[Hello Security]

WGUiSW

0x03 Stay safe, realistically

Krystian Bajno, 2024

baysec.

[Table of Contents]

[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

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*

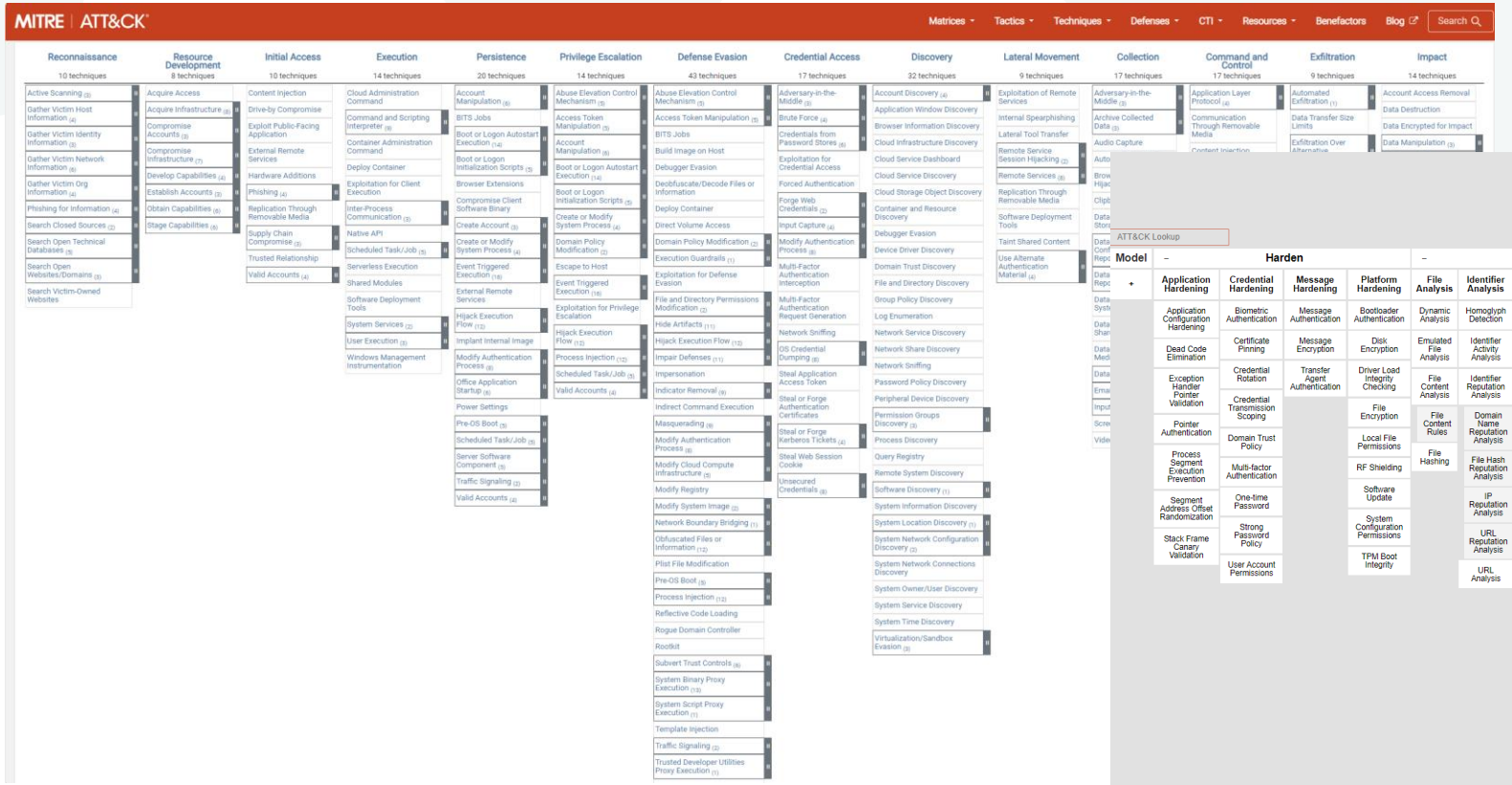
- Anything ***denying an access to a resource***
- Crashes, glitches, overloads
- Power outages
- System compromise

