[Hello Security]

PITRADWAR WGUiSW

0x03 Stay safe, realistically

Krystian Bajno, 2024

_baycode.eu

[Table of Contents]

0x03 Stay safe, realistically

0x04 Whoami

0x05 What could happen to me?

0x06 MITRE – the actual techniques

0x07 Web Application Security

0x08 Network Security

0x09 Authentication anatomy

0x0A Proper password policy

0x0B Cyber Threat Intelligence

0x0C Open Source Intelligence

0x0D VPNs don’t make you totally anon

0x0E AVs will not save the day

0x0F Falling into a rabbit hole

0x10 Q&A

0x11 Thank you

[Links are clickable]

[Links]

https://d3fend.mitre.org

https://attack.mitre.org

https://owasp.org/Top10/

https://portswigger.net/web-security

https://owasp.org/www-project-web-security-testing-guide/

https://pages.nist.gov/800-63-3/sp800-63b.html

https://haveibeenpwned.com

https://cert.pl/hasla

https://www.nomoreransom.org/pl/index.html

https://map.snapchat.com/

https://www.osintdojo.com/diagrams/main

https://github.com/jivoi/awesome-osint

https://maldevacademy.com/

https://www.fortinet.com/resources/cyberglossary/defense-in-depth

0x04 Whoami

Krystian Bajno

Cyber Security Specialist
Penetration Tester

Full-Stack Software Engineer
Backend, Frontend, Mobile

Comp. Sci. I – Cloud Computing Technology

Comp. Sci. II - Cloud Computing Architecture and Security

0x05 What could happen to me?

🛡️ *CIA Triad – anatomy of a cyber attack*

🤫 *Confidentiality*

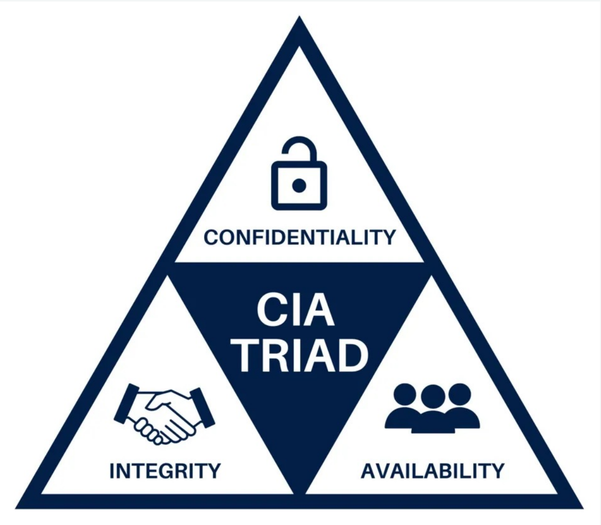
- ***Sensitive information disclosure***
- Data breaches
- Data interception
- Intelligence gathering
- Insider threats
- Physical theft
- Social engineering
- System compromise

✏️ *Integrity*

- ***Modification / creation / deletion of data***
- Fraud
- Disinformation
- Forgery
- Identity theft
- Social Engineering
- Ransomware
- System compromise

➡️ *Availability*

- Anything ***denying an access to a resource***
- Crashes, glitches, overloads
- Power outages
- System compromise



