VIAVIS střežíme podstatné

Kyber bezpečnost

Útoky na aplikace

Vladimír Lazecký

Obsah přednášky

- Útoky na aplikace – trendy
- Jak se stát hackerem snadno a rychle
- Darknet

Trendy

- Útoky jsou čím dál dostupnější laikům
- Snadné provedení
- Oběti samy útok přivolají
- OSINT – velmi efektivní pro plánování útoků

Jak se stát hackerem snadno a rychle

- Vyhledávání zranitelností
- Databáze exploitů
- Identifikace cílů
- Otevřený internet
- Darknet

Hledání zranitelností

- Otevřený internet
  - Oficiální databáze:
    - Národní autority
    - Open source databáze
    - Placené databáze
    - Zprávy v otevřených zdrojích
    - Výrobci (rizika Zero Day Vulnerability)
  - Darknet

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

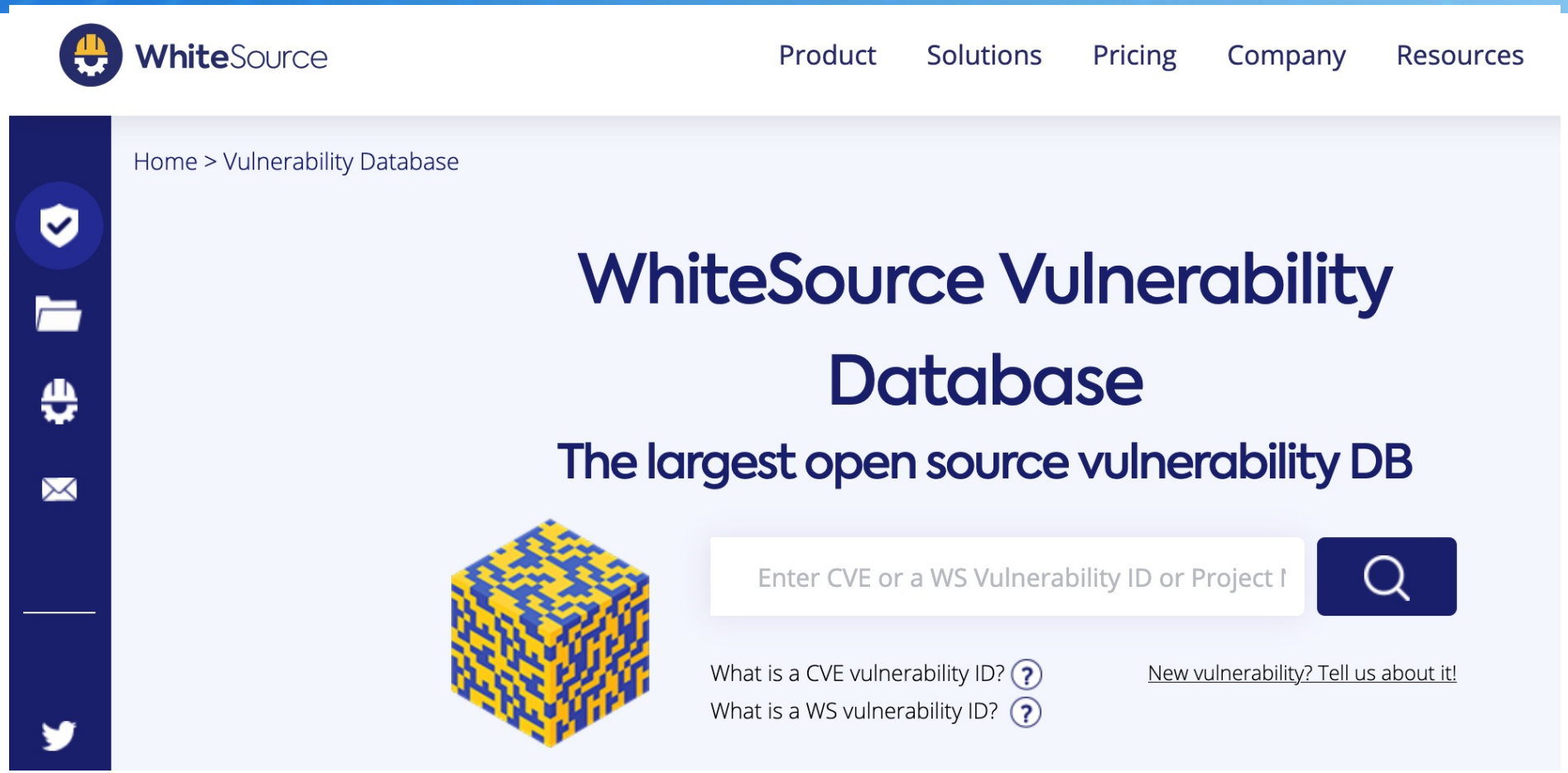
https://www.cisa.gov/known-exploited-vulnerabilities-catalog

