VIAVIS střežíme podstatné

Rostoucí význam OSINT v kybernetické bezpečnosti

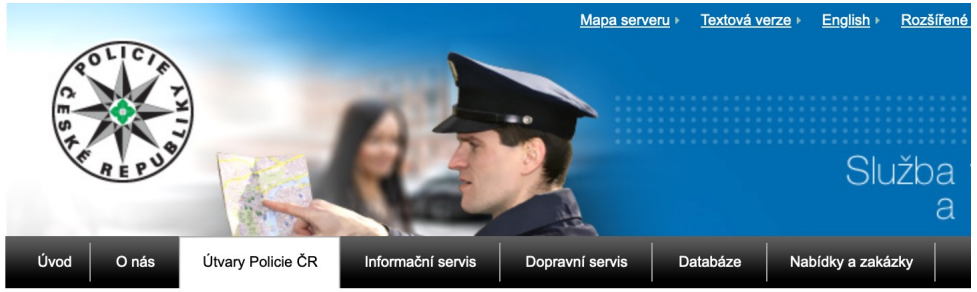
Seminář CACIO

Vladimír Lazecký

vladimir.lazecky@viavis.cz

Léta hojnosti 2021, 2022… – 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.

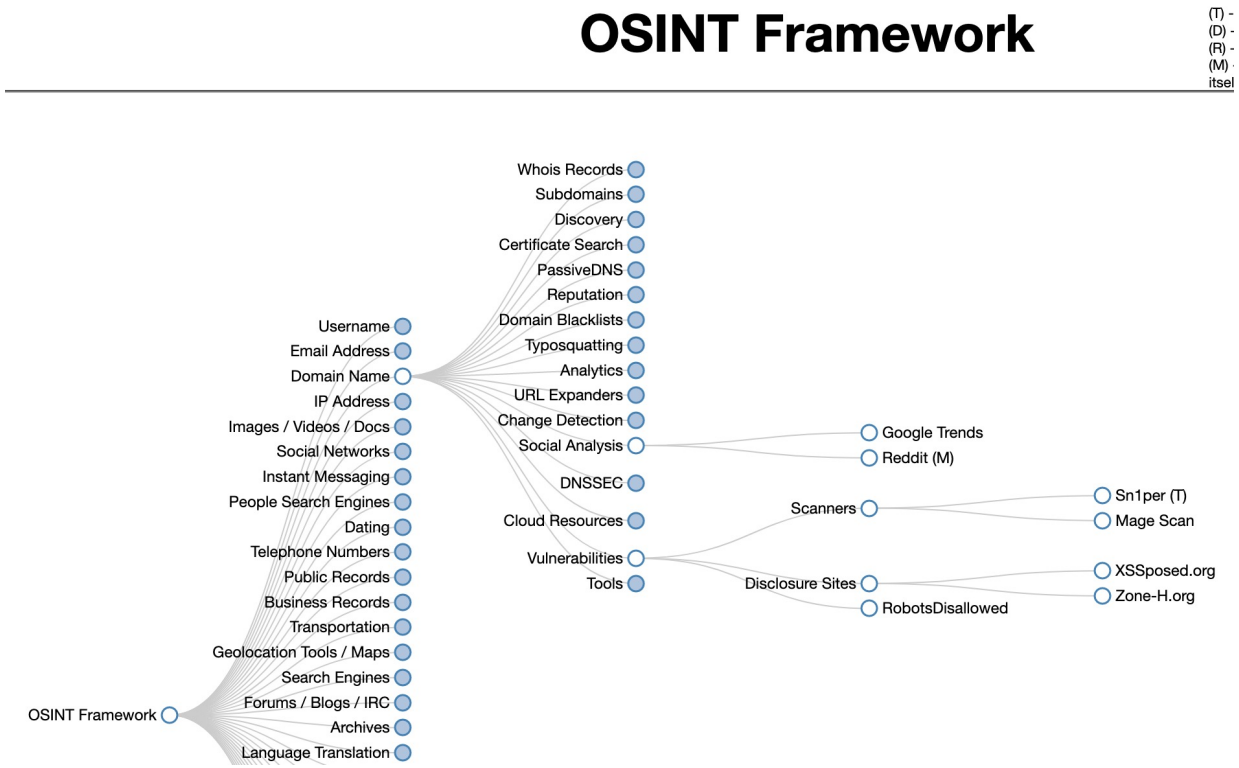
Kriminalisté odboru analytiky a kybernetické kriminality Krajského ředitelství policie Olomouckého kraje odložili trestní věc podezření ze spáchání přečinu neoprávněný přístup k počítačovému systému a nosiči informací, týkající se napadení počítačové sítě Magistrátu města Olomouce z počátku dubna 2021, 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

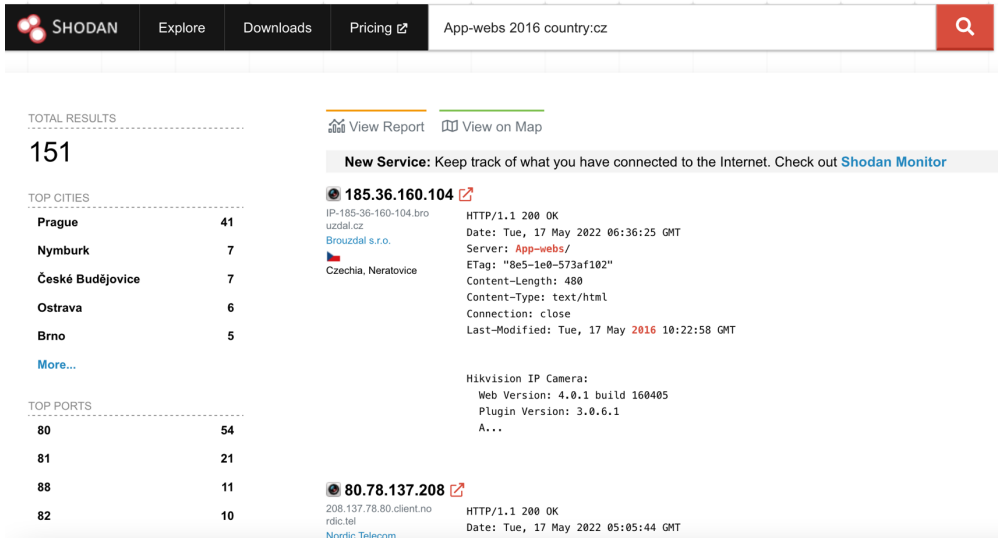
OSINT – Open Source Intelligence

- Vyhledávání informací ve veřejných zdrojích
- Neinvazivní metoda
- Subjekt OSINT jej nemůže identifikovat
- OSINT na organizace, osoby…