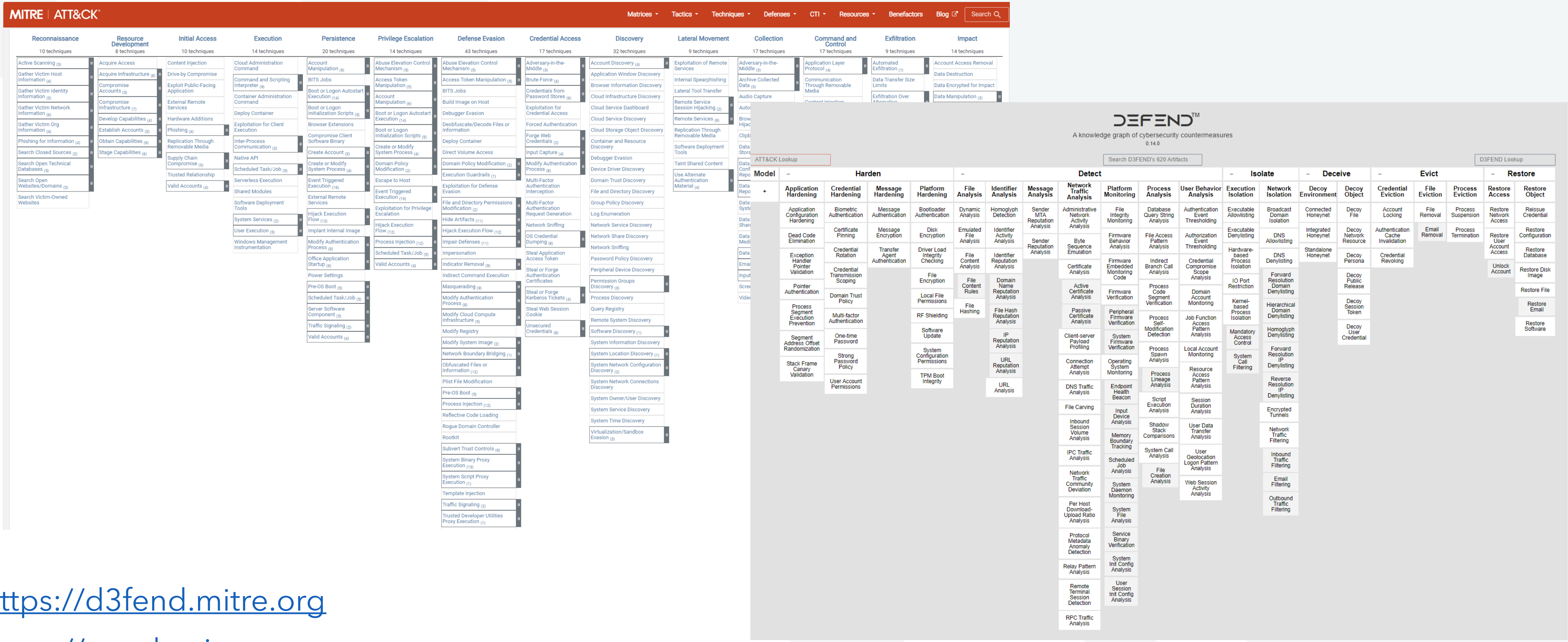
Functionality vs Security principle

[Hello Security]

PITRADWAR WGUiSW _baycode.eu

0x06 MITRE – the actual techniques

🍒 *ATT&CK, D3FEND*



MITRE | ATT&CK®

Matrices ▾ Tactics ▾ Techniques ▾ Defenses ▾ CTI ▾ Resources ▾ Benefactors Blog Search

Reconnaissance – 10 techniques
- Active Scanning (3)
- Gather Victim Host Information (4)
- Gather Victim Identity Information (3)
- Gather Victim Network Information (6)
- Gather Victim Org Information (4)
- Phishing for Information (4)
- Search Closed Sources (2)
- Search Open Technical Databases (5)
- Search Open Websites/Domains (3)
- Search Victim-Owned Websites

Resource Development – 8 techniques
- Acquire Access
- Acquire Infrastructure (8)
- Compromise Accounts (3)
- Compromise Infrastructure (7)
- Develop Capabilities (4)
- Establish Accounts (3)
- Obtain Capabilities (6)
- Stage Capabilities (6)

Initial Access – 10 techniques
- Content Injection
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (4)
- Replication Through Removable Media
- Supply Chain Compromise (3)
- Trusted Relationship
- Valid Accounts (4)

Execution – 14 techniques
- Cloud Administration Command
- Command and Scripting Interpreter (9)
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (3)
- Native API
- Scheduled Task/Job (5)
- Serverless Execution
- Shared Modules
- Software Deployment Tools
- System Services (2)
- User Execution (3)
- Windows Management Instrumentation

Persistence – 20 techniques
- Account Manipulation (6)
- BITS Jobs
- Boot or Logon Autostart Execution (14)
- Boot or Logon Initialization Scripts (5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (3)
- Create or Modify System Process (4)
- Event Triggered Execution (16)
- External Remote Services
- Hijack Execution Flow (12)
- Implant Internal Image
- Modify Authentication Process (8)
- Office Application Startup (6)
- Power Settings
- Pre-OS Boot (5)
- Scheduled Task/Job (5)
- Server Software Component (5)
- Traffic Signaling (2)
- Valid Accounts (4)

Privilege Escalation – 14 techniques
- Abuse Elevation Control Mechanism (5)
- Access Token Manipulation (5)
- Account Manipulation (6)
- Boot or Logon Autostart Execution (14)
- Boot or Logon Initialization Scripts (5)
- Create or Modify System Process (4)
- Domain Policy Modification (2)
- Escape to Host
- Event Triggered Execution (16)
- Exploitation for Privilege Escalation
- Hijack Execution Flow (12)
- Process Injection (12)
- Scheduled Task/Job (5)
- Valid Accounts (4)

Defense Evasion – 43 techniques
- Abuse Elevation Control Mechanism (5)
- Access Token Manipulation (5)
- BITS Jobs
- Build Image on Host
- Debugger Evasion
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain Policy Modification (2)
- Execution Guardrails (1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (2)
- Hide Artifacts (11)
- Hijack Execution Flow (12)
- Impair Defenses (11)
- Impersonation
- Indicator Removal (9)
- Indirect Command Execution
- Masquerading (9)
- Modify Authentication Process (8)
- Modify Cloud Compute Infrastructure (5)
- Modify Registry
- Modify System Image (2)
- Network Boundary Bridging (1)
- Obfuscated Files or Information (12)
- Plist File Modification
- Pre-OS Boot (5)
- Process Injection (12)
- Reflective Code Loading
- Rogue Domain Controller
- Rootkit
- Subvert Trust Controls (6)
- System Binary Proxy Execution (13)
- System Script Proxy Execution (1)
- Template Injection
- Traffic Signaling (2)
- Trusted Developer Utilities Proxy Execution (1)