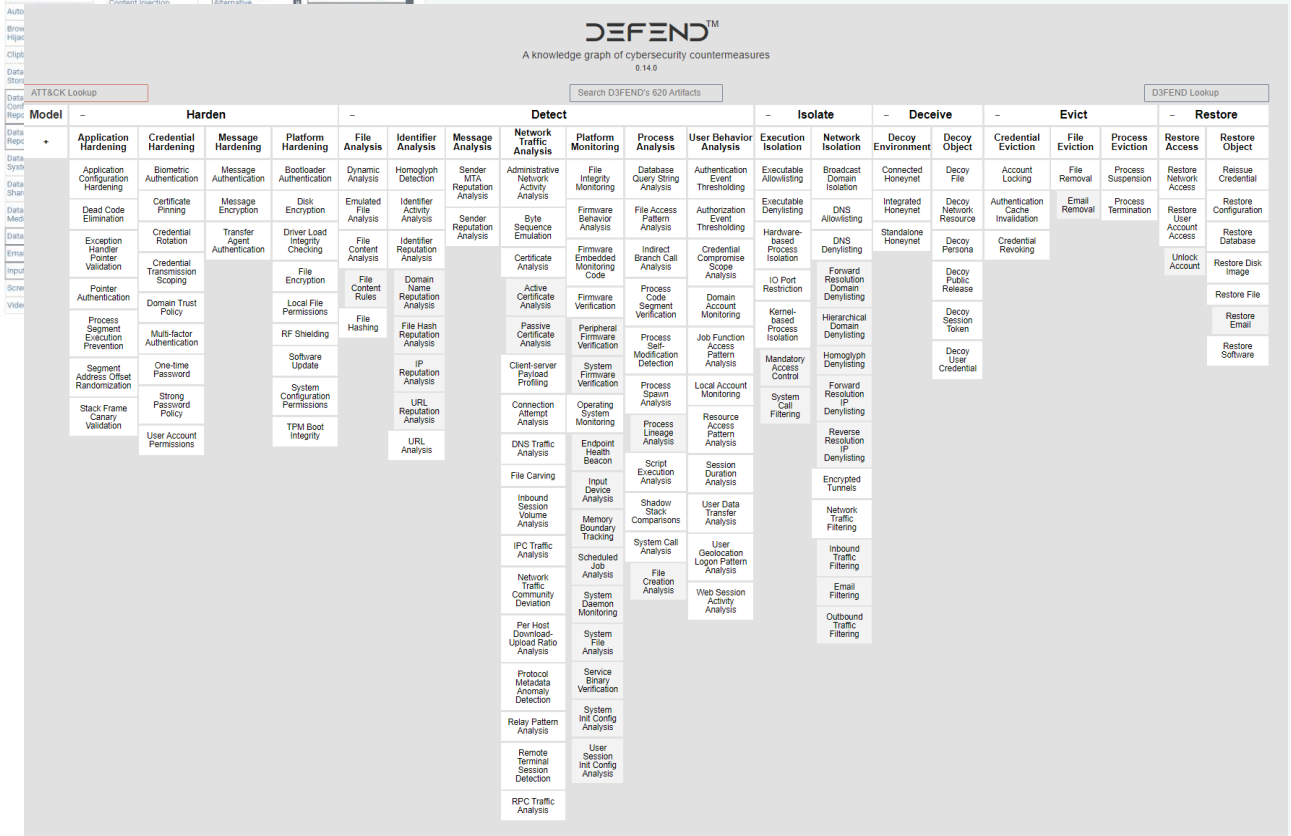
Functionality vs Security principle

WGUiSW baysec.