VIAVIS

Zranitelnosti – otevřený internet – blogy, články

https://portswigger.net/daily-swig/vulnerabilities

Zranitelnosti – otevřený internet – placené databáze



https://www.whitesourcesoftware.com/vulnerability-database/

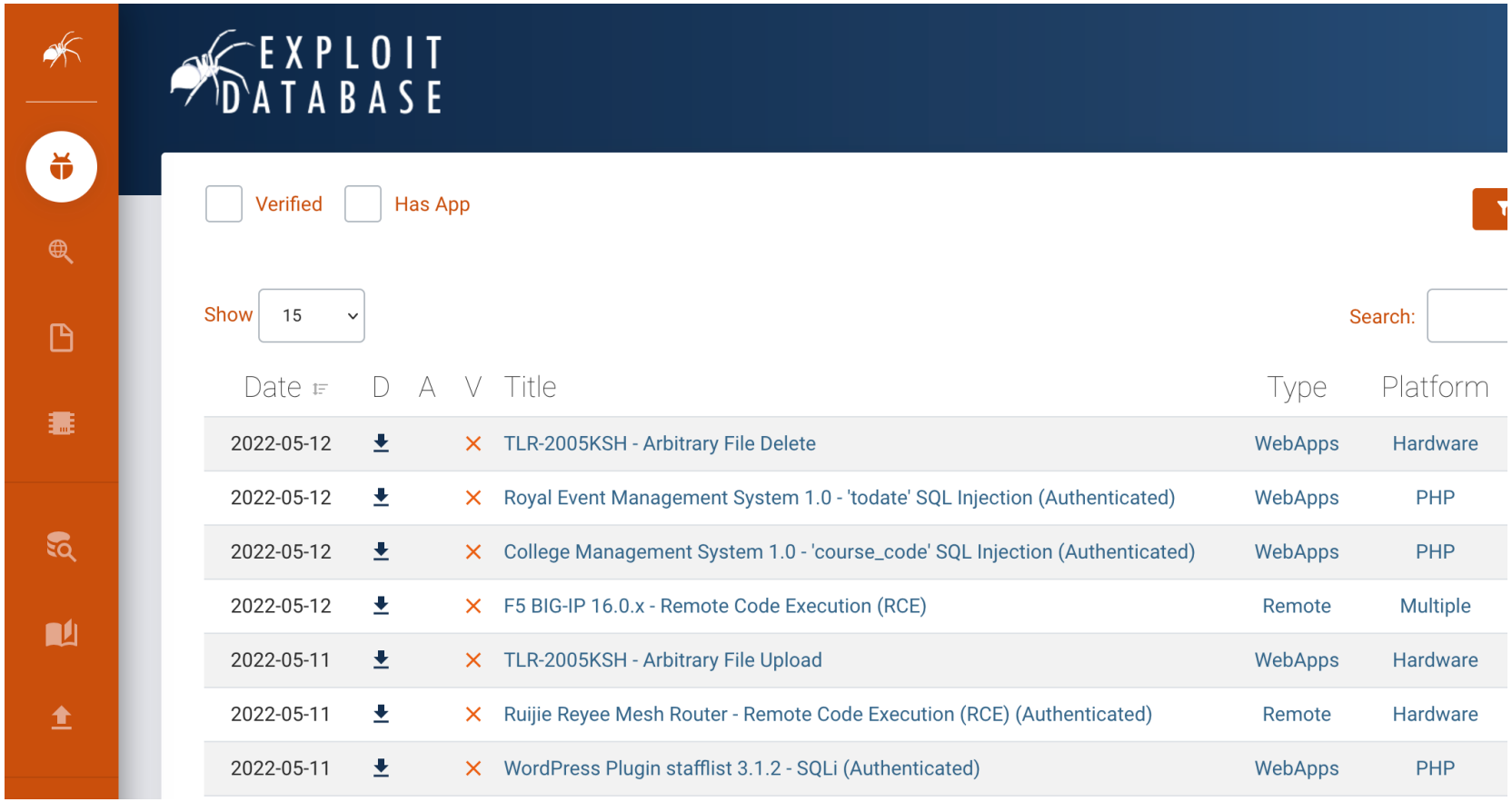
Hledání exploitů

- Exploit = programový kód využívající zranitelnost

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

  - Darknet

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 útok

Kamery HIKVISION – OSINT zranitelností

Watchful_IP›_

Security researching in the middle of the night.
Focusing on ARM based embedded IoT

Unauthenticated Remote Code Execution (RCE) vulnerability in Hikvision IP camera/NVR firmware (CVE-2021-36260)

Published on 18 Sep 2021

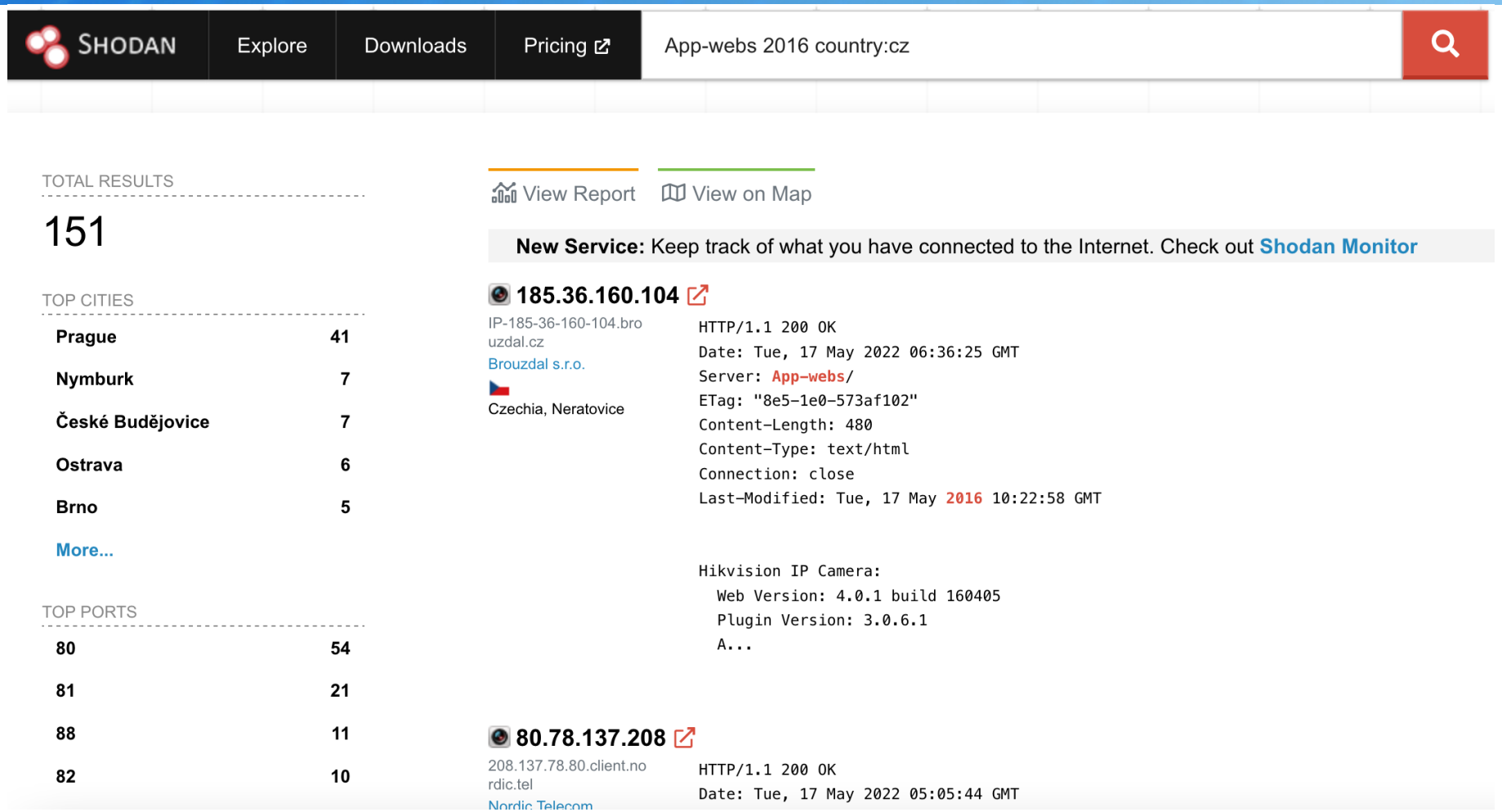
› This article has been written for a technical audience._