Credential Access – 17 techniques
- Adversary-in-the-Middle (3)
- Brute Force (4)
- Credentials from Password Stores (6)
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (2)
- Input Capture (4)
- Modify Authentication Process (8)
- Multi-Factor Authentication Interception
- Multi-Factor Authentication Request Generation
- Network Sniffing
- OS Credential Dumping (8)
- Steal Application Access Token
- Steal or Forge Authentication Certificates
- Steal or Forge Kerberos Tickets (4)
- Steal Web Session Cookie
- Unsecured Credentials (8)

Discovery – 32 techniques
- Account Discovery (4)
- Application Window Discovery
- Browser Information Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion
- Device Driver Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Group Policy Discovery
- Log Enumeration
- Network Service Discovery
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery (3)
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery (1)
- System Information Discovery
- System Location Discovery (1)
- System Network Configuration Discovery (2)
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery
- Virtualization/Sandbox Evasion (3)

Lateral Movement – 9 techniques
- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (2)
- Remote Services (8)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (4)

Collection – 17 techniques
- Adversary-in-the-Middle (3)
- Archive Collected Data (3)
- Audio Capture
- Auto
- Brow Hijac
- Clipb
- Data Stora
- Data Confi Repo
- Data Repo
- Data Syste
- Data Share
- Data Medi
- Data
- Emai
- Input
- Scree
- Vide

Command and Control – 17 techniques
- Application Layer Protocol (4)
- Communication Through Removable Media
- Content Injection

Exfiltration – 9 techniques
- Automated Exfiltration (1)
- Data Transfer Size Limits
- Exfiltration Over Alternative

Impact – 14 techniques
- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation (3)

D3FEND™

A knowledge graph of cybersecurity countermeasures

0.14.0

ATT&CK Lookup | Search D3FEND's 620 Artifacts | D3FEND Lookup

Model +

– Harden

- **Application Hardening**: Application Configuration Hardening; Dead Code Elimination; Exception Handler Pointer Validation; Pointer Authentication; Process Segment Execution Prevention; Segment Address Offset Randomization; Stack Frame Canary Validation
- **Credential Hardening**: Biometric Authentication; Certificate Pinning; Credential Rotation; Credential Transmission Scoping; Domain Trust Policy; Multi-factor Authentication; One-time Password; Strong Password Policy; User Account Permissions
- **Message Hardening**: Message Authentication; Message Encryption; Transfer Agent Authentication
- **Platform Hardening**: Bootloader Authentication; Disk Encryption; Driver Load Integrity Checking; File Encryption; Local File Permissions; RF Shielding; Software Update; System Configuration Permissions; TPM Boot Integrity

– Detect

- **File Analysis**: Dynamic Analysis; Emulated File Analysis; File Content Analysis; File Content Rules; File Hashing
- **Identifier Analysis**: Homoglyph Detection; Identifier Activity Analysis; Identifier Reputation Analysis; Domain Name Reputation Analysis; File Hash Reputation Analysis; IP Reputation Analysis; URL Reputation Analysis; URL Analysis
- **Message Analysis**: Sender MTA Reputation Analysis; Sender Reputation Analysis
- **Network Traffic Analysis**: Administrative Network Activity Analysis; Byte Sequence Emulation; Certificate Analysis; Active Certificate Analysis; Passive Certificate Analysis; Client-server Payload Profiling; Connection Attempt Analysis; DNS Traffic Analysis; File Carving; Inbound Session Volume Analysis; IPC Traffic Analysis; Network Traffic Community Deviation; Per Host Download-Upload Ratio Analysis; Protocol Metadata Anomaly Detection; Relay Pattern Analysis; Remote Terminal Session Detection; RPC Traffic Analysis
- **Platform Monitoring**: File Integrity Monitoring; Firmware Behavior Analysis; Firmware Embedded Monitoring Code; Firmware Verification; Peripheral Firmware Verification; System Firmware Verification; Operating System Monitoring; Endpoint Health Beacon; Input Device Analysis; Memory Boundary Tracking; Scheduled Job Analysis; System Daemon Monitoring; System File Analysis; Service Binary Verification; System Init Config Analysis; User Session Init Config Analysis
- **Process Analysis**: Database Query String Analysis; File Access Pattern Analysis; Indirect Branch Call Analysis; Process Code Segment Verification; Process Self-Modification Detection; Process Spawn Analysis; Process Lineage Analysis; Script Execution Analysis; Shadow Stack Comparisons; System Call Analysis; File Creation Analysis
- **User Behavior Analysis**: Authentication Event Thresholding; Authorization Event Thresholding; Credential Compromise Scope Analysis; Domain Account Monitoring; Job Function Access Pattern Analysis; Local Account Monitoring; Resource Access Pattern Analysis; Session Duration Analysis; User Data Transfer Analysis; User Geolocation Logon Pattern Analysis; Web Session Activity Analysis