0x06 MITRE – the actual techniques

ATT&CK, D3FEND





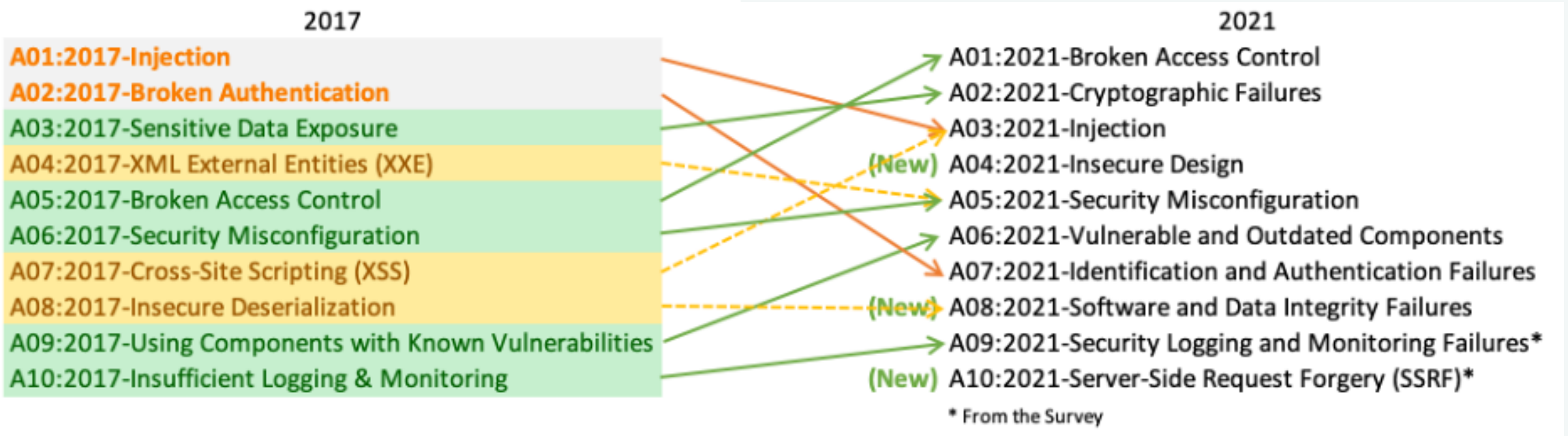
https://d3fend.mitre.org

https://attack.mitre.org

0x07 Web Application Security

Your trust, in others hands

Database breaches may expose your credentials



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:

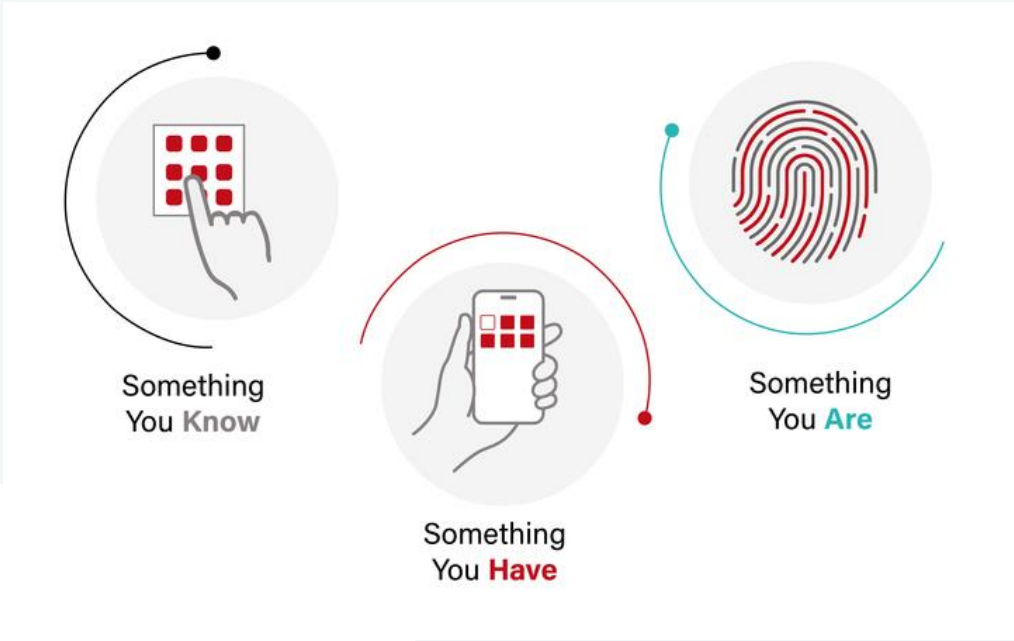
1. The IPv6 is preferred over IPv4, but no-one controls it.
2. If no one controls the IPv6, then who is able to lease DHCPv6 IP's and become the DNS Man in the Middle controller?
3. Relay the creds over LDAP in order to create a delegated machine account.
4. ***Compromise the whole network***

Credential leaks are not your fault.