Vulnerability discovered 20 June 2021

Table of Contents:

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

Hurá na zranitelné systémy – kamery HIKVISION, kde jsou



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

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 OSIS	WEBAPPS		2018-03-23

EDB Verified: ✕

Explo

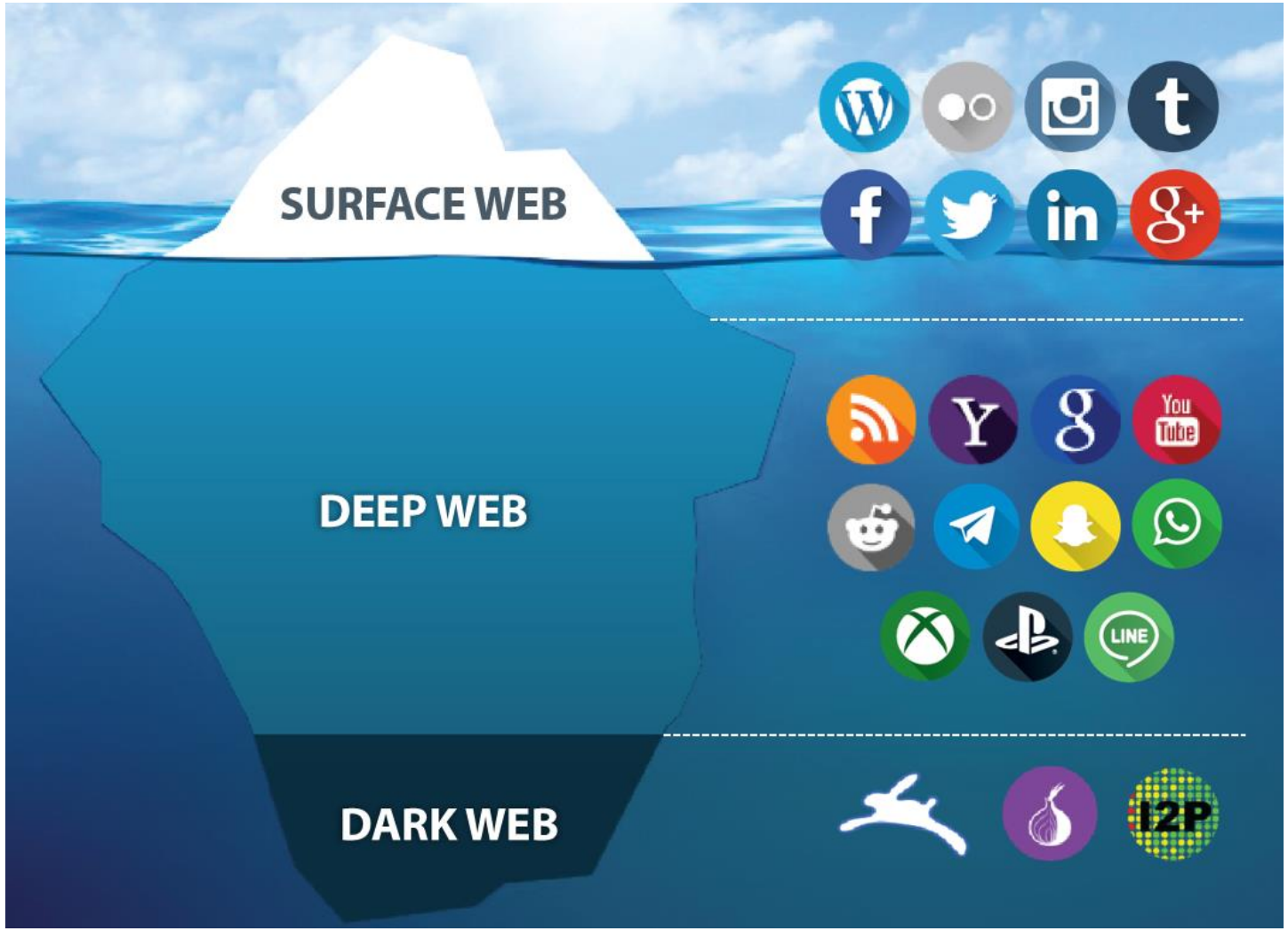
https://www.exploit-db.com/exploits/44328

```
# 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
```


VIAVIS

Výsledek…

Darknet… - začneme internetem



Deepweb x Darknet

- Deepweb:
  - Stránky neindexované vyhledávači
  - Používají HTTP/HTTPS protokoly
  - Lze se na ně dostat běžným prohlížečem
  - Je nutné znát adresu
  - Části firemních extranetů, blogy, eshopy…

Deepweb x Darknet

- Darknet:
  - Stránky přístupné pomocí speciálních prohlížečů TOR…
  - Snaha o anonymitu - onion
  - Je nutno znát adresu
  - Nefunkční vyhledávače
  - HiddenWiki
  - POZOR – využití pro nelegální činnost
  - Plnou anonymitu nikdo nezaručí
  - **NIC NESTAHOVAT**

Darknet

- Legální obsah
  - Alternativní články, zpravodajství
  - Diskusní fóra
  - Informační obsah nelegální v některých zemích
  - Vazby – společnosti, osoby, transakce
- Nelegální obsah
  - Tržiště – nelegální zboží
  - Kriminální činy
  - Hackerská fóra
  - **Obsah, který nechcete vidět**

Způsoby připojení

Anonet
?

Freenet
A darknet that is primarily concerned with censorship rather than privacy. It is used for storing data. Will expose your IP unless you use another darknet (ie a VPN) in conjunction, or only use peers you trust.

Tor
The most well known of darknets, and one of the first. One of the best for circumventing firewalls. Tor operates by routing a given connection through a series of nodes, and optionally a bridge if necessary.

