VIAVIS střežíme podstatné

# Hackerem snadno a rychle

## Analýza a bezpečnost dat

**Vladimír Lazecký**

**vladimir.lazecky@viavis.cz**

# Analýza a bezpečnost dat



- OSINT – základní techniky a postupy
  - OSINT na osobu
  - OSINT na systém
- Forenzní analýza digitálních stop
  - Obecné principy a zásady – znalecké postupy
  - Zajištění digitálních stop u kybernetických incidentů

# OSINT



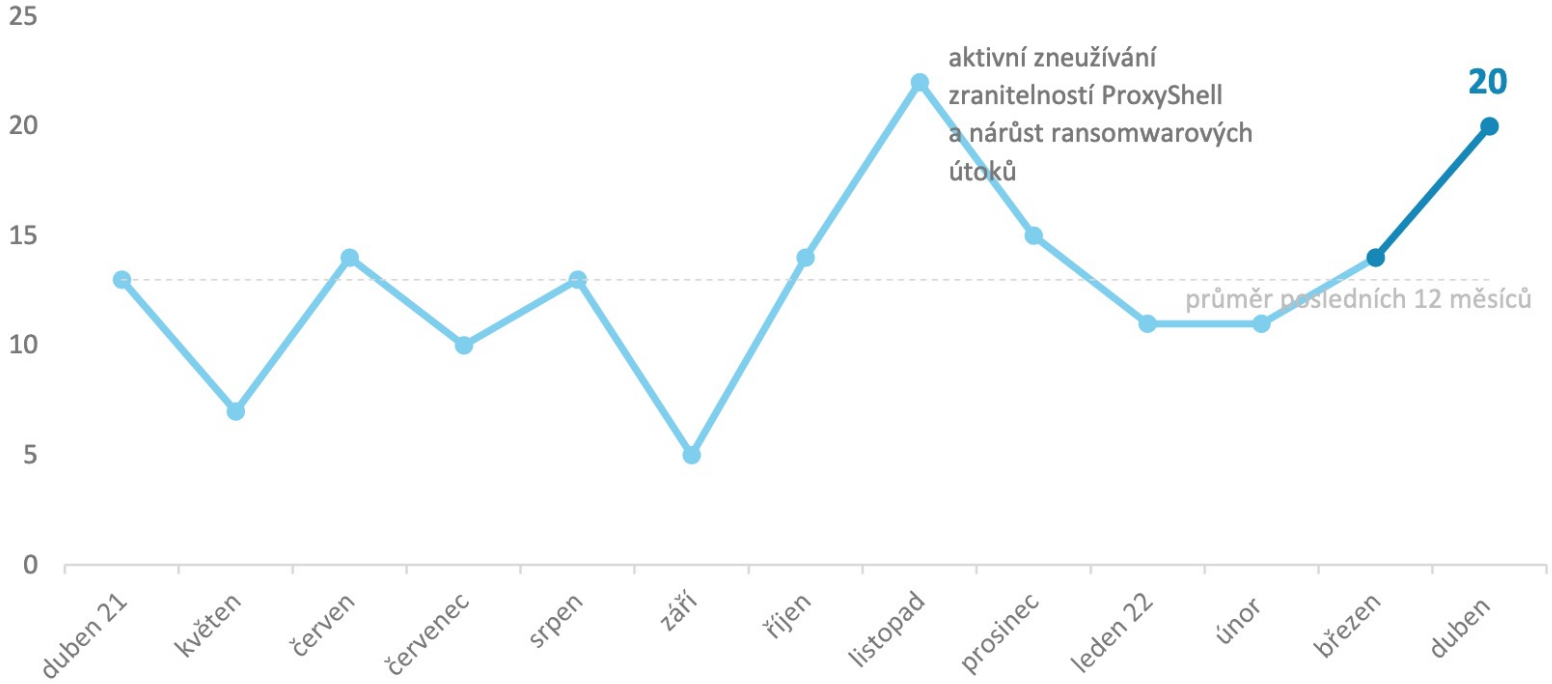
- Co to je OSINT?
- Proč OSINT?
- V čem je výhoda OSINT?

# Kyber incidenty pohledem NÚKIB



## Počet kybernetických bezpečnostních incidentů nahlášených NÚKIB

Duben se stal měsícem s druhým nejvyšším počtem incidentů za posledních dvanáct měsíců. Předčil jej pouze listopad, kdy docházelo k aktivnímu zneužívání zranitelností ProxyShell.[1]




https://nukib.cz/download/publikace/vyzkum/2022-04_Kyberneticke_incidenty.pdf

# Zpráva NÚKIB září 2022



Zisk těchto informací slouží jako ideální stavební kámen pro další fáze průzkumu (tzv. re-connaissance), vytvoření operačních zdrojů nebo prvotní přístup do sítě oběti. Samotná technika se dále rozpadá do trojice sub-technik, jmenovitě T1589.001: Credentials, T1589.002: Email Addresses a T1589.003: Employee Names.

Velice podobnou technikou je T1589: Gather Victim Org Information. V té se útočníci zaměřují na zjištění fyzických lokací (např. infrastruktura), byznysové vztahy, zjištění tempa byznysu a identifikaci rolí.

**Mitigace:** Danou techniku nelze snadno mitigovat. Subjekty by se měly primárně zaměřit, aby minimalizovaly množství dat (primárně citlivých), která jsou externě dostupná, a tedy zneužitelná v rámci OSINT.

https://www.nukib.cz/download/publikace/vyzkum/2022-09_Kyberneticke_incidenty.pdf

# Hezká sada návodů



SURVEILLANCE
SELF-DEFENSE

https://ssd.eff.org/en/module-categories/tool-guides

## Tool Guides

Below are step-by-step tutorials to help you install and use handy privacy and security tools. Surveillance Self-Defense encourages you to think about online privacy and security in a sophisticated way. We want to give you the power to choose tools and habits that work for you. We suggest conducting a threat modeling assessment before moving on to the following install guides. Please note that the law and technology can change quickly, and portions of SSD can become out of date. Check EFF's Security Education blog for the latest news.

