

[Hello Security]

WGUISW

0x03 Stay safe, realistically

Krystian Bajno, 2024

baysec.

[Table of Contents]

[0x03 Stay safe, realistically](#)

[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.nomore ransom.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>

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



Ox06 MITRE – the actual techniques

ATT&CK, D3FEND

MITRE ATT&CK

Matrices - Tactics - Techniques - Defenses - CTI - Resources - Benefactors Blog Search Q

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Active Scanning (2)	Acquire Access (2)	Content Injection (2)	Cloud Administration Command (2)	Account Manipulation (2)	Abuse Elevation Control Mechanism (2)	Abuse Elevation Control Mechanism (2)	Adversary-in-the-Middle (2)	Account Discovery (2)	Exploitation of Remote Services (2)	Adversary-in-the-Middle (2)	Application Layer Protocol (2)	Automated Exfiltration (1)	Account Access Removal (2)
Gather Victim Host Information (4)	Acquire Infrastructure (2)	Drive-by Compromise (2)	Command and Scripting Interpreter (2)	BITS Jobs (2)	Access Token Manipulation (2)	Access Token Manipulation (2)	Brute Force (2)	Browser Information Discovery (2)	Internal Spearphishing (2)	Archive Collected Data (2)	Communication Through Removable Media (2)	Data Transfer Size Limits (2)	Data Destruction (2)
Gather Victim Identity Information (2)	Compromise Accounts (2)	Exploit Public-Facing Application (2)	Container Administration Command (2)	Boot or Logon Autostart Execution (14)	Account Manipulation (2)	Account Manipulation (2)	Credentials from Password Stores (2)	Cloud Infrastructure Discovery (2)	Remote Service Session Hijacking (2)	Audio Capture (2)	Content Injection (2)	Exfiltration Over Intermediaries (2)	Data Encrypted for Impact (2)
Gather Victim Network Information (2)	Compromise Infrastructure (2)	External Remote Services (2)	Deploy Container (2)	Boot or Logon Autostart Execution (14)	Debugger Evasion (2)	Debugger Evasion (2)	Build Image on Host (2)	Cloud Service Dashboard (2)	Remote Services (2)	Auto (2)			Data Manipulation (2)
Gather Victim Org Information (4)	Develop Capabilities (2)	Hardware Additions (2)	Exploitation for Client Execution (2)	Browser Extensions (2)	Deobfuscate/Decode Files or Information (2)	Deobfuscate/Decode Files or Information (2)	Build Image on Host (2)	Cloud Service Dashboard (2)	Remote Services (2)	Browser Hijack (2)			
Flushing for Information (4)	Establish Capabilities (2)	Phishing (2)	Inter-Process Communication (2)	Compromise Client Software Binary (2)	Boot or Logon Initialization Scripts (2)	Boot or Logon Initialization Scripts (2)	Boot or Logon Initialization Scripts (2)	Cloud Storage Object Discovery (2)	Remote Services (2)	Client (2)			
Search Closed Sources (2)	Obtain Capabilities (2)	Replication Through Removable Media (2)	Native API (2)	Create or Modify System Process (2)	Deploy Container (2)	Deploy Container (2)	Boot or Logon Initialization Scripts (2)	Container and Resource Discovery (2)	Remote Services (2)	Cloud Stor (2)			
Search Open Technical Databases (2)	Stage Capabilities (2)	Supply Chain Compromise (2)	Scheduled Task/Job (2)	Create or Modify System Process (2)	Domain Policy Modification (2)	Domain Policy Modification (2)	Boot or Logon Initialization Scripts (2)	Debugger Evasion (2)	Remote Services (2)	Data Stor (2)			
Search Open Websites/Domains (2)	Trusted Relationship (2)	Serverless Execution (2)	Event Triggered Execution (2)	Escape to Host (2)	Execution Guardrails (2)	Execution Guardrails (2)	Event Triggered Execution (2)	Device Driver Discovery (2)	Remote Services (2)	Data Stor (2)			