I2P

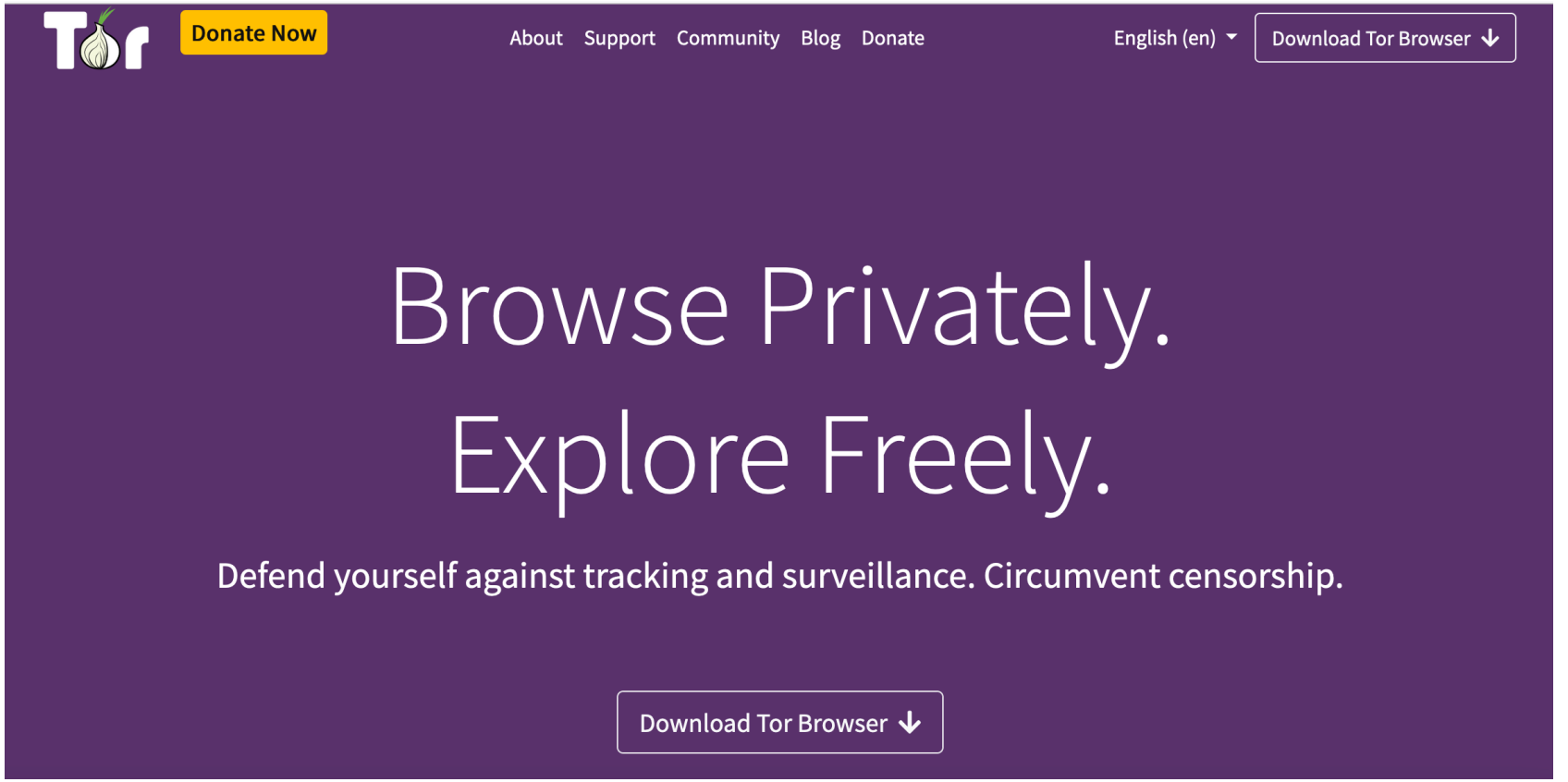
The second most well known darknet, I2P operates in a peer-to-peer manner.

I2Prouter	https://geti2p.net/	Written in Java, the standard router
I2P+	https://i2pplus.github.io/	A fork of the Java router
I2Pd	https://i2pd.website/	Written in C++, is easier on resources and more minimal
Kovri	https://web.getmonero.org/resources/moneropedia/kovri.html [Archive]	An in-development i2p thing designed for the Monero/XMR cryptocurrency

Gnunet
?

Lokinet
An onion router that seeks to fix Sybil attacks by way of having exit nodes be invested in. http://web.archive.org/web/20211228031014/http://cheapskatesguide.org/articles/lokinet.html