# Pasivní OSINT metody k detekci útočmníků



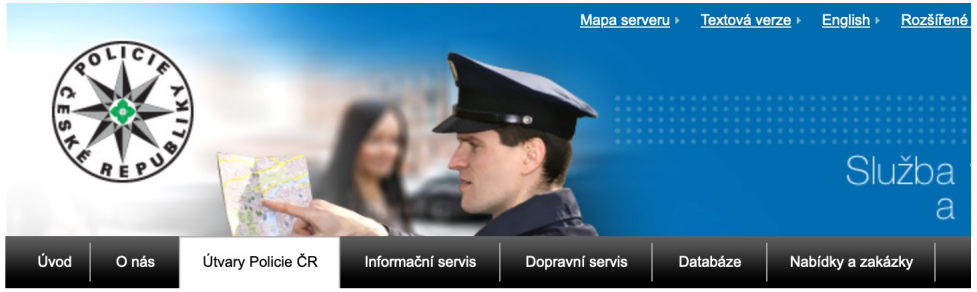

## 8 Passive OSINT Methods for Profiling Cybercriminals on the Dark Web

https://flare.systems/learn/resources/blog/8-passive-osint-methods-for-profiling-cybercriminals-on-the-dark-web/

# Úrodný rok 2021 – bez nároku na generalizaci



- Řádový nárůst útoků
- Útoky vedené ručně
- U 90% útoků došlo k extrakci dat
- 50% obětí platilo výkupné
- V 99% případů si oběť o útok sama řekla




ZPRAVODAJSTVÍ OLK

**Úvodní strana** / Útvary Policie ČR / Krajská ředitels

**Policie České republiky – KŘP Olomouckého kraje**

## Kybernetický útok na Magistrát města Olomouce odložen

OLOMOUCKÝ KRAJ - Kriminalisté na případu spolupracovali i s Europolem.

Kriminalisté odboru analytiky a kybernetické kriminality Krajského ředitelství policie Olomouckého kraje odložili trestní věc podezření ze spáchání přečinu neoprávněný přístup k počítačovému systému a nosiči informací, týkající se napadení počítačové sítě Magistrátu města Olomouce z počátku dubna 2021, neboť se nepodařilo zjistit skutečnosti opravňující zahájit trestní stíhání vůči konkrétní osobě.

https://www.policie.cz/clanek/kyberneticky-utok-na-magistrat-mesta-olomouce-odlozen.aspx



VIAVIS

# Úrodný rok 2021 – časté chyby s velkými dopady



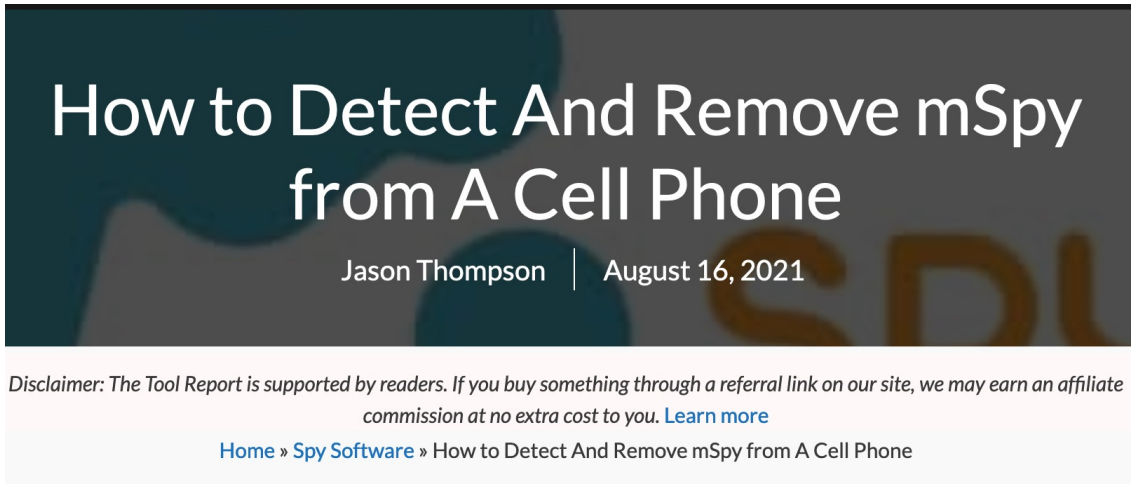
- Zmatek, nefunkční BCP a DRP plány, priority
- Obnova 1:1
- **Nezajištění stop pro forenzní analýzu**
- Zaměstnanci a sociální sítě
- Naivní vyjednávání s útočníky

```
-------===    Your network has been infected!    ===-------

*****************    DO NOT DELETE THIS FILE UNTIL ALL YOUR DATA HAVE BEEN RECOVERED    *****************

All your documents, photos, databases and other important files have been encrypted and have the extension:[redacted]
You are not able to decrypt it by yourself. But don't worry, we can help you to restore all your files!
The only way to restore your files is to buy our special software. Only we can give you this software and only we can restore your files!

We have also downloaded a lot of private data from your network.
If you do not contact as in a 3 days we will post information about your breach on our public news website and after 7 days the whole downloaded info.

You can get more information on our page, which is located in a Tor hidden network.

How to get to our page
--------------------------------------------------------------------------------
|
|  1. Download Tor browser - https://www.torproject.org/
|  2. Install Tor browser
|  3. Open link in Tor browser - avaddonbotrxmuyl.onion
|  4. Follow the instructions on this page
|
--------------------------------------------------------------------------------

Your ID:[redacted]
```

# Trendy 2022



- Masivní nárůst útoků na osoby
- Po útlumu v Q1 opět růst útoků s extrakcí dat
- Cíle stále komunikují zranitelnosti
- **Využití OSINT – velmi efektivní pro plánování útoků**
  - OSINT = Open Source Intelligence




https://www.thetoolreport.com/how-to-detect-and-remove-mspy-from-cell-phone/

# Hackerem snadno a rychle



- *Kdo se již setkal s kyber útokem?*
- *Kdo je hacker?*
- *Kdo se pokoušel něco hacknout?*

# Jak se stát hackerem snadno a rychle – využití OSINT



- Motivace, výchozí znalosti minimální
  - Vyhledávání zranitelností
  - Identifikace cílů
  - Databáze exploitů
- Zdroje:
  - Otevřený internet
  - Darknet

***Jen vědět, jak a kde hledat…***

# Hledání zranitelností



- **Otevřený internet**
  - Národní autority
  - Open source databáze
  - Placené databáze
  - Zprávy v otevřených zdrojích
  - Výrobci (rizika ZeroDay Vulnerability)

**Hackers Exploiting VMware Horizon to Target South Korea with NukeSped Backdoor**

May 20, 2022 Ravie Lakshmanan

The North Korea-backed Lazarus Group has been observed leveraging the Log4Shell vulnerability in VMware Horizon...