0x09 Authentication anatomy

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

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



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

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.**

Bad password examples:

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

Good password examples:

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

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.

https://cert.pl/hasla

https://haveibeenpwned.com

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

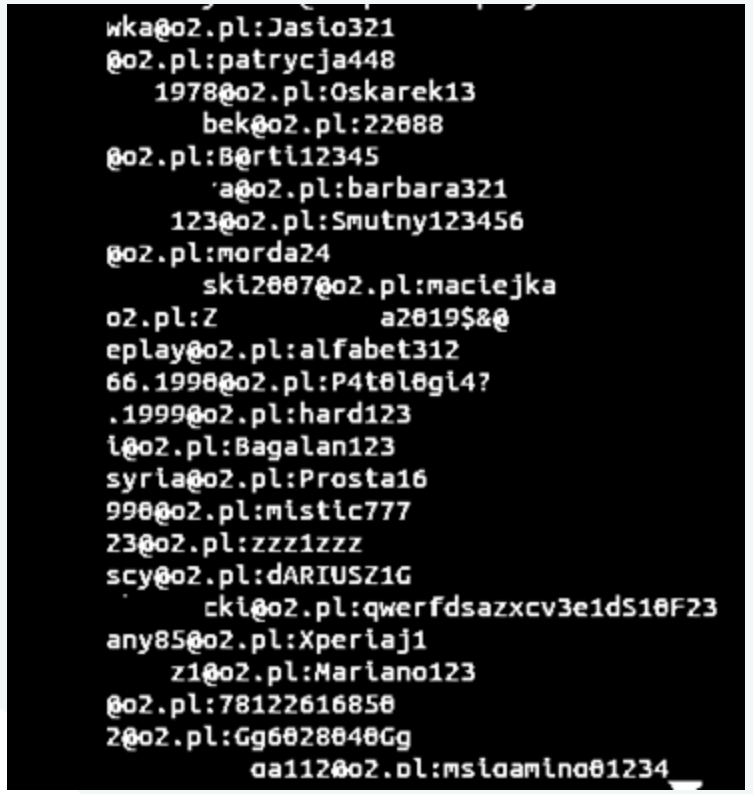
[Hello Security]

WGUiSW baysec.

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.



Credentials reuse is a frequent cause of a compromise

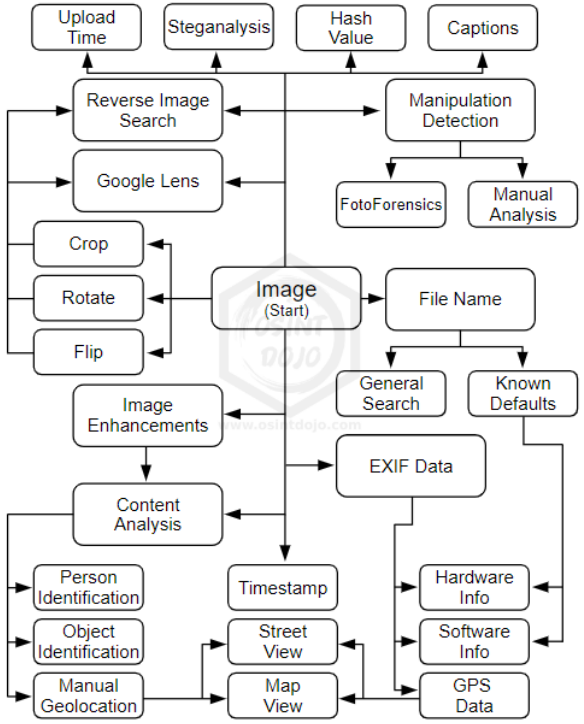
I have become a ransomware victim. What do I do?