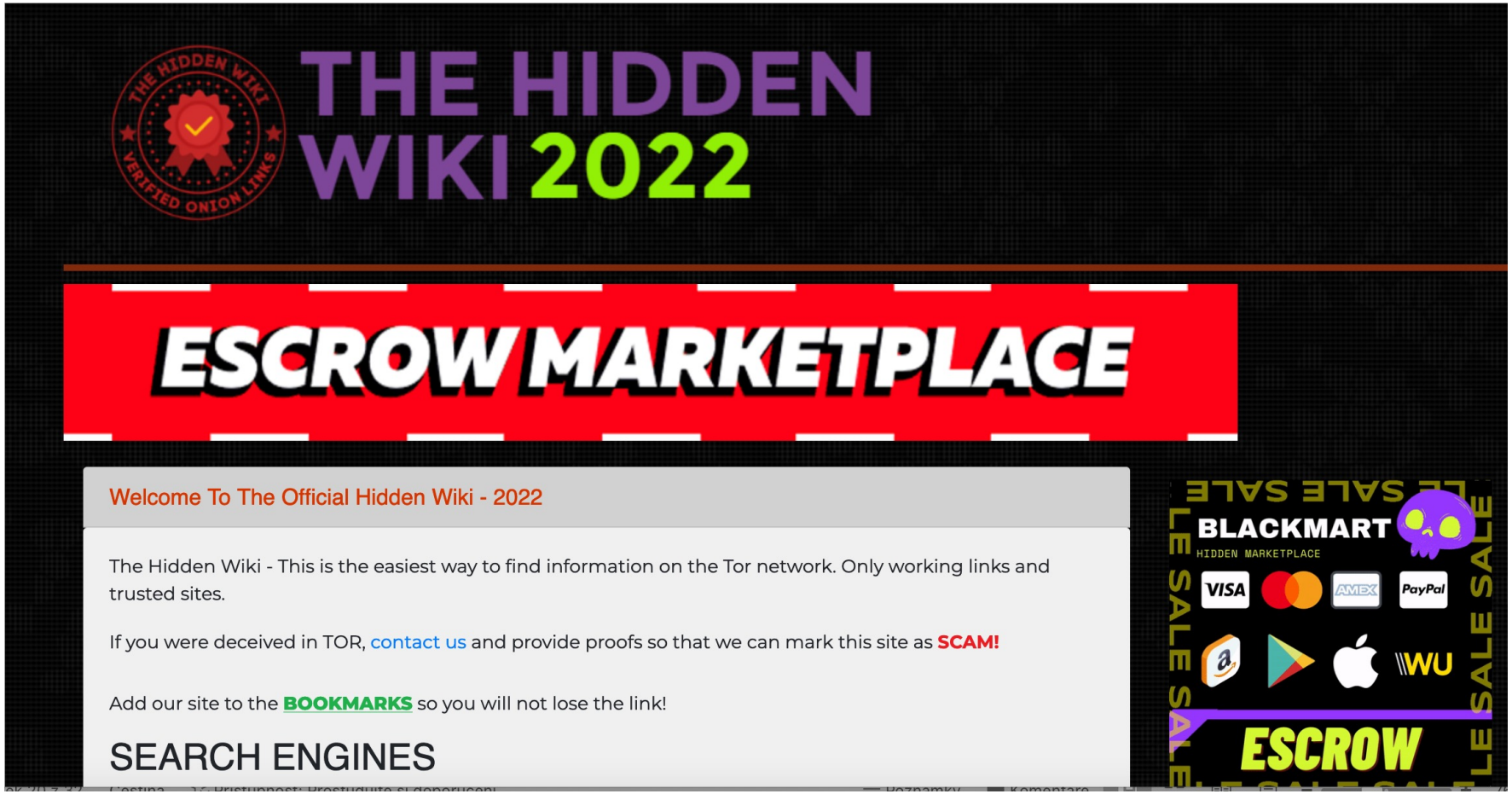
TOR – dále už bez odkazů…



„Bezpečný“ OS

VIAVIS

The Hidden Wiki



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/

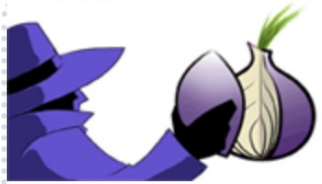
Uncensored Hidden Wiki can be accessed using wiki47qgn6tey4id7xeqb6l7uj6jueacxlqtk3adshox3zdohvo35vad.onion

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

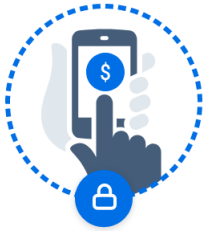
Dark Market – možné fungování

The Escrow

Home About Us Place Order Services Why Choose Us Terms & Conditions

How it works

1. Buyer and Seller agree to terms



2. Buyer submits payment to Escrow

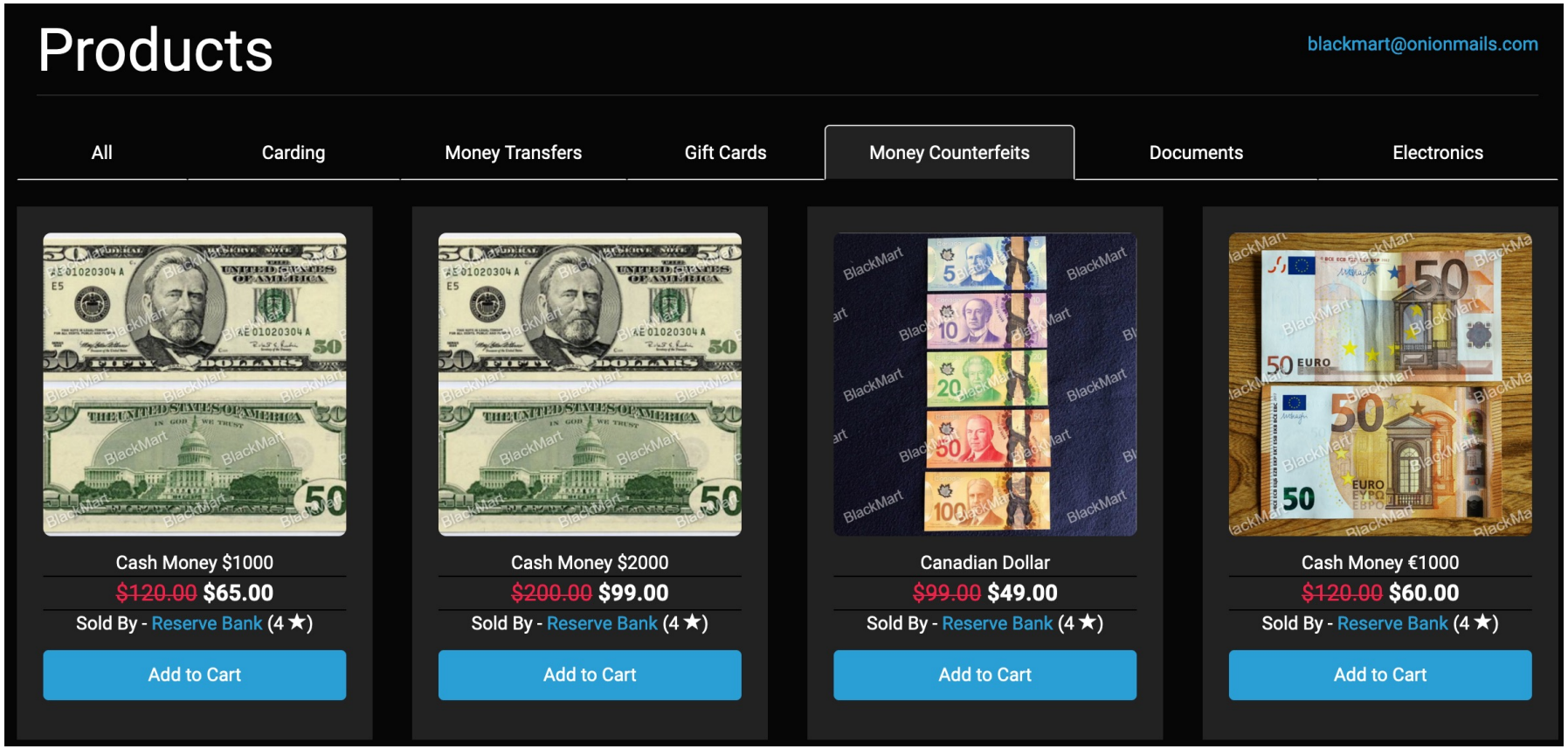
3. Seller delivers goods or service to buyer