Search Victim-Owned Websites (2)	Valid Accounts (2)	Shared Modules (2)	External Remote Services (2)	Exploitation for Defense Evasion (2)	File and Directory Permissions Modification (2)	File and Directory Permissions Modification (2)	Event Triggered Execution (2)	Domain Trust Discovery (2)	Remote Services (2)	Data Stor (2)			
		Software Deployment Tools (2)	Hijack Execution Flow (12)	Impersonation (2)	Hide Artifacts (11)	Hide Artifacts (11)	External Remote Services (2)	File and Directory Discovery (2)	Remote Services (2)	Data Stor (2)			
		System Services (2)	Implant Internal Image (2)	Impersonation (2)	Hijack Execution Flow (12)	Hijack Execution Flow (12)	Software Deployment Tools (2)	Group Policy Discovery (2)	Remote Services (2)	Data Stor (2)			
		User Execution (2)	Modify Authentication Process (2)	Impersonation (2)	Process Injection (12)	Process Injection (12)	Software Deployment Tools (2)	Log Enumeration (2)	Remote Services (2)	Data Stor (2)			
		Windows Management Instrumentation (2)	Office Application Startup (2)	Impersonation (2)	Scheduled Task/Job (2)	Scheduled Task/Job (2)	Software Deployment Tools (2)	Network Share Discovery (2)	Remote Services (2)	Data Stor (2)			
			Power Settings (2)	Impersonation (2)	Valid Accounts (2)	Valid Accounts (2)	Software Deployment Tools (2)	Network Stalling (2)	Remote Services (2)	Data Stor (2)			
			Pre-OS Boot (2)	Impersonation (2)	Valid Accounts (2)	Valid Accounts (2)	Software Deployment Tools (2)	Password Policy Discovery (2)	Remote Services (2)	Data Stor (2)			
			Scheduled Task/Job (2)	Impersonation (2)	Valid Accounts (2)	Valid Accounts (2)	Software Deployment Tools (2)	Peripheral Device Discovery (2)	Remote Services (2)	Data Stor (2)			
			Server Software Component (2)	Impersonation (2)	Valid Accounts (2)	Valid Accounts (2)	Software Deployment Tools (2)	Permission Groups Discovery (2)	Remote Services (2)	Data Stor (2)			
			Traffic Signaling (2)	Impersonation (2)	Valid Accounts (2)	Valid Accounts (2)	Software Deployment Tools (2)	Process Discovery (2)	Remote Services (2)	Data Stor (2)			
				Impersonation (2)	Valid Accounts (2)	Valid Accounts (2)	Software Deployment Tools (2)	Query Registry (2)	Remote Services (2)	Data Stor (2)			
				Impersonation (2)	Valid Accounts (2)	Valid Accounts (2)	Software Deployment Tools (2)	Remote System Discovery (2)	Remote Services (2)	Data Stor (2)			
				Impersonation (2)	Valid Accounts (2)	Valid Accounts (2)	Software Deployment Tools (2)	System Information Discovery (2)	Remote Services (2)	Data Stor (2)			
				Impersonation (2)	Valid Accounts (2)	Valid Accounts (2)	Software Deployment Tools (2)	System Location Discovery (1)	Remote Services (2)	Data Stor (2)			
				Impersonation (2)	Valid Accounts (2)	Valid Accounts (2)	Software Deployment Tools (2)	System Network Configuration Discovery (2)	Remote Services (2)	Data Stor (2)			
				Impersonation (2)	Valid Accounts (2)	Valid Accounts (2)	Software Deployment Tools (2)	System Network Connections Discovery (2)	Remote Services (2)	Data Stor (2)			
				Impersonation (2)	Valid Accounts (2)	Valid Accounts (2)	Software Deployment Tools (2)	System Owner/User Discovery (2)	Remote Services (2)	Data Stor (2)			
				Impersonation (2)	Valid Accounts (2)	Valid Accounts (2)	Software Deployment Tools (2)	System Service Discovery (2)	Remote Services (2)	Data Stor (2)			
				Impersonation (2)	Valid Accounts (2)	Valid Accounts (2)	Software Deployment Tools (2)	System Time Discovery (2)	Remote Services (2)	Data Stor (2)			
				Impersonation (2)	Valid Accounts (2)	Valid Accounts (2)	Software Deployment Tools (2)	Virtualization/Sandbox Evasion (2)	Remote Services (2)	Data Stor (2)			