**Hackers Trick Users with Fake Windows 11 Downloads to Distribute Vidar Malware**

May 19, 2022 Ravie Lakshmanan

Fraudulent domains masquerading as Microsoft's Windows 11 download portal are attempting to trick users into...

https://thehackernews.com/

**Doporučuji pravidelně sledovat**

# Jak najít zranitelnosti – mnoho možností



NIST

NVD ME

Information Technology Laboratory

**NATIONAL VULNERABILITY DATABASE**

NVD

- **General** +
- **Vulnerabilities** +
- **Vulnerability Metrics** +
- **Products** +
- **Developers** +
- **Contact NVD**
- **Other Sites** +
- **Search** +

Understanding Vulnerability Detail Pages

Vulnerability Statuses

**Vulnerabilities**

https://nvd.nist.gov/vuln

# Jak najít zranitelnosti – národní autority




cisa.gov/uscert

Report Cyber Issue

Subscribe to Alerts

## KNOWN EXPLOITED VULNERABILITIES CATALOG

Download CSV version

Download JSON version

Download JSON schema

Subscribe to the Known Exploited Vulnerabilities Catalog Update Bulletin

Back to previous page for background on known exploited vulnerabilities

Show 10 entries Search:

| CVE | Vendor/Project | Product | Vulnerability Name | Date Added to Catalog | Short Description | Action | Due Date | Notes |
|---|---|---|---|---|---|---|---|---|

https://www.cisa.gov/known-exploited-vulnerabilities-catalog



VIAVIS

# Hledání exploitů

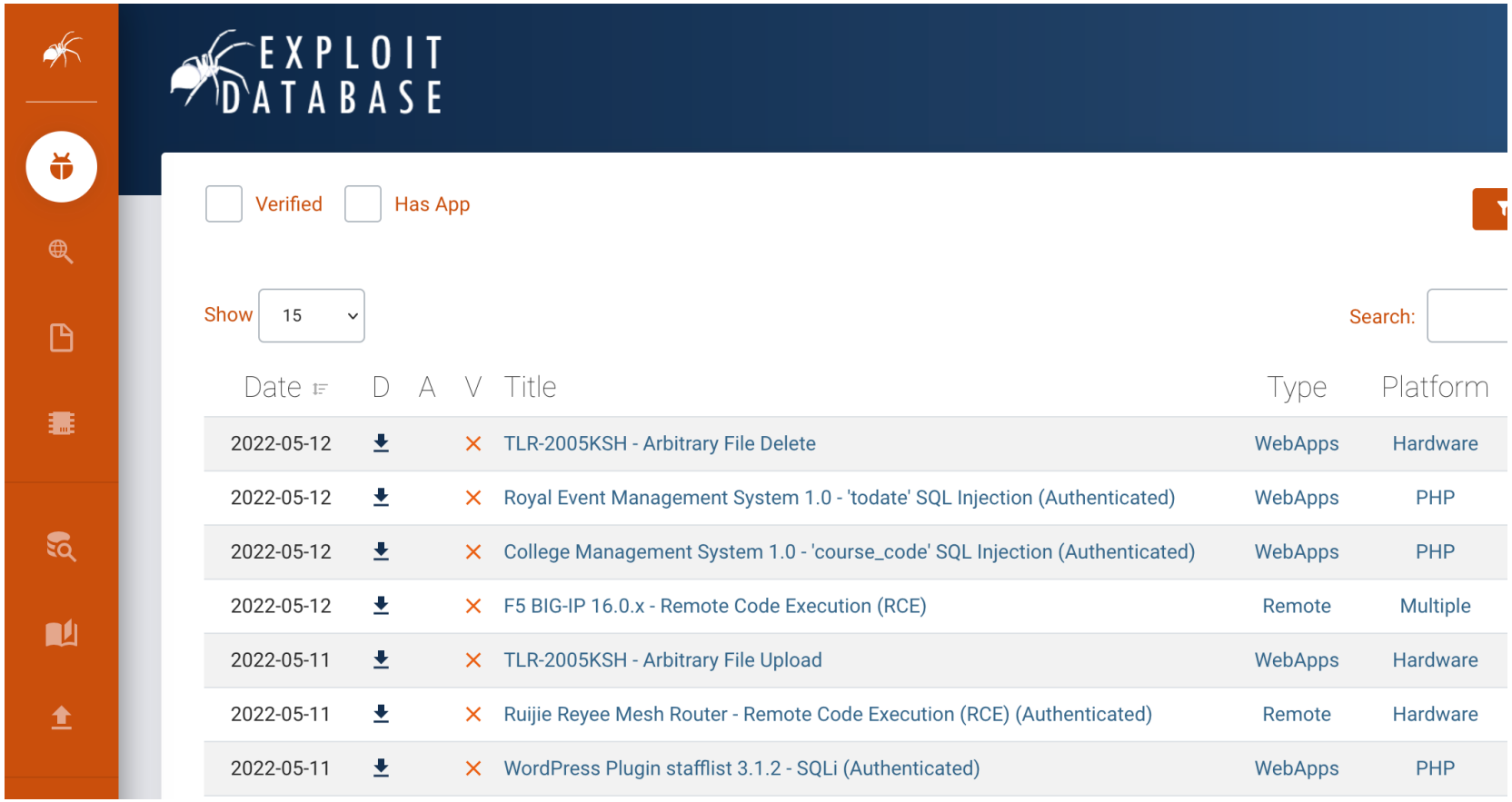


- Exploit = programový kód využívající zranitelnost

- Otevřený internet
  - Databáze exploitů
  - Open source databáze
  - Hackerská fóra

# Jak najít exploit – otevřený internet






https://www.exploit-db.com/



VIAVIS

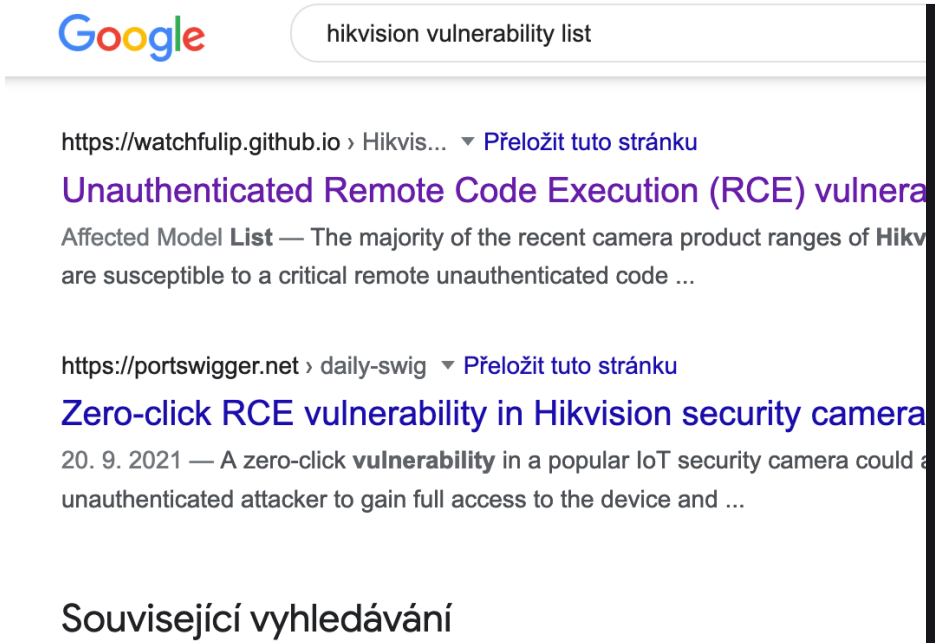
# Hackerem snadno a rychle - ukázka…



- OSINT – vyhledání zranitelností – kamery HIKVISION
  - Zranitelnost z roku 2016
  - Vyhledání zranitelných systémů
  - Získání exploitu
  - Plošný/cílený útok

# Kamery HIKVISION – OSINT zranitelností







https://watchfulip.github.io/2021/09/18/Hikvision-IP-Camera-Unauthenticated-RCE.html



VIAVIS

# Hurá na zranitelné systémy – kamery HIKVISION, kde jsou?



SHODAN | Explore | Downloads | Pricing | App-webs 2016 country:cz

TOTAL RESULTS

151

TOP CITIES

| | |
|---|---|
| Prague | 41 |
| Nymburk | 7 |
| České Budějovice | 7 |
| Ostrava | 6 |
| Brno | 5 |

More...