4. Buyer approves goods or services

5. The Escrow releases payment to seller

VIAVIS

Dark Market – trestná činnost



OSINT – vazby, souvislosti

Organizations related to intel.com

ORGANIZATION DETAILS

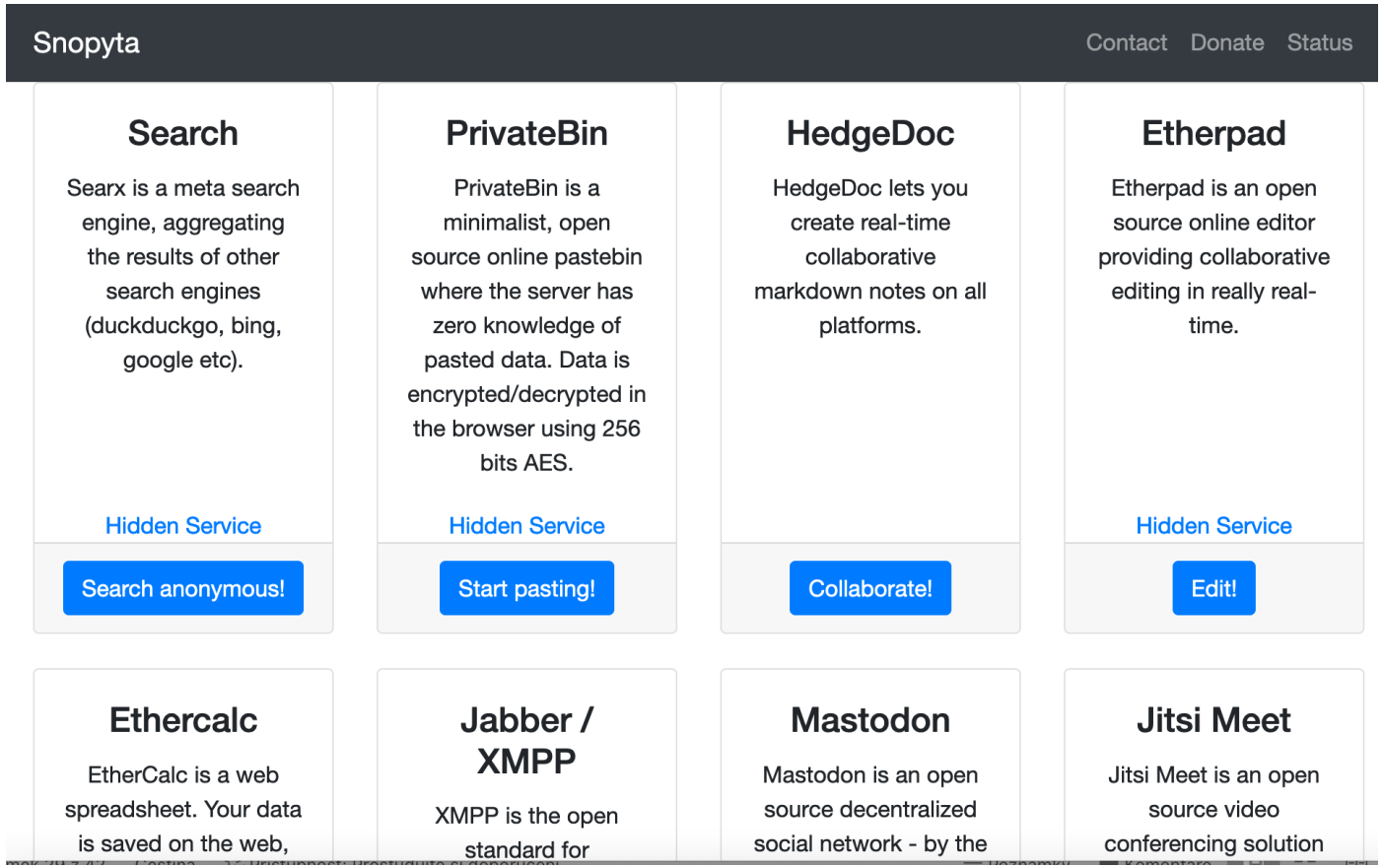
Host intel.com
Name Intel
Contacts 2,868
Documents 1,219
Related 17,685 organizations. Wildcards (*.org, *.edu, *.com, *.gov...) available.

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

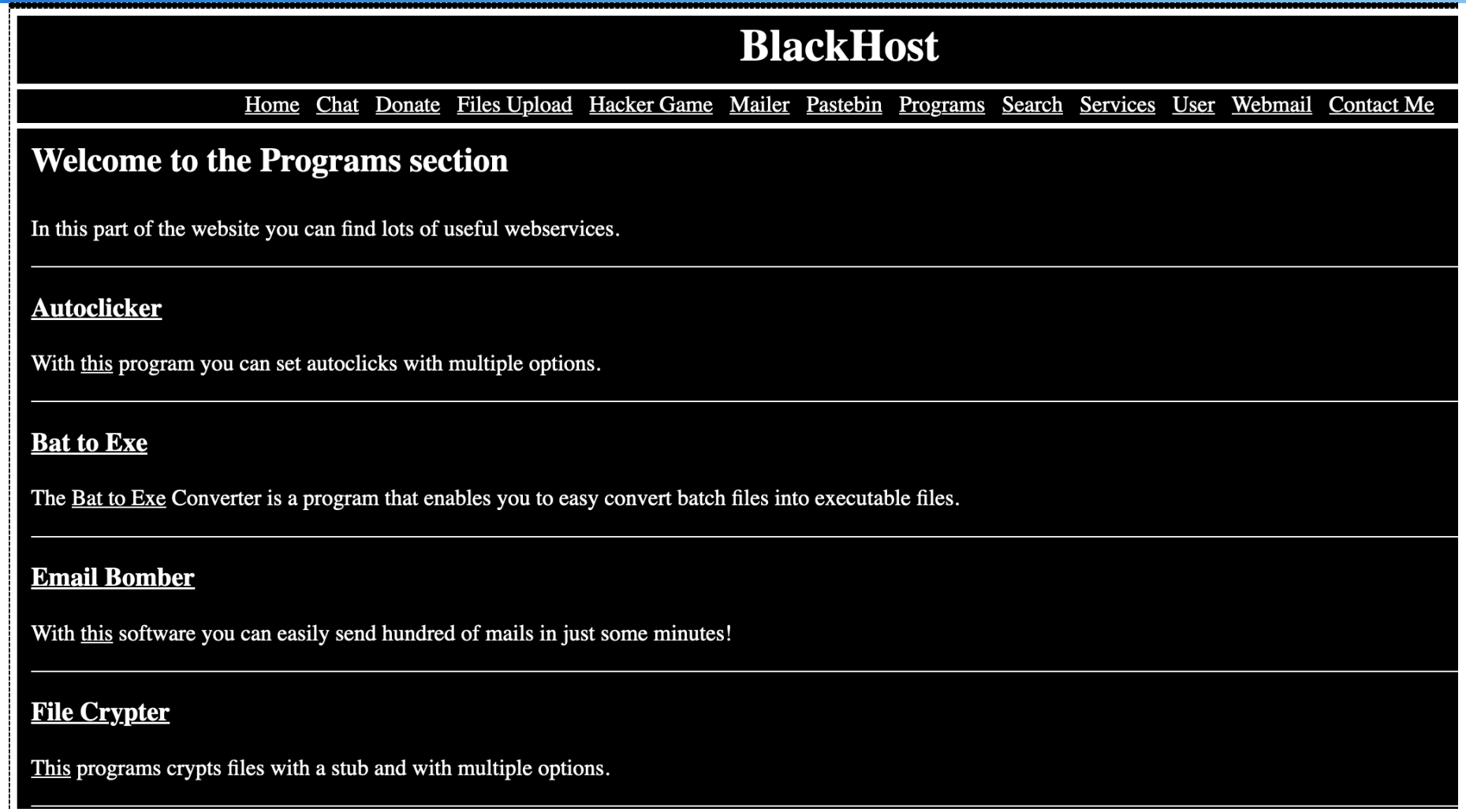
VIAVIS

Hidden services



VIAVIS

Darknet nabízí další možnosti…



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.

