a process to handle them
    - Vendors: track vulnerabilities and issue fixes to clients
    - Clients: be informed about vulnerabilities and apply updates
  - Not all vulnerabilities can be corrected.
    - Sometimes only the attack is mitigated (e.g. segmenting the network, or disabling a feature)

Zero Day (or Zero Hour) Attack/Threat

- Attack using vulnerabilities which are:
  - Unknown to others
  - Undisclosed to the software vendor

- Occurs **at the day zero** of the knowledge about those vulnerabilities
  - For which no security fix is available

- A single “day zero” may exist for months/years
  - Known to attackers, unknown to others
  - Frequently part of attack arsenal
  - Traded around in specific markets



Vulnerability Disclosure

- Disclosure of new vulnerabilities should be **coordinated** with the vendor
  - Typical Coordination:
    1. Describe vulnerability to vendor
    2. Vendor starts the correction process and agrees on a timeline
    3. Updates are issued and a CVE entry is created (Vulnerability is made public)
    4. Clients update the software, deploy protections or mitigate the impact
    5. The community discuss the root cause of the issue

- Vital to prevent Zero Day attacks
  - Clients will be (mostly) fixed when the vulnerability becomes public

- Requires collaboration from vendors

Vulnerability detection

- Specific tools can detect vulnerabilities
  - Exploiting **known vulnerabilities**
  - Testing known **vulnerability patterns**
    - e.g., buffer overflow, SQL injection, XSS, etc.

- Specific tools can replicate known attacks
  - Use **known exploits** for known vulnerabilities
    - e.g.: MS Samba v1 exploit used by WannaCry
  - Can be used to **implement countermeasures**

- It is vital to assert the robustness of production systems and applications
  - Auditing service often provided by third-party companies

Vulnerability detection

- Can be applied to:
  - Source code (static analysis)
    - OWASP LAPSE+, RIPS, Veracode, …
  - Running application (dynamic analysis)
    - Valgrind, Rational, AppScan, GCC, …
  - Externally as a remote client:
    - OpenVAS, Metasploit, …

- Should not be blindly applied to production systems!
  - Potential data loss/corruption
  - Potential DoS
  - Potential illegal activity

Vulnerability management

- Discussing and fixing vulnerabilities is important, yet insufficient
  - They will just keep appearing, non-stop

- Vital to discuss the **root mistake** of each vulnerability
  - So that it can be fixed**, preventing future vulnerabilities**

- Vulnerabilities exist because of **Anti-patterns**
  - Wrong or fragile implementation of logic structures
  - Which exist because of **lack of training, wrongly defined features, wrong design, wrong processes**…

Symptoms / Vulnerabilities

Mistakes / Anti-patterns

CWE - Common Weakness Enumeration

- **Common language** for **discussing, finding and dealing** with the **causes of software security vulnerabilities**
  - Found in code, design, or system architecture
  - Each individual CWE represents a single vulnerability type
  - Currently maintained by the MITRE Corporation
    - A detailed CWE list is currently available at the MITRE website
  - The list provides a detailed definition for each individual CWE

- Individual CWEs are held within a hierarchical structure
  - CWEs at higher levels provide a broad overview of a vulnerability type
    - Can have many children CWEs associated with them
  - CWEs at deeper levels provide a finer granularity
    - Usually have fewer or no children CWEs

Symptoms / Vulnerabilities
Represented as CVE

Mistakes / Anti-patterns
Represented as CWE

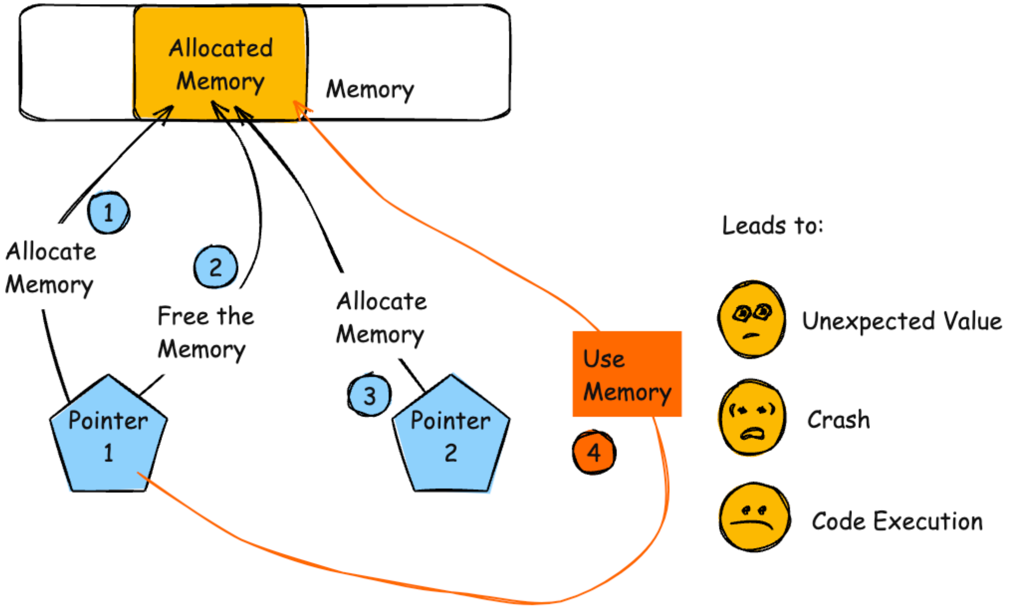
CWE-416: Use After Free

https://cwe.mitre.org/data/definitions/416.html

- The product **reuses or references memory after it has been freed**.
  - At some point afterward, the memory may be allocated again and saved in another pointer, while the original pointer references a location somewhere within the new allocation. Any operations using the original pointer are no longer valid because the memory "belongs" to the code that operates on the new pointer.