TOP PORTS

| | |
|---|---|
| 80 | 54 |
| 81 | 21 |
| 88 | 11 |
| 82 | 10 |

View Report | View on Map

**New Service:** Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

**185.36.160.104**

IP-185-36-160-104.brouzdal.cz
Brouzdal s.r.o.
Czechia, Neratovice

```
HTTP/1.1 200 OK
Date: Tue, 17 May 2022 06:36:25 GMT
Server: App-webs/
ETag: "8e5-1e0-573af102"
Content-Length: 480
Content-Type: text/html
Connection: close
Last-Modified: Tue, 17 May 2016 10:22:58 GMT

Hikvision IP Camera:
  Web Version: 4.0.1 build 160405
  Plugin Version: 3.0.6.1
  A...
```

**80.78.137.208**

208.137.78.80.client.nordic.tel
Nordic Telecom

```
HTTP/1.1 200 OK
Date: Tue, 17 May 2022 05:05:44 GMT
```

https://www.shodan.io/search?query=App-webs+2016+country%3Acz



VIAVIS

# Exploit – bez práce, jen hledat



EXPLOIT DATABASE

## Hikvision IP Camera versions 5.2.0 - 5.3.9 (Builds 140721 < 170109) - Access Control Bypass

| EDB-ID: | CVE: | Author: | Type: | Platfor | Date: |
|---|---|---|---|---|---|
| 44328 | N/A | MATAMORPH | WEBAPPS | | 2018-03-23 |

**EDB Verified:** ✕

```
# Exploit Title: Hikvision IP Camera versions 5.2.0 - 5.3.9 (Builds: 140721 - 170109) Backdoor
# Date: 15-03-2018
# Vendor Homepage: http://www.hikvision.com/en/
# Exploit Author: Matamorphosis
# Category: Web Apps
# Description: Exploits a backdoor in Hikvision camera firmware versions 5.2.0 - 5.3.9 (Builds:
deployed between 2014 and 2016, to assist the owner recover their password.
# Vulnerability Exploited: ICSA-17-124-01 - http://seclists.org/fulldisclosure/2017/Sep/23

#!/usr/bin/env python
# Usage: python exploit.py [IP Address] [Port] [SSL (Y/N)]

import requests
import re
import sys
```

https://www.exploit-db.com/exploits/44328



VIAVIS

# Výsledek…



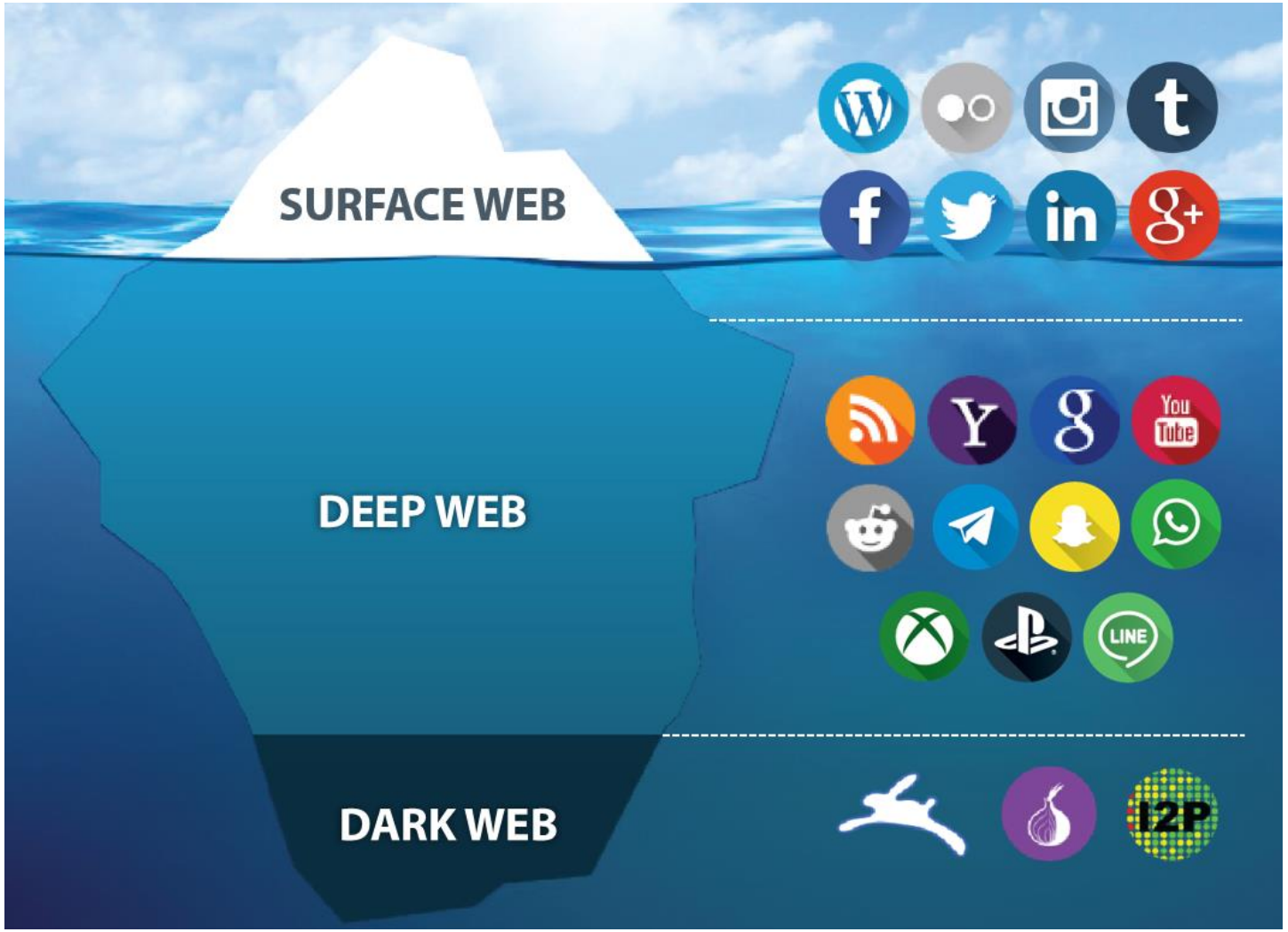
# Maximální využití OSINT



- Hádejte:
  - ***Proč je OSINT pro útočníky tak efektivní?***
  - ***Co je pro oběť incidentu při jeho zvládání nejobtížnější?***

# Darknet a deepweb - nové možnosti






- Nedoporučuji zkoušet

Nestahovat

Neotevírat

Anonymita

https://www.verint.com



VIAVIS

# The Hidden Wiki



**TheHidden.Wiki** TOR Onion Directory

## Verified Dark Web Links 2022

### Hidden Wiki

Hidden Wiki has been the directory for TOR onion links for the past decade, listing only verified dark web links.