Spyware – analýza SW

Articles Mirrors Misc

Online Spyware Watchdog

The goal of this website is to classify spyware programs, so that users can be more aware that they are installing spyware.

Many "everyday" applications are actually spyware. **We take an expansive and strict stance on what constitutes spyware.** We define spyware as anything that includes telemetry, phoning home, automatic updates or is listening in without the user's knowledge or consent.

This website contains articles on popular programs with explanations of the spyware features found in them. Included are easy to understand ratings, detailed explanations, and proof, of how features of these programs can spy on the user.

If you want to contribute to this website, you can always make a pull request.
All contributions must be licensed under the CC0 license to be accepted.

PUBLIC DOMAIN

Uživatelské účty

Digital Thrift Shop

Best digital stuff in Tor network!

Search products…

Shop | Announcements | About | Terms and conditions | My account | Help | $0.00 0 items

Home › Data Leak › Facebook users

Facebook users

$4.00

0.00013731	0.0203419	46.389607
29,130.48 USD/BTC	196.64 USD/BCH	0.086 USD/DOGE
0.0592544	0.070027	0.02434
67.51 USD/LTC	57.12 USD/DASH	164.34 USD/XMR

Product categories

- Apps (24)
- Books (70)
- Botnets (5)
- Data Leak (12)
- Databases (51)
- Docs (30)

VIAVIS

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.

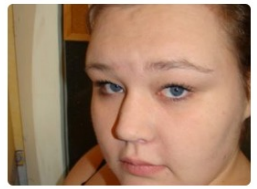
$5.00

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

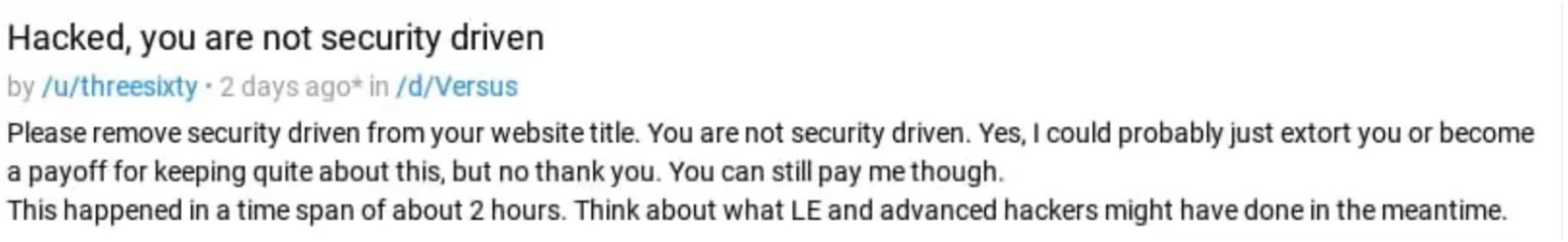
Home / Posts / Paris: Versus Market Exploit “is Real”

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

Zranitelnosti, exploity…

Darknetlive

Home Arrests Markets Crypto Forums Onions Sh

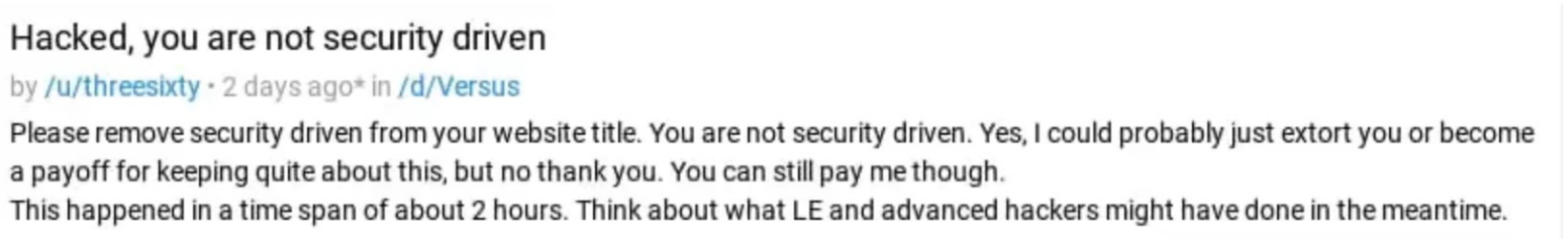
Home / Posts / Paris: Versus Market Exploit “is Real”