– Isolate

- **Execution Isolation**: Executable Allowlisting; Executable Denylisting; Hardware-based Process Isolation; IO Port Restriction; Kernel-based Process Isolation; Mandatory Access Control; System Call Filtering
- **Network Isolation**: Broadcast Domain Isolation; DNS Allowlisting; DNS Denylisting; Forward Resolution Domain Denylisting; Hierarchical Domain Denylisting; Homoglyph Denylisting; Forward Resolution IP Denylisting; Reverse Resolution IP Denylisting; Encrypted Tunnels; Network Traffic Filtering; Inbound Traffic Filtering; Email Filtering; Outbound Traffic Filtering

– Deceive

- **Decoy Environment**: Connected Honeynet; Integrated Honeynet; Standalone Honeynet
- **Decoy Object**: Decoy File; Decoy Network Resource; Decoy Persona; Decoy Public Release; Decoy Session Token; Decoy User Credential

– Evict

- **Credential Eviction**: Account Locking; Authentication Cache Invalidation; Credential Revoking
- **File Eviction**: File Removal; Email Removal
- **Process Eviction**: Process Suspension; Process Termination

– Restore

- **Restore Access**: Restore Network Access; Restore User Account Access; Unlock Account
- **Restore Object**: Reissue Credential; Restore Configuration; Restore Database; Restore Disk Image; Restore File; Restore Email; Restore Software

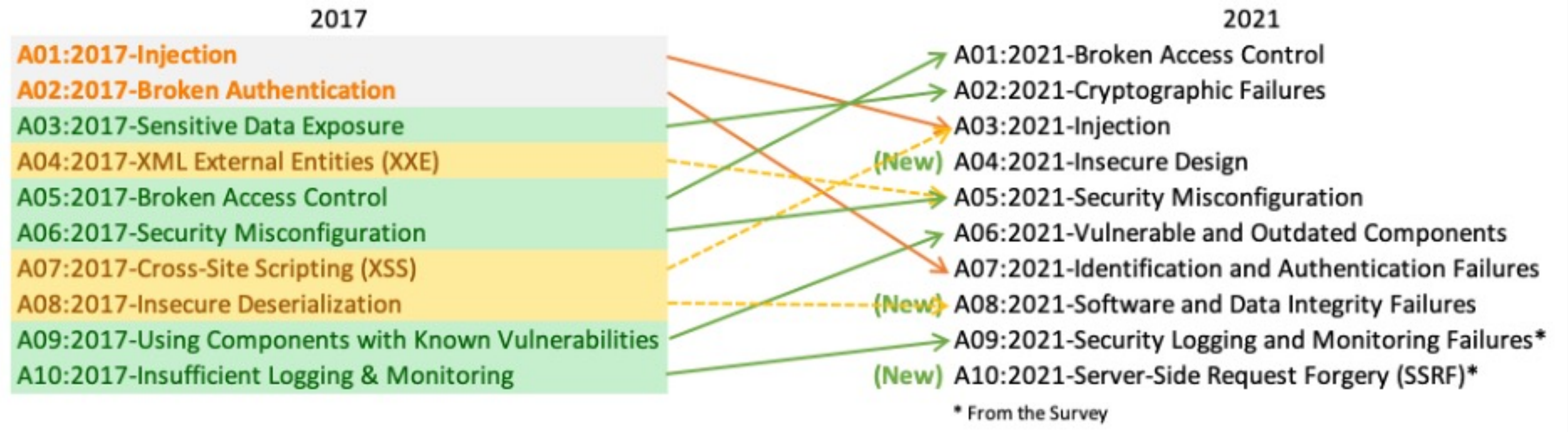
https://d3fend.mitre.org

https://attack.mitre.org

0x07 Web Application Security

👾 Your trust, in others hands

Database breaches may expose your credentials



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/

https://portswigger.net/web-security

https://owasp.org/www-project-web-security-testing-guide/

Credential leaks are not your fault.

0x08 Network Security

👾 Intruders on their way

Phishing is the most common external, initial access vector.

Windows systems are insecure by default – hardening and monitoring is important.

Segment your networks.

Example:

1. The IPv6 is preferred over IPv4, but no-one controls it.
2. If no one controls the IPv6, then who is able to lease DHCPv6 IP’s and become the DNS Man in the Middle controller?
3. Relay the creds over LDAP in order to create a delegated machine account.
4. ***Compromise the whole network***

Credential leaks are not your fault.