Last Updated on **May 2022.**

Install TOR Browser from http://torproject.org/

Uncensored Hidden Wiki can be accessed using wiki47qgn6tey4id7xeqb6l7uj6jueacxlqtk3adshox3zdohvo35vad.onion

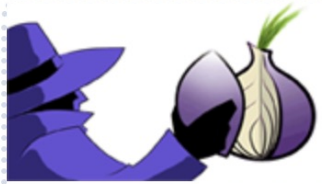
Take a minute and check our scam list to know more about dark web scammers.

### Hidden Search Engines

- http://oniondxjxs2mzjkbz7ldlflenh6huksestjsisc3usxht3wqgk6a62yd.onion/ — OnionIndex Search Engine
- http://duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt6twagswzczad.onion/ — DuckDuckGo Search Engine
- http://3bbad7fauom4d6sgppalyqddsqbf5u5p56b5k5uk2zxsy3d6ey2jobad.onion/ — OnionLand Search
- http://tordexu73joywapk2txdr54jed4imqledpcvcuf75qsas2gwdgksvnyd.onion/ — tordex
- http://xmh57jrknzkhv6y3ls3ubitzfqnkrwxhopf5aygthi7d6rplyvk3noyd.onion/ — Torch

# The Hidden Wiki





OnionLinks

## *OnionLinks*

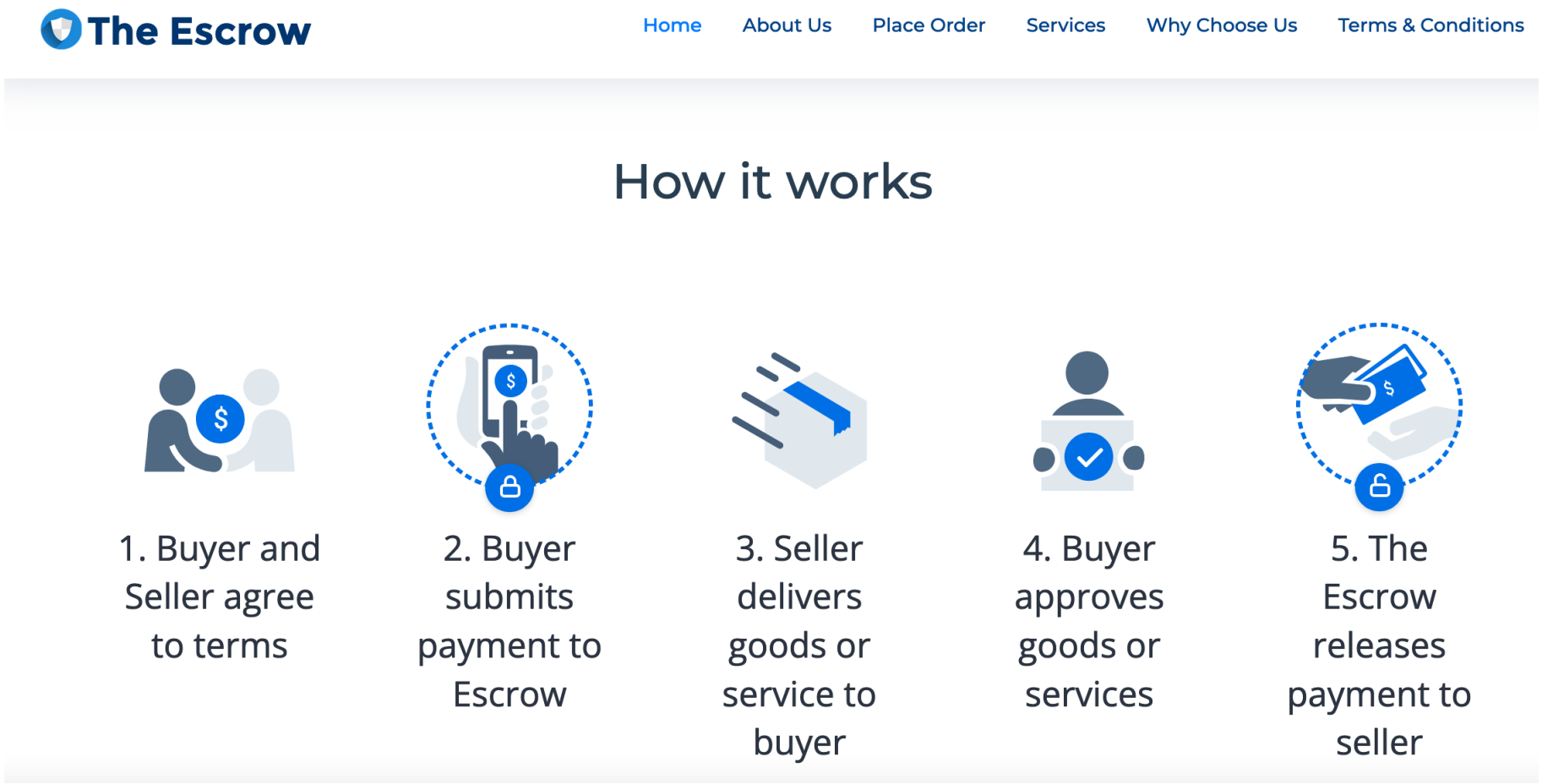
Short .onion v2 websites will stop working in October 2021. Bookmark OnionLinks or **DARKWEBLINKS.COM** for working v3 .onion sites!