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

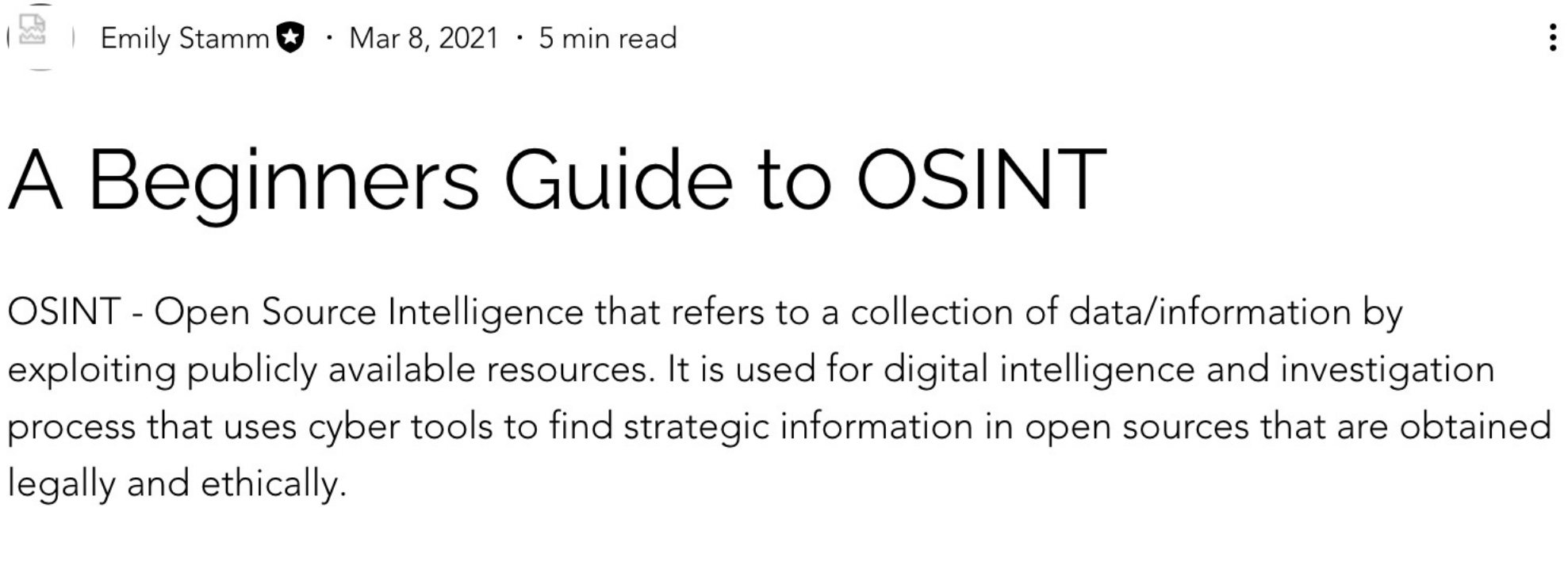
Lze se bránit? Ano, lze

- Brát bezpečnost vážně
  - Důslednost, systematičnost, vytrvalost
- Nepřitahovat pozornost
  - Sledovat zranitelnosti
  - Odstraňovat je
  - Nekomunikovat je
- Mít svou digitální stopu pod kontrolou
  - OSINT
  - Proaktivní kroky

Proč OSINT

- Trend v plánování útoků (nejen kyber)
  - Útoky na organizace
  - Útoky na osoby
- OSINT lze jen velmi obtížně zachytit
- Český jazyk – pomalu ztrácí svou výhodu
- Kdo z nás má svou digitální stopu pod kontrolou?

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

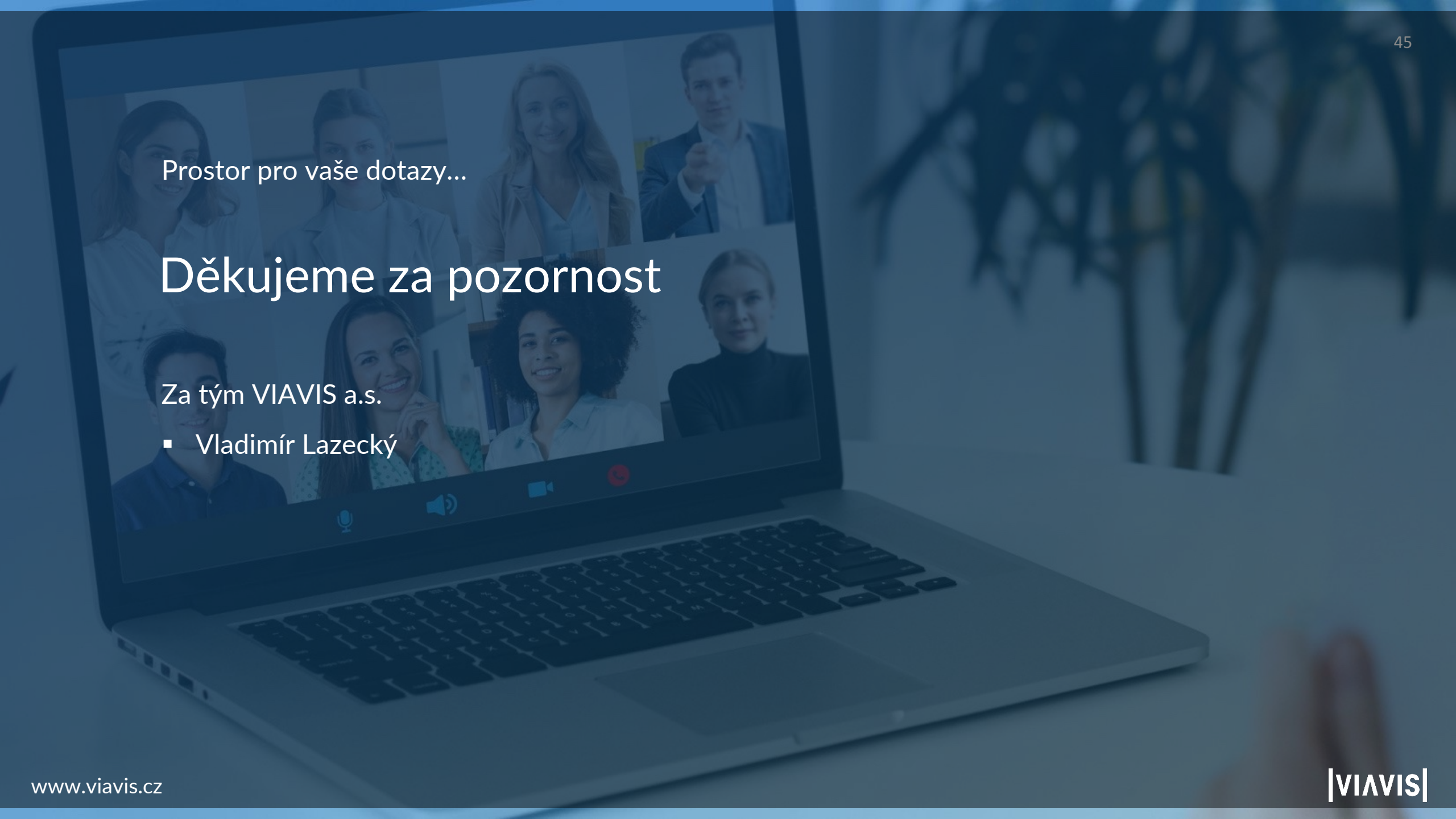
https://i-intelligence.eu/

Doporučení

- Nepodceňovat digitální stopy
- Mít přehled o zranitelnostech
- Pravidelný OSINT – organizace, osoba
- Brát bezpečnost vážně

Profesionální OSINT

- Otevřený WEB, deepweb, darknet
- Organizace, osoba
- Vazby mezi subjekty, uniklé dokumenty a data, hesla, osobní data
- Nejde o levnou službu (placené přístupy do tržišť)
- OSINT vyplatí, jde o nezbytnou součást bezpečnosti



Prostor pro vaše dotazy…

Děkujeme za pozornost

Za tým VIAVIS a.s.

- Vladimír Lazecký