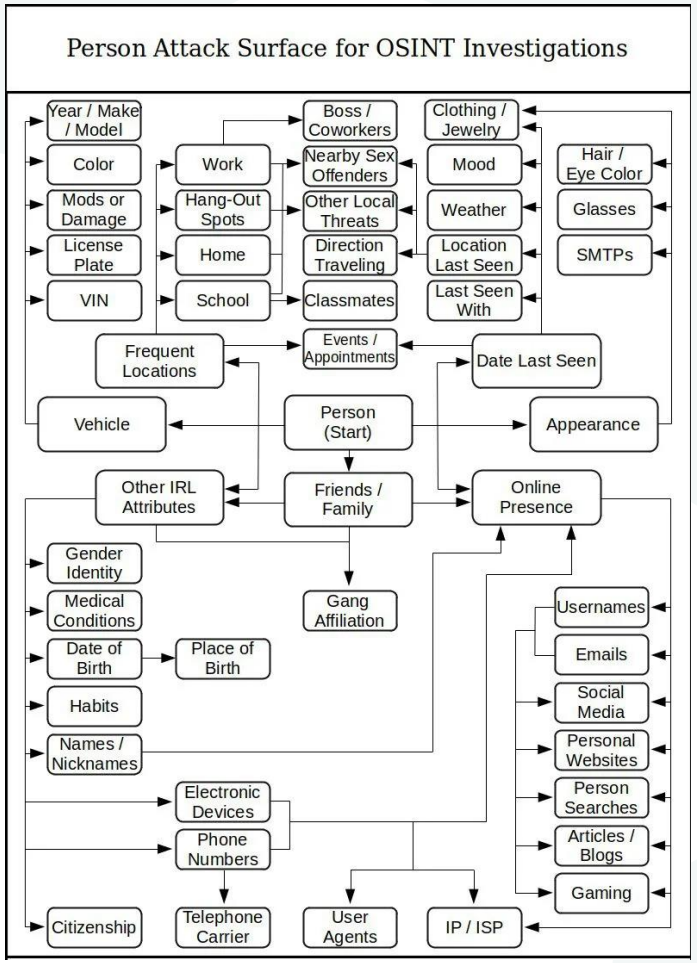
Do not negotiate with terrorists.
https://www.nomoreransom.org/pl/index.html