**Navigation:**

**Introduction Points**
**Financial Services**
**Commercial Services**
**Drugs**
**Chans**
**Privacy Services**
**Email Providers**
**Blogs And Personal Sites**
**Hacking**
**News Sites**
**Open Source Software**
**Others**

# Dark Market – možný model








VIAVIS

# OSINT – vazby, souvislosti



## Organizations related to intel.com

**ORGANIZATION DETAILS**

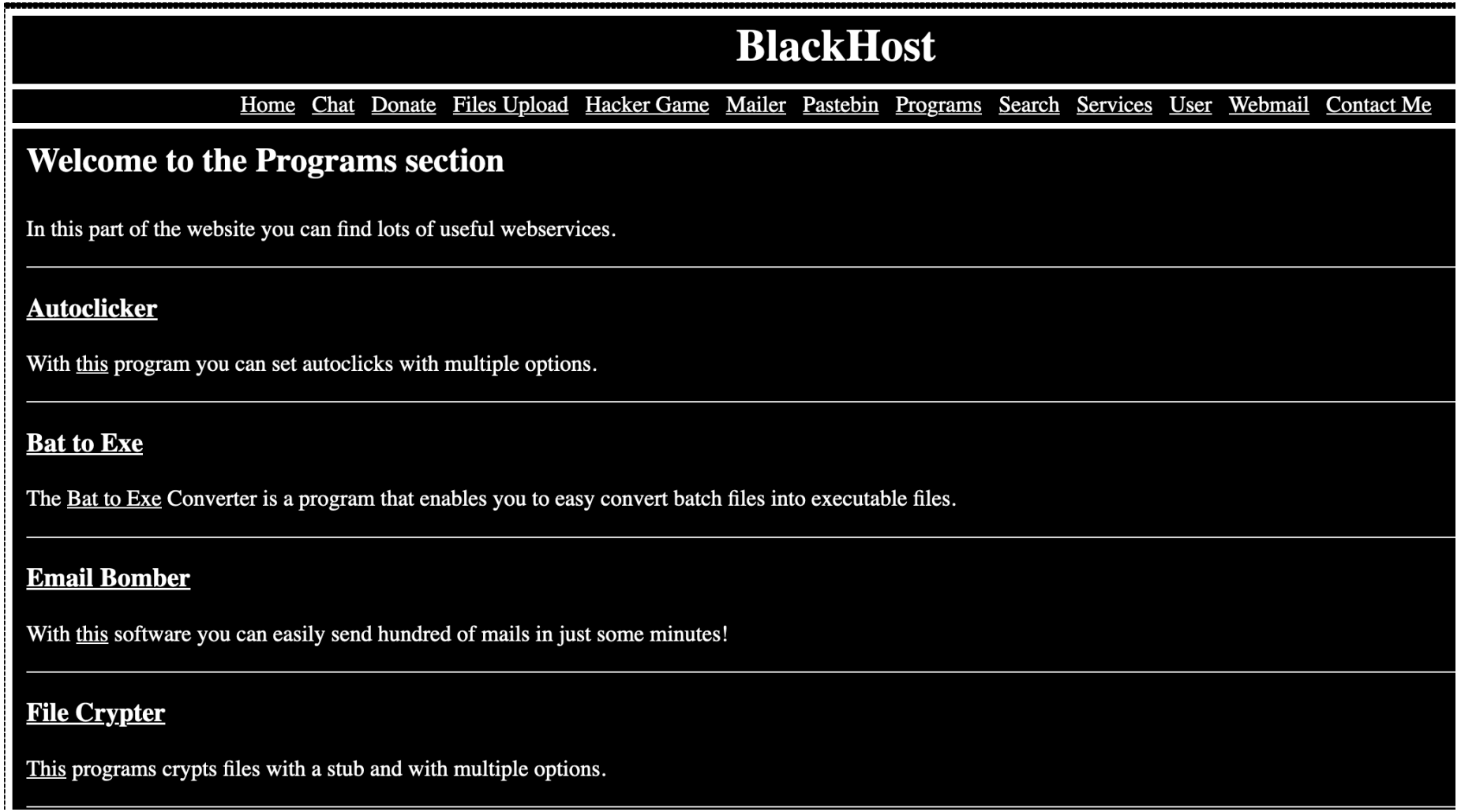
Host intel.com
Name Intel
Contacts 2,868
Documents 1,219
Related 17,685 organizations. Wildcards (*.org, *.edu, *.com, *.gov... ) available.

What this information means and where it comes from

| | Name | Site | Share of all intel.com contacts | Share of all related site contacts | Affinity index | Common contacts |
|---|---|---|---|---|---|---|
| 1 | International Business Machines | us.ibm.com | 27.36% | 14.88% | 3 | view |
| 2 | Hewlett-Packard | hp.com | 23.55% | 17.31% | 2 | view |
| 3 | Army Knowledge Online (AKO) | us.army.mil | 17.49% | 4.46% | 79 | view |
| 4 | Qwest.net | uswest.net | 17.21% | 8.68% | 32 | view |
| 5 | IEEE - Networking The World | ieee.org | 16.08% | 12.32% | 8 | view |
| 6 | Cisco Systems | cisco.com | 15.80% | 16.79% | 4 | view |
| 7 | Association for Computing Machinery (ACM) | acm.org | 15.37% | 17.93% | 12 | view |
| 8 | Microsoft | microsoft.com | 15.23% | 7.63% | 26 | view |

# Darknet nabízí další možnosti – ZeroDay Vulnerabilities





**BlackHost**

Home Chat Donate Files Upload Hacker Game Mailer Pastebin Programs Search Services User Webmail Contact Me

## Welcome to the Programs section

In this part of the website you can find lots of useful webservices.

---

**Autoclicker**

With this program you can set autoclicks with multiple options.

---

**Bat to Exe**

The Bat to Exe Converter is a program that enables you to easy convert batch files into executable files.

---

**Email Bomber**

With this software you can easily send hundred of mails in just some minutes!

---

**File Crypter**

This programs crypts files with a stub and with multiple options.

---

# Proč si hlídat digitální identitu

## Dox

Stolen identity. Humiliating photos. Blackmail. Stupid chicks and few guys 😉 All profiles apply only to adults. If you are one of the girls, and want your profile to be removed from the site, or you are a boyfriend, of one, of the girls and want to help her disappear from the network, please contact us using the contact form. For only $ 1000 in BTC, your profile will be removed from this shop. Stay safe!

Default sorting | Showing 1–15 of 55 results | 1 2 3 4 ▸

Adrianna Ba

$3.00

Add to cart

Agnieszka C.

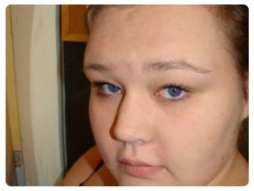
$5.00

Add to cart

Agnieszka Kl.

$3.00

Add to cart



Aleksandra Bo.

$4.00

Add to cart

Aleksandra Sn.