- Mitigation Phase: Architecture and Design Strategy:
  - **Language Selection**: Choose a language that provides automatic meme management.

- Mitigation Phase: Implementation Strategy:
  - **Attack Surface Reduction**: When freeing pointers, be sure to set them to NULL once they are freed. However, the utilization of multiple or complex data structures may lower the usefulness of this strategy.
  - **Effectiveness**: Defense in Depth



Note: check the URL to see the parent CWEs and associated CVEs

OWASP Top 10

10 most common vulnerability types found in real systems

- Reviewed **every 4 years** from real world security assessments
  - 2025 Edition being prepared now!
- Each type contains multiple CWEs to be prevented
- Industry can focus on the most common problems
  - Improve training, testing and awareness on this areas
  - Improve toolkits, languages and frameworks
  - Create detection and defenses against typical vulnerabilities

A01 Broken Access Control

A02 Cryptographic Failures

A03 Injection

A04 Insecure Design

A05 Security Misconfiguration

A06 Vulnerable and Outdated Components

A07 Identification and Authentication Failures

A08 Software and Data Integrity Failures

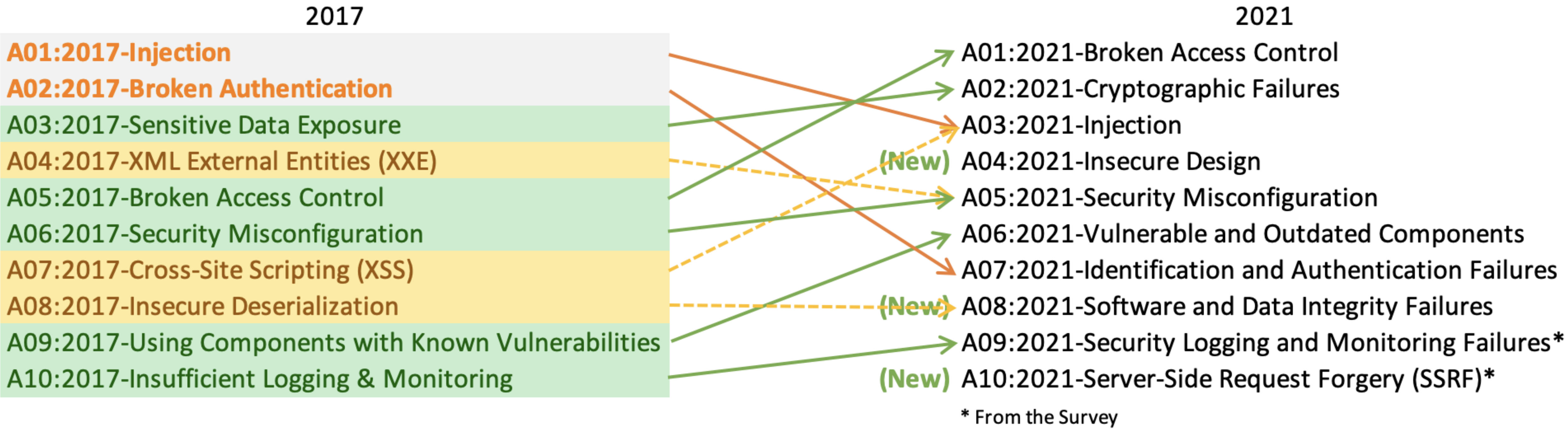
A09 Security Logging and Monitoring Failures

A10 Server Side Request Forgery (SSRF)

https://owasp.org/Top10/

OWASP Top 10

Popular mistakes are prevented, while other arise



2017

- A01:2017-Injection
- A02:2017-Broken Authentication
- A03:2017-Sensitive Data Exposure
- A04:2017-XML External Entities (XXE)
- A05:2017-Broken Access Control
- A06:2017-Security Misconfiguration
- A07:2017-Cross-Site Scripting (XSS)
- A08:2017-Insecure Deserialization
- A09:2017-Using Components with Known Vulnerabilities
- A10:2017-Insufficient Logging & Monitoring

2021

- A01:2021-Broken Access Control
- A02:2021-Cryptographic Failures
- A03:2021-Injection
- (New) A04:2021-Insecure Design
- A05:2021-Security Misconfiguration
- A06:2021-Vulnerable and Outdated Components
- A07:2021-Identification and Authentication Failures
- (New) A08:2021-Software and Data Integrity Failures
- A09:2021-Security Logging and Monitoring Failures*
- (New) A10:2021-Server-Side Request Forgery (SSRF)*

* From the Survey

https://owasp.org/Top10/