0x09 Authentication anatomy

🙋‍♂️ I am, I know, I have - the identity principle

Standard good old passwords

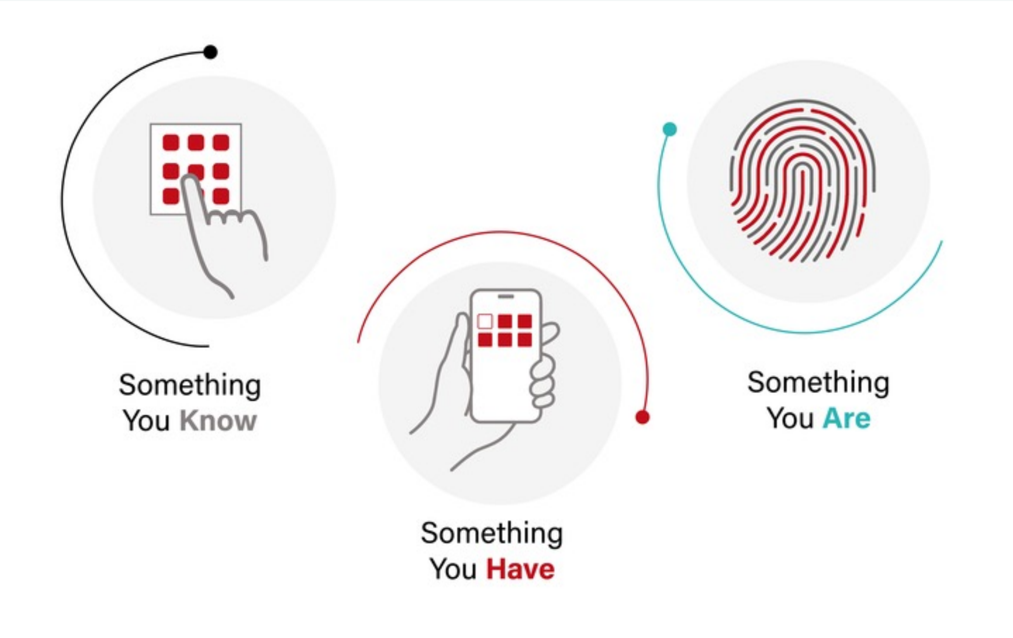
Multi Factor Authentication

- SMS – GSM based – *not really secure*
- Apps – crypto based (Authy, Microsoft Authenticator)
- Bio-authentication

Passwordless

- One Time Passwords
- Certificate-based authentication
- FIDO, U2F

https://www.cloudradius.com/secure-authentication-without-multi-factor-authentication-mfa/



But how FIDO's really work?

0x0A Proper password policy

⭐ Yes, your credentials will be found.

- **A good password consists of a sentence.**
- It should not contain dates, names, companies, cities and combinations of them.
- Use the quotes as an inspiration, not as an actual password.
- **Do not store credentials in plaintext on your desktop.**
- **Old e-mails may be able to reset your account passwords.**

Change your passwords regularly and ***avoid reusing them***.

Do not use passwords with less than 12 characters. The longer the better.

The recommendation is to use longer passwords instead of special characters.

Use password management solutions, especially PAM's.

Bad password examples:

- Apple1!
- zaq1@WSX
- amelka123
- Marzec2024
- Cze$tochowice123432!

Good password examples:

- zielonyParkingDla3malychSamolotow
- DwaBialeLatajaceSophisticatedKroliki
- KrukiLasery$DzikiJenoty2Rowery3Bajery
- DlazlKostekNaMostek/I$tuka