$6.00

Add to cart

# Jde i o osobní bezpečnost



| | | |
|---|---|---|
| Remote control the phone of someone else, most new models supported | 700 USD = 0.02348 ฿ | 1 X Buy now |
| Facebook and Twitter account hacking | 500 USD = 0.01677 ฿ | 1 X Buy now |
| Other social network account hacks, for example reddit or instagram | 450 USD = 0.01510 ฿ | 1 X Buy now |
| Full package deal, getting access to personal or company devices and accounts and searching for the data you need. | 1800 USD = 0.06038 ฿ | 1 X Buy now |
| DDOS for protected websites for 1 month | | |
| DDOS for unprotected websites for 1 month | | |
| Hacking webservers, game servers or other internet infrastructur | | |

| Product | Price | Quantity |
|---|---|---|
| Destroying someones life: Your target will have legal problems or financial problems, proven methods including child porn that always works | 1700 USD = 0.05703 ฿ | 1 X Buy now |
| Spreading false information about someone on social media, not as life ruining but still nasty | 450 USD = 0.01510 ฿ | 1 X Buy now |
| Social engineering to get secrets from a person, private or from some employee | 450 USD = 0.01510 ฿ | 1 X Buy now |
| Other social engineering work | 500 USD = 0.01677 ฿ | 1 X Buy now |
| 30 days full service, i will work 8 hours per day for 30 days only on your project | 7500 USD = 0.25160 ฿ | 1 X Buy now |

# Pro představu…



| Product | Price | Quantity |
|---|---|---|
| Czech ID Card | 500 EUR = 0.01729 ฿ | 1 X Buy now |
| Netherlands ID Card | 550 EUR = 0.01902 ฿ | 1 X Buy now |
| Denmark ID Card | 550 EUR = 0.01902 ฿ | 1 X Buy now |

# Zranitelnosti, exploity…



Darknetlive

Home Arrests Markets Crypto Forums Onions Sh

Home / Posts / Paris: Versus Market Exploit “is Real”

## Paris: Versus Market Exploit “is Real”

~14 mins | Published by Darknetlive on 18 May, 2022 in News and tagged Darkweb Markets using 2948 words. | 16 Comments

The Versus Market exploit is legitimate, Paris claimed.

A user on Dread (/u/threesixty) hacked Versus Market “in a time span of about 2 hours,” according to a post on th Versus subdread. “Please remove security driven from your website title. You are not security driven.”

Hacked, you are not security driven

by /u/threesixty · 2 days ago* in /d/Versus

Please remove security driven from your website title. You are not security driven. Yes, I could probably just extort you or become a payoff for keeping quite about this, but no thank you. You can still pay me though.
This happened in a time span of about 2 hours. Think about what LE and advanced hackers might have done in the meantime.



VIAVIS

# Proč to vše?



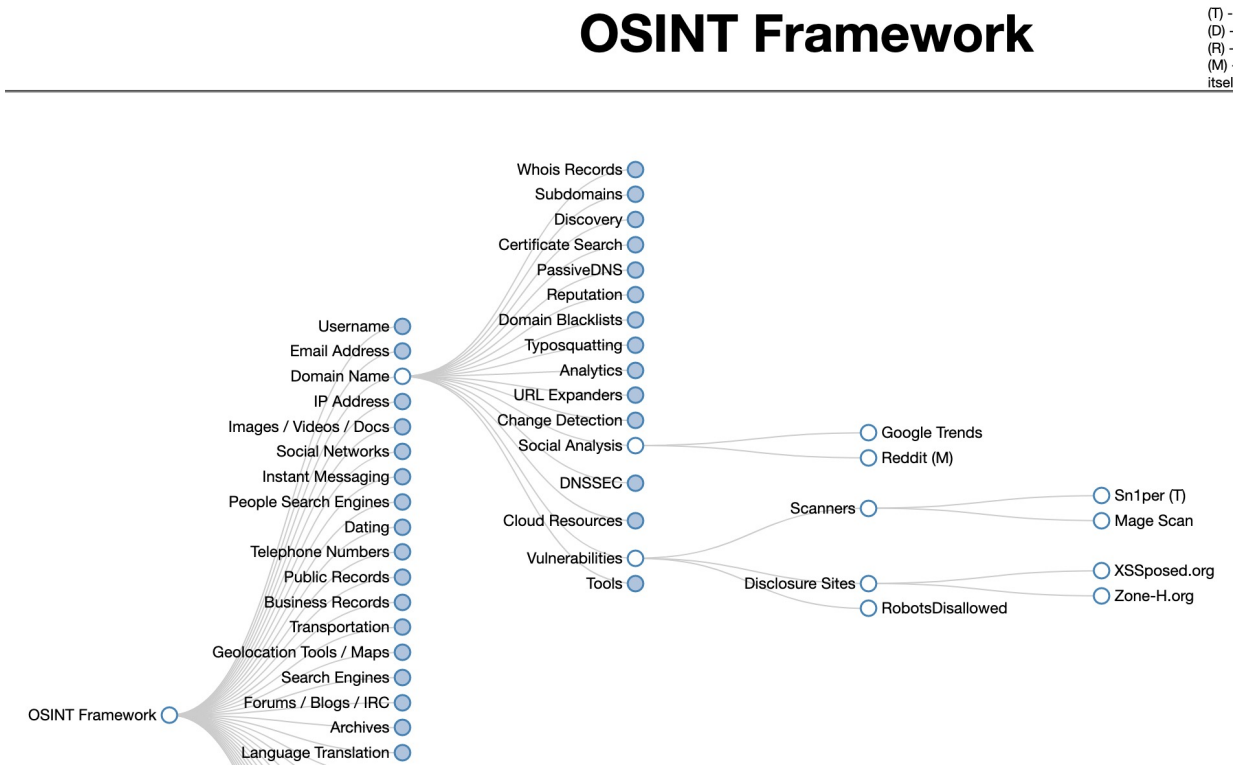
- Útoky jsou dostupnější
- **Nepřitahovat pozornost**
  - Sledovat zranitelnosti
  - Odstraňovat je
  - Nekomunikovat je
- **OSINT jako nezbytná součást kyber bezpečnosti**
- **OSINT je součástí investigativní práce**

***Kdo si udělal na sebe/organizaci profesionální OSINT?***

# Nepřitahovat pozornost – vědět, co se ví…



- Bezpečnost organizace
  - Sledovat zranitelnosti - systematicky
  - Odstraňovat je
  - Nekomunikovat je
- Osobní bezpečnost
  - Digitální identita pod kontrolou
  - Digitální stopa pod kontrolou
  - Osobní zařízení pod kontrolou
  - OSINT, OSINT, OSINT…