DEFEND™

A knowledge graph of cybersecurity countermeasures

ATT&CK Lookup

Search D3FEND's 820 Artifacts

D3FEND Lookup

Model	Harden				Detect				Isolate		Deceive		Evict		Restore					
	Application Hardening	Credential Hardening	Message Hardening	Platform Hardening	File Analysis	Identifier Analysis	Message Analysis	Network Traffic Analysis	Platform Monitoring	Process Analysis	User Behavior Analysis	Execution Isolation	Network Isolation	Decoy Environment	Decoy Object	Credential Eviction	File Eviction	Process Eviction	Restore Access	Restore Object
Application Configuration Hardening	Biometric Authentication	Message Authentication	Bootloader Authentication	Dynamic File Analysis	Homograph Detection	Sender MTA Reputation Analysis	Administrative Network Activity Analysis	File Integrity Monitoring	Database Query String Analysis	Authentication Event Thresholding	Executable Allowlisting	Broadcast Domain Isolation	Connected Honeynet	Decoy File	Account Locking	File Removal	Process Suspension	Restore Network Access	Restore Credential	Restore Object
Dead Code Elimination	Certificate Pinning	Transfer Agent Authentication	Disk Encryption	Emulated File Analysis	Identifier Activity Analysis	Sender Reputation Analysis	Byte Sequence Emulation	Firmware Pattern Analysis	Authorization Event Thresholding	Executable Denylisting	DNS Allowlisting	Integrated Honeynet	Decoy Network Resource	Authentication Cache Invalidation	Email Removal	Process Termination	Restore Network Access	Restore Configuration	Restore Database	Restore Disk Image
Exception Handler Pointer Validation	Credential Rotation	Domain Trust Scoping	Driver Load Integrity Checking	File Content Analysis	Identifier Reputation Analysis	Certificate Analysis	Active Certificate Verification	Firmware Embedded Monitoring Code	Indirect Branch Call Analysis	Credential Compromise Scope Analysis	Hardware-based Process Isolation	DNS Denylisting	Decoy Persona	Credential Revoking	Unlock Account	Restore File	Restore Email	Restore Software		
Pointer Authentication	Domain Trust Policy	Multi-factor Authentication	File Encryption	File Content Rules	Domain Name Reputation Analysis	File Hash Reputation Analysis	File Hash Reputation Analysis	Peripheral Firmware Verification	Domain Account Monitoring	Job Function Access Pattern Analysis	IO Port Restriction	Forward Resolution Domain Denylisting	Decoy Public Release	Decoy Session Token						
Process Segment Execution Prevention	One-time Password	Strong Password Policy	Local File Permissions	File Hashing	IP Reputation Analysis	URL Reputation Analysis	URL Reputation Analysis	Client-server Firmware Verification	System Firmware Verification	Resource Access Pattern Analysis	Mandatory Access Control	Hierarchical Domain Denylisting	Decoy User Credential							
Segment Address Offset Randomization	Strong Password Policy	User Account Permissions	RF Shielding	Software Update	System Configuration Permissions	TPM Boot Integrity		Connection Attempt Analysis	Operating System Monitoring	Process Spawn Analysis	System Call Filtering	Forward Resolution IP Denylisting								
Stack Frame Canary Validation	User Account Permissions							DNS Traffic Analysis	Endpoint Health Beacon	Script Execution Analysis	Session Duration Analysis	Encrypted Tunnels								
								File Carving	Input Device Analysis	Shadow Stack Comparisons	User Data Transfer Analysis	Network Traffic Filtering								
								Inbound Session Volume Analysis	Memory Boundary Tracking	System Call Analysis	User Credentialation Logon Pattern Analysis	Inbound Traffic Filtering								
								IPC Traffic Analysis	Scheduled Job Analysis	File Creation Analysis	Web Session Activity Analysis	Outbound Traffic Filtering								
								Network Traffic Community Deviation	System Dilemma Monitoring											
								Per Host Download/Upload Ratio Analysis	System File Analysis	Service Binary Verification										
								Protocol Metadata Anomaly Detection	System Int Config Analysis	System Int Config Analysis										
								Relay Pattern Analysis	User Session Int Config Analysis											
								Remote Terminal Session Detection												
								RPC Traffic Analysis												