https://cert.pl/hasla

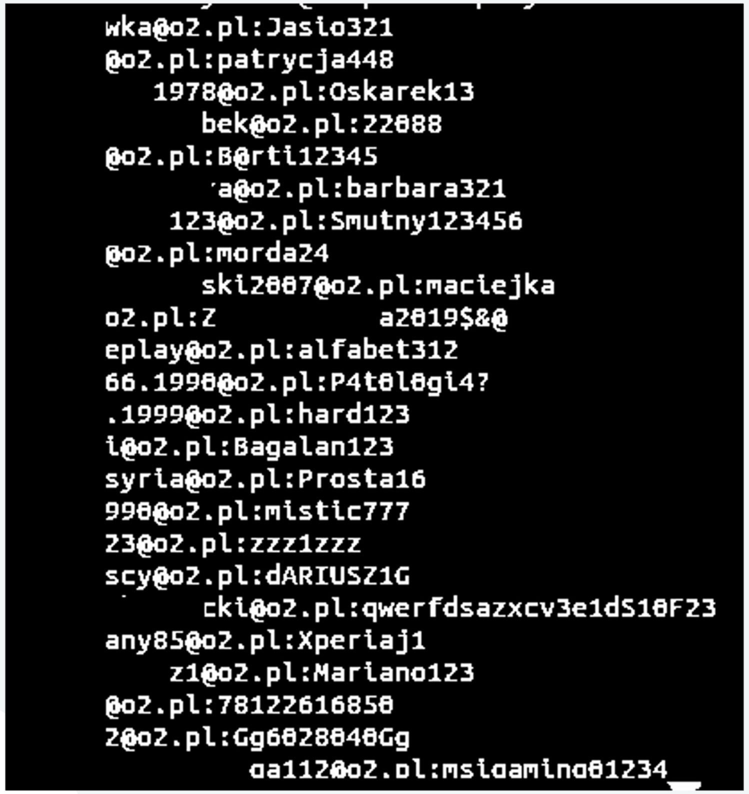
https://haveibeenpwned.com

https://pages.nist.gov/800-63-3/sp800-63b.html

0x0B Cyber Threat Intelligence

The 21st century intelligence operations lie in the internet

- Monitoring the darknet
- Monitoring the telegram channels
- Monitoring the ongoing cyber-attacks.
- Monitoring the credential leaks
- Analyzing the intelligence data.
- Acquiring the intelligence data.



```
wka@o2.pl:Jasio321
@o2.pl:patrycja448
   1978@o2.pl:Oskarek13
      bek@o2.pl:22088
@o2.pl:B@rti12345
       'a@o2.pl:barbara321
    123@o2.pl:Smutny123456
@o2.pl:morda24
      ski2007@o2.pl:maciejka
o2.pl:Z          a2019$&@
eplay@o2.pl:alfabet312
66.1998@o2.pl:P4t0l0gi4?
.1999@o2.pl:hard123
i@o2.pl:Bagalan123
syria@o2.pl:Prosta16
998@o2.pl:mistic777
23@o2.pl:zzz1zzz
scy@o2.pl:dARIUSZ1G
      cki@o2.pl:qwerfdsazxcv3e1dS10F23
any85@o2.pl:Xperiaj1
    z1@o2.pl:Mariano123
@o2.pl:78122616850
2@o2.pl:Gg6028048Gg
         aa112@o2.pl:msiaamina01234
```

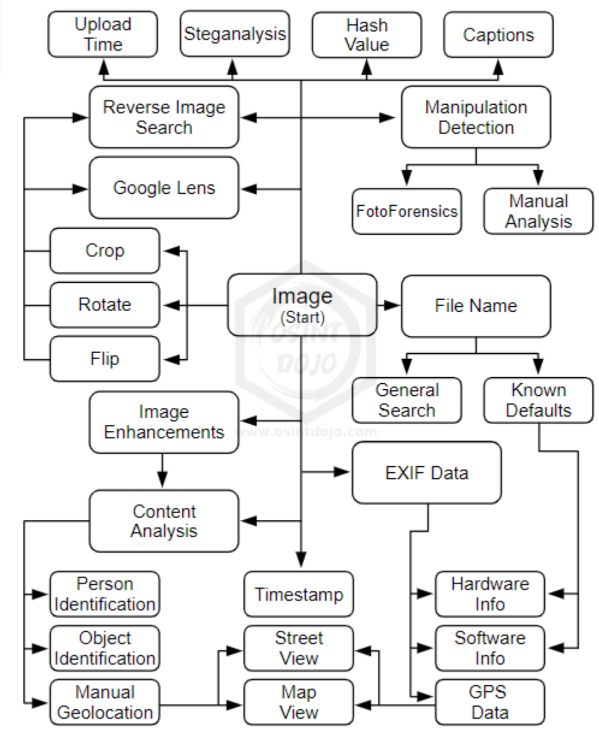
Credentials reuse is a frequent cause of a compromise

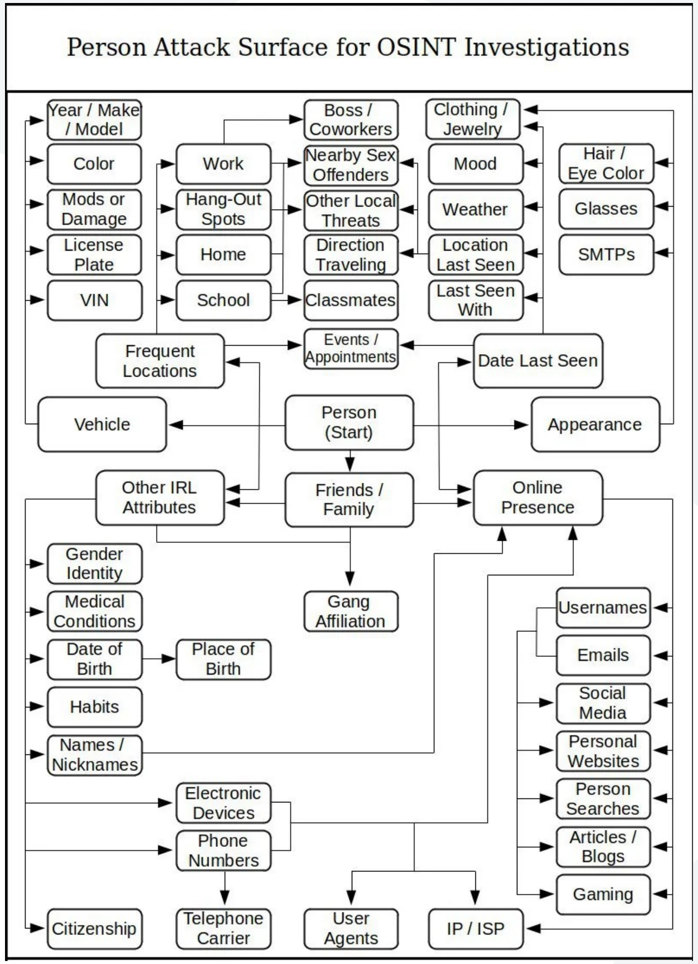
I have become a ransomware victim. What do I do?