https://osintframework.com/



VIAVIS

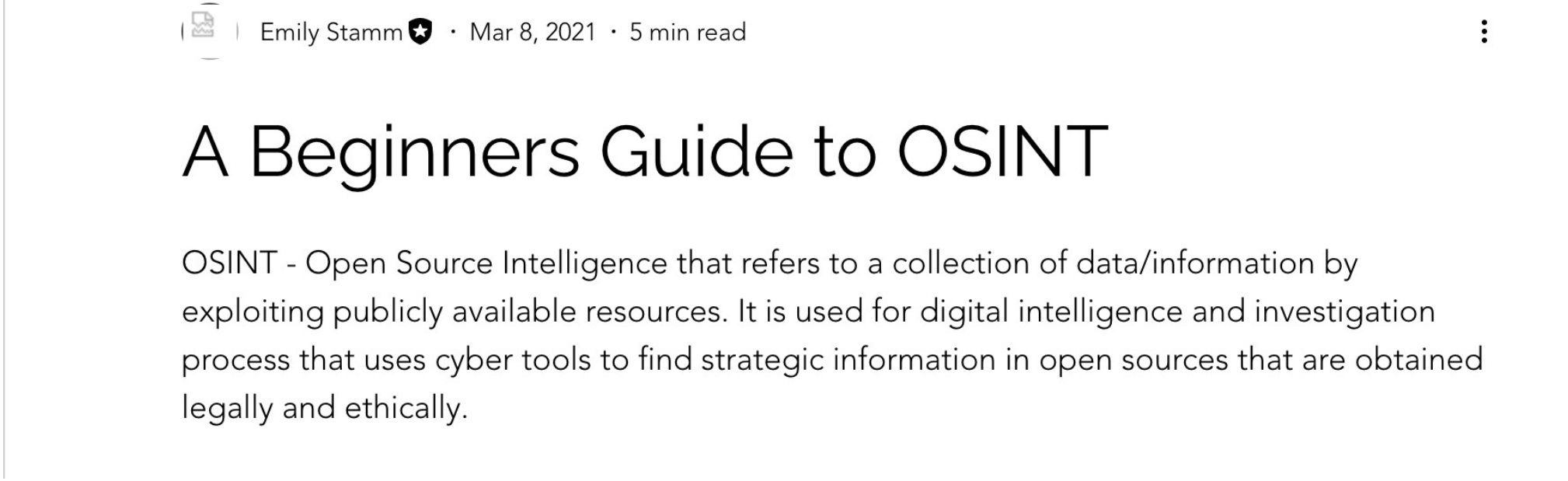
# Útoky s využitím OSINT – nejen technické



- Vydírání s využitím extrakce dat
- Phishing a vishing
  - Využití digitální identity a známého hesla
  - Znalost spojení osoba(organizace)/banka
- Přesměrování plateb
  - Zdroj = registr smluv
  - Cílené reputační útoky
  - **Český jazyk – pomalu ztrácí svou výhodu**

# OSINT – Open Source Intelligence





Emily Stamm · Mar 8, 2021 · 5 min read

## A Beginners Guide to OSINT

OSINT - Open Source Intelligence that refers to a collection of data/information by exploiting publicly available resources. It is used for digital intelligence and investigation process that uses cyber tools to find strategic information in open sources that are obtained legally and ethically.

https://www.csnp.org/post/a-beginners-guide-to-osint

# OSINT – něco odkazů pro inspiraci

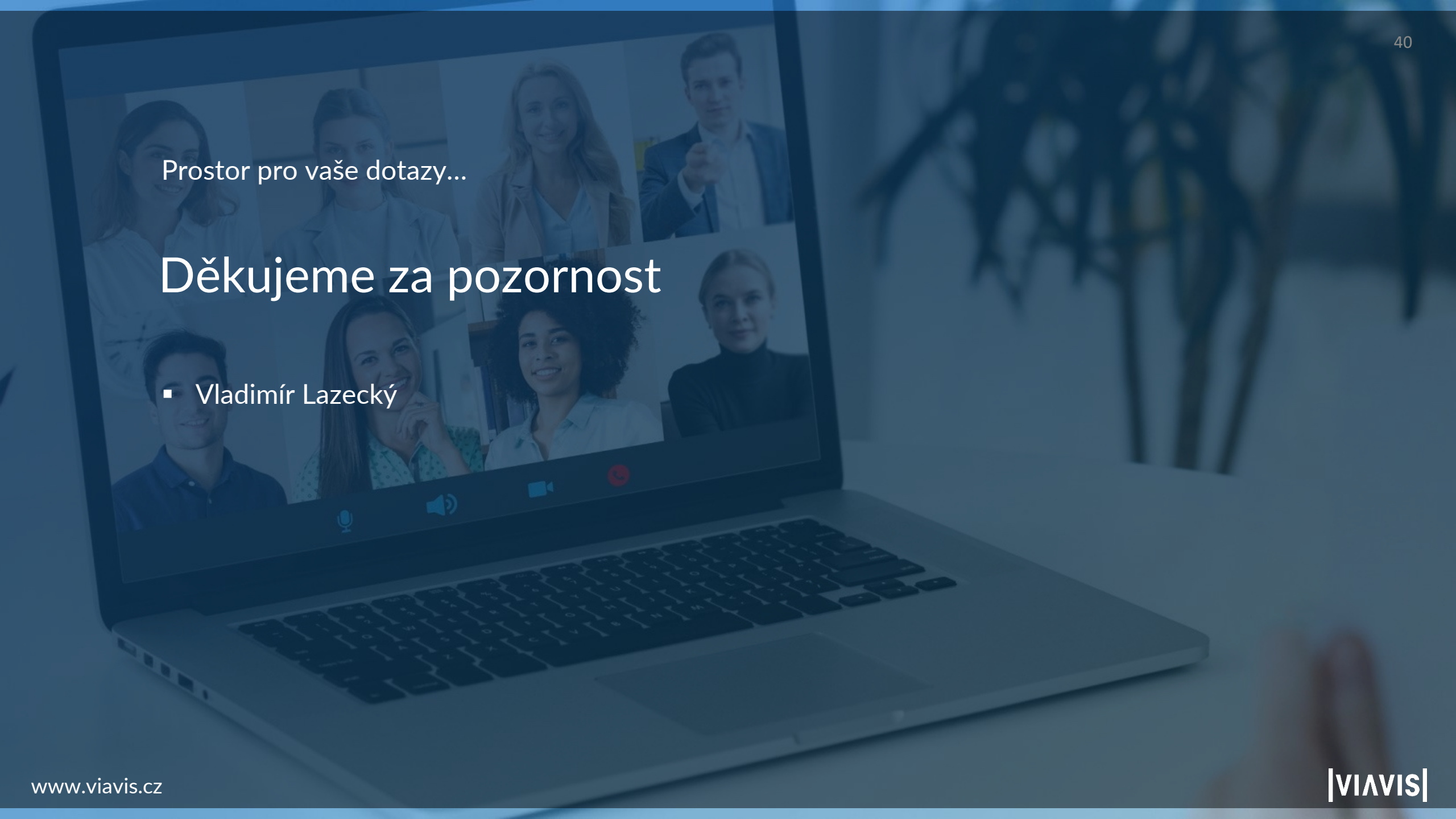



https://i-intelligence.eu/

# Úkol



- **Vyberte si oběť**
  - MS Kraj…
- Vymyslete, jak zaútočíte
- Prezentujte



Prostor pro vaše dotazy…

# Děkujeme za pozornost

- Vladimír Lazecký