<https://d3fend.mitre.org>

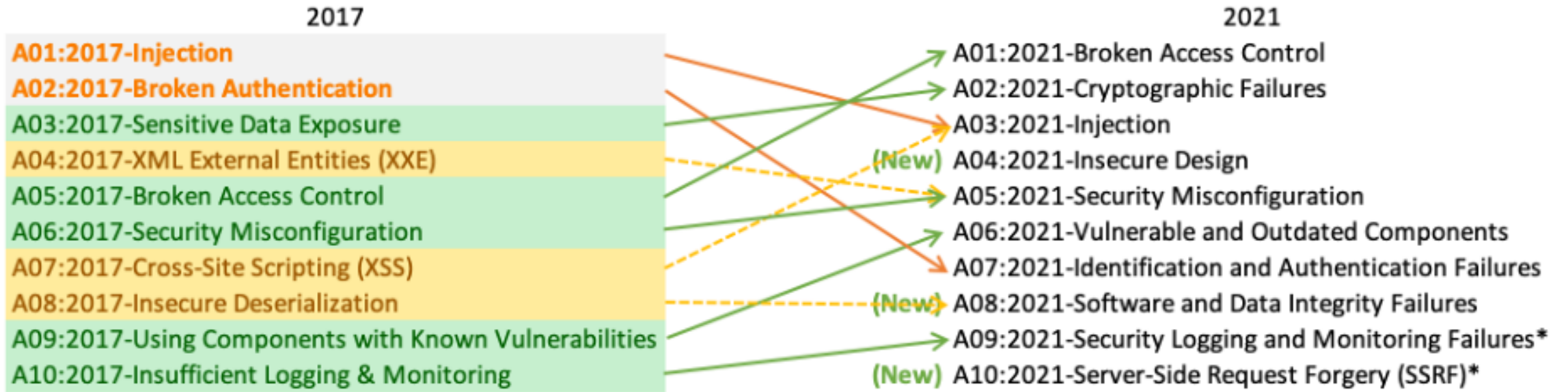
<https://attack.mitre.org>

Ox07 Web Application Security



Your trust, in others hands

Database breaches may expose your credentials



* 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.

Ox09 Authentication anatomy

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

Standard good old passwords

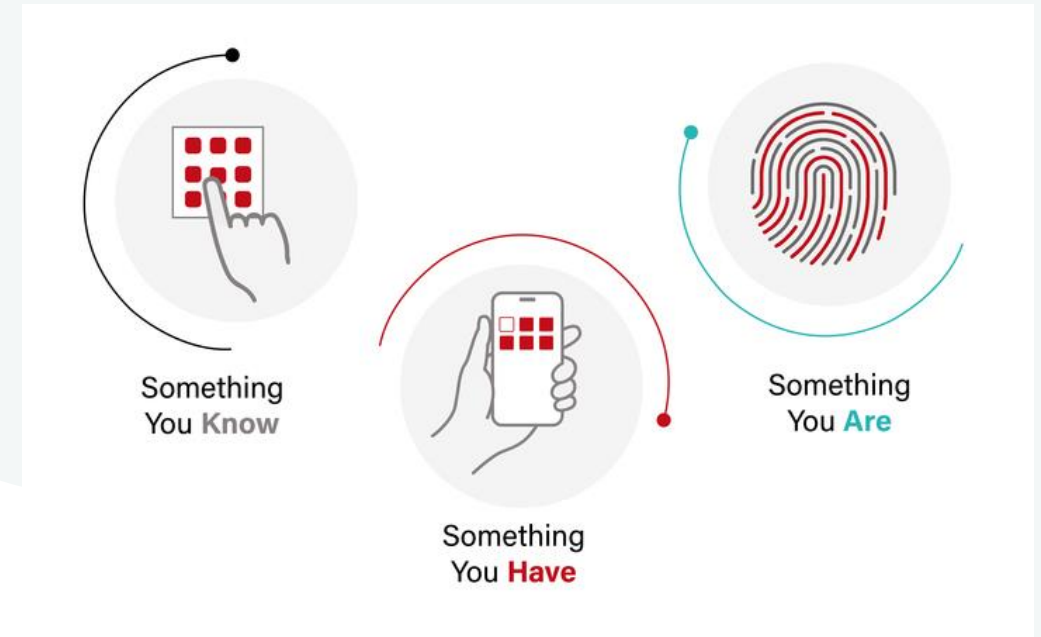
Multi Factor Authentication

- 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?

Ox0A 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
- DlaziKostekNaMostek/I\$tuka