***Do not negotiate with terrorists*.**
https://www.nomoreransom.org/pl/index.html

0x0C Open Source Intelligence

Don't get stalked

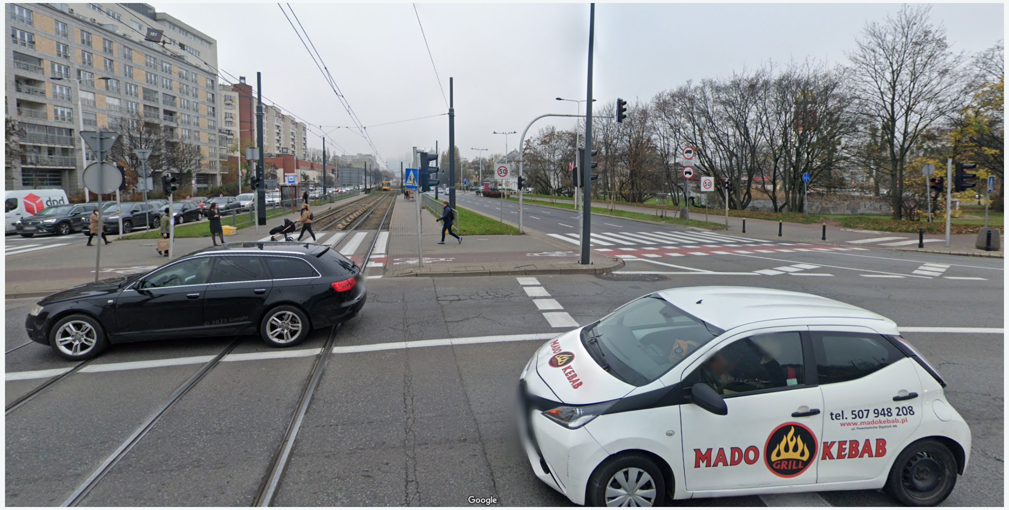



Person Attack Surface for OSINT Investigations

https://map.snapchat.com/

https://www.osintdojo.com/diagrams/main

https://github.com/jivoi/awesome-osint



Where in the world is this place?

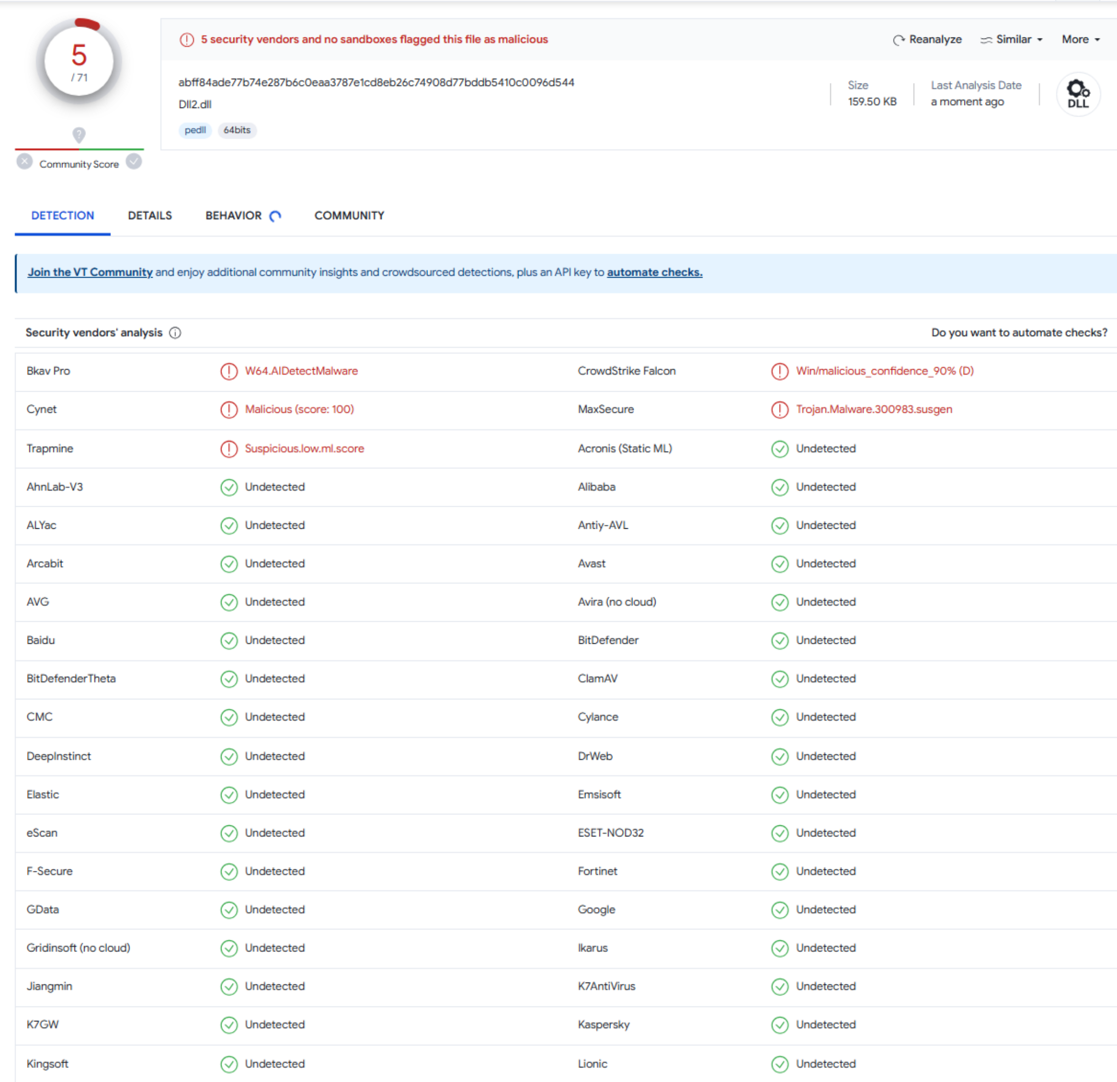
- Right-hand traffic
- Polish phone on a car
- *Tier* company scootie
- The woman is coming back from CCC store (bag)
- Railroad
- Skyscrapers in the back
- Park nearby
- Probable reverse roundabout sign