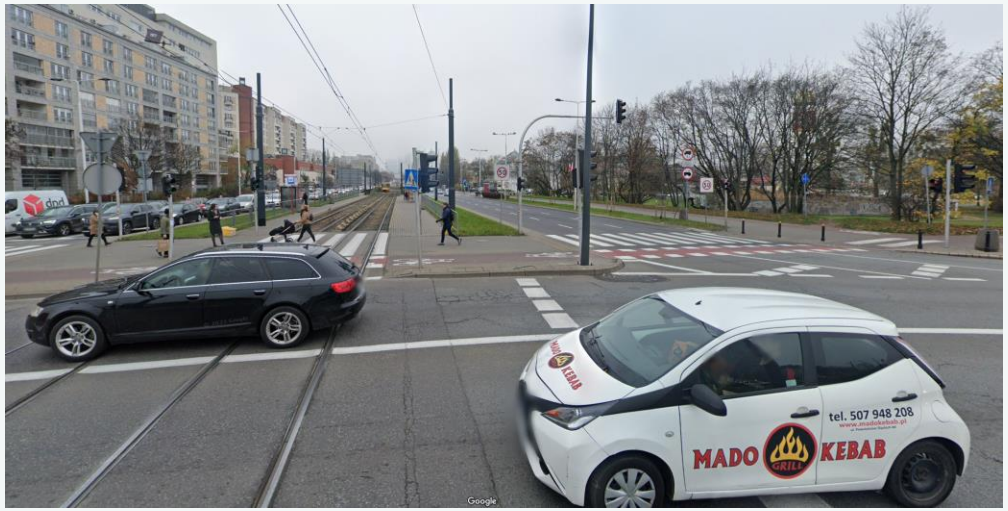
LOCKBIT 3.0

0x0C 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

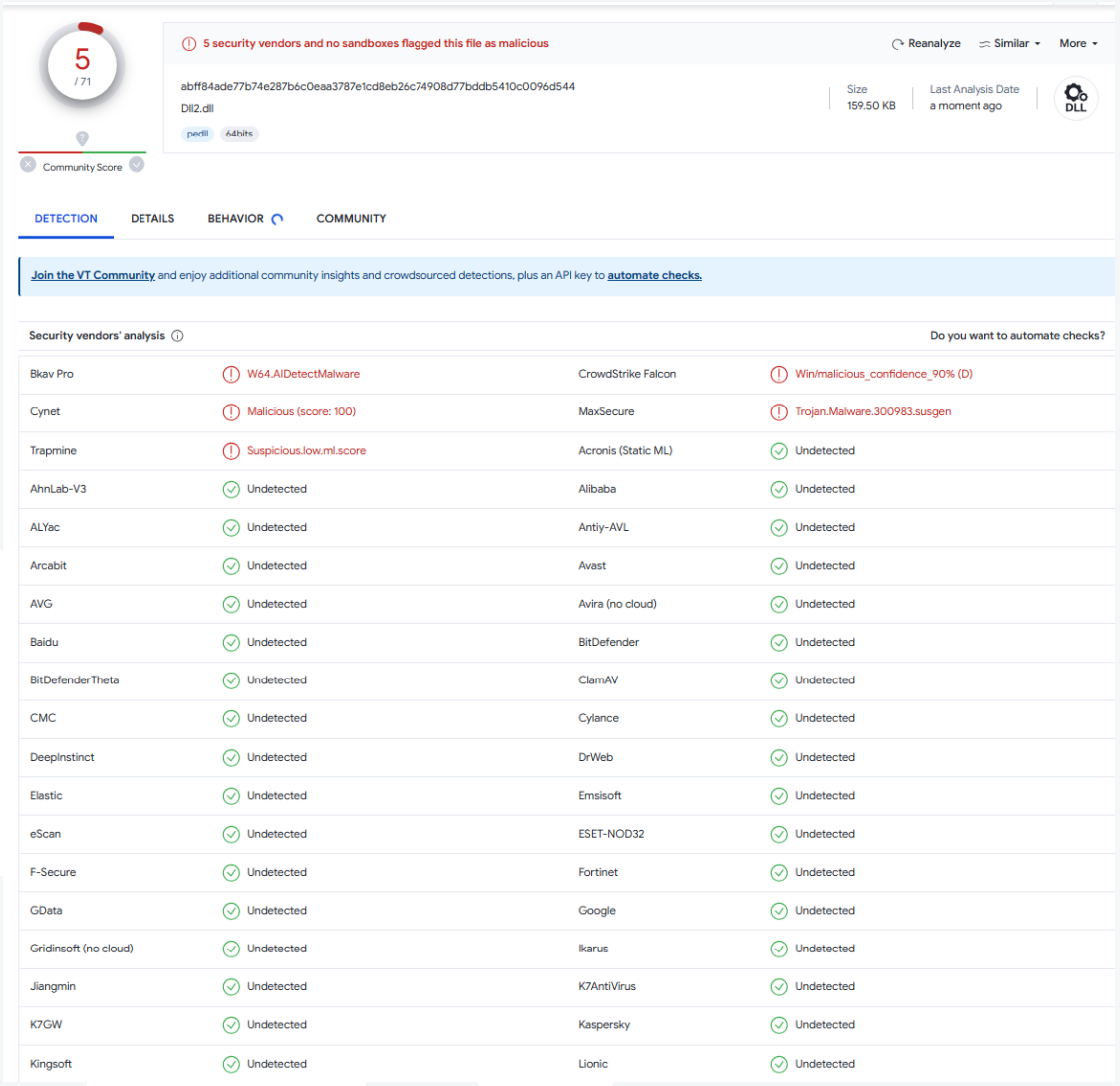
0x0D VPN's don't make you totally anon

- 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***

WGUiSW baysec.

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?



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/

WGUiSW baysec.

0x10 Q&A

Ask me anything you want

0x11 Thank you

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

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