<https://cert.pl/hasla>

<https://haveibeenpwned.com>

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

Ox0B 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:maclejka
o2.pl:Z a2019$&@
eplay@o2.pl:alfabet312
66.1998@o2.pl:P4t0l0gi4?
.1999@o2.pl:hard123
l@o2.pl:Bagalan123
syrla@o2.pl:Prosta16
998@o2.pl:mistic777
23@o2.pl:zzz1zzz
scy@o2.pl:dARIUSZ1G
cki@o2.pl:qwerfdsazxcv3e1dS10F23
any85@o2.pl:Xperlaj1
z1@o2.pl:Marlano123
@o2.pl:78122616850
2@o2.pl:Gg6028040Gg
aa112@o2.pl:mslaamina01234
```

Credentials reuse is a frequent cause of a compromise



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

Do not negotiate with terrorists.

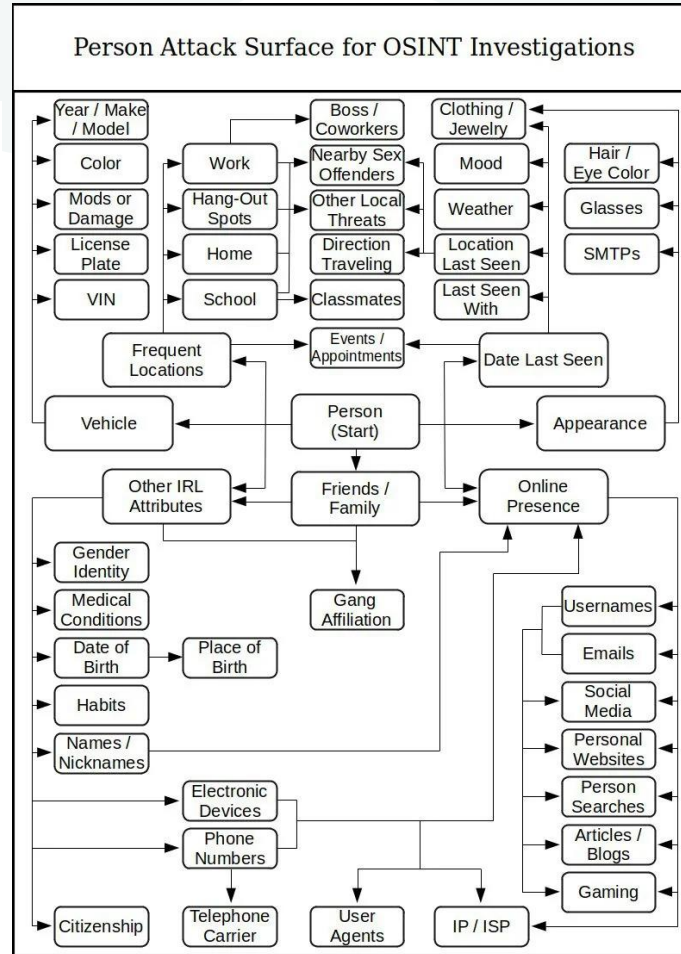
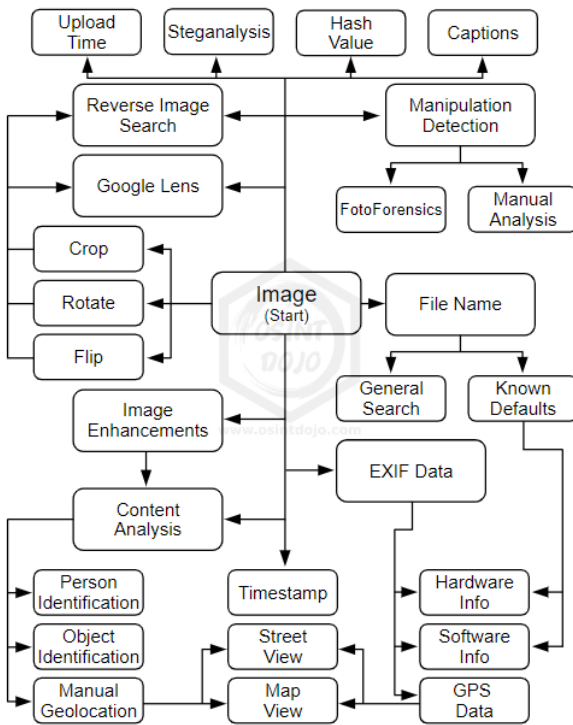
<https://www.nomoreransom.org/pl/index.html>



LOCKBIT 3.0

OxOC Open Source Intelligence

Don't get stalked



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

<https://map.snapchat.com/>

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

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

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***

OxOE 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?

<https://maldevacademy.com/>

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

5 / 171

5 security vendors and no sandboxes flagged this file as malicious

abff84ade77b74e287b6c0eaa3787e1cd8eb26c74908d77bddb5410c0096d544

Dll2.dll

Size: 159.50 KB

Last Analysis Date: a moment ago

pedll 64bits

Community Score

DETECTION DETAILS BEHAVIOR COMMUNITY

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

Security vendors' analysis

Vendor	Detection	Vendor	Detection
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

OxOF 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?

[Hello Security]

WGUiSW

baysec.

0x10 Q&A

Ask me anything you want

Ox11 Thank you

Presentation in PDF format is available on <https://insights.baysec.eu>

Meet me again at <https://wguisw.org>