0x0D VPN’s don’t make you totally anon

- VPNs may guard you from network attacks and open access to services closed for certain geolocation.
- VPN’s don’t make you all anonymous – all your privacy is in hands of a VPN provider.
- The ISP sees you connecting to a VPN.
- Beware the VPN entry point as an initial access vector to domain. **It is recommended to segment your network**.
- ***Free VPN’s may sell your data***

0x0E AV will not save the day

- AV is better than nothing
- Cyber threats and evasion techniques are constantly evolving
- Relying solely on AV's is no longer sufficient.
- Organizations must adapt multi-layered approach – Defense in Depth.
- Monitoring, Detecting, and Preventing is crucial.
- The attackers **will** find a way, that is their job.
- Let them have their job while the **DFIR blue team investigates** – deception, decoys, honeypots, threat hunting.
- What if AV gets trojanized?



5 / 71

Community Score

(!) 5 security vendors and no sandboxes flagged this file as malicious

abff84ade77b74e287b6c0eaa3787e1cd8eb26c74908d77bddb5410c0096d544

Dll2.dll

pedll 64bits

Size 159.50 KB

Last Analysis Date a moment ago

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis ⓘ

Do you want to automate checks?

Bkav Pro	(!) W64.AIDetectMalware	CrowdStrike Falcon	(!) Win/malicious_confidence_90% (D)
Cynet	(!) Malicious (score: 100)	MaxSecure	(!) Trojan.Malware.300983.susgen
Trapmine	(!) Suspicious.low.ml.score	Acronis (Static ML)	✓ Undetected
AhnLab-V3	✓ Undetected	Alibaba	✓ Undetected
ALYac	✓ Undetected	Antiy-AVL	✓ Undetected
Arcabit	✓ Undetected	Avast	✓ Undetected
AVG	✓ Undetected	Avira (no cloud)	✓ Undetected
Baidu	✓ Undetected	BitDefender	✓ Undetected
BitDefenderTheta	✓ Undetected	ClamAV	✓ Undetected
CMC	✓ Undetected	Cylance	✓ Undetected
DeepInstinct	✓ Undetected	DrWeb	✓ Undetected
Elastic	✓ Undetected	Emsisoft	✓ Undetected
eScan	✓ Undetected	ESET-NOD32	✓ Undetected
F-Secure	✓ Undetected	Fortinet	✓ Undetected
GData	✓ Undetected	Google	✓ Undetected
Gridinsoft (no cloud)	✓ Undetected	Ikarus	✓ Undetected
Jiangmin	✓ Undetected	K7AntiVirus	✓ Undetected
K7GW	✓ Undetected	Kaspersky	✓ Undetected
Kingsoft	✓ Undetected	Lionic	✓ Undetected

https://maldevacademy.com/

https://www.fortinet.com/resources/cyberglossary/defense-in-depth

0x0F Falling into a rabbit hole

Win a bunny

1. **How** insecure is IoT?
2. **What** is the name of the ransomware group compromised by FBI lately?
3. **Is real-time** voice cloning possible?
4. **Name** one example of an internal threat.
5. **What** is the name of the proces of collecting, safeguarding, and analysis lifecycle of the criminal cyber-evidence?
6. **What** is the most common Web Application vulnerability class as of 2021?
7. **What** is the most common external initial access vector?
8. **Is** it worth it to segment the network?
9. **What** is an example of a good password?
10. **What** is cyber threat intelligence?

https://www.shodan.io/

0x10 Q&A

Ask me anything you want

0x11 Thank you

Presentation in PDF format is available on **https://news.baycode.eu**

Meet me again at ***https://wguisw.org***

[BEC Poland]

WGUiSW | Mar 5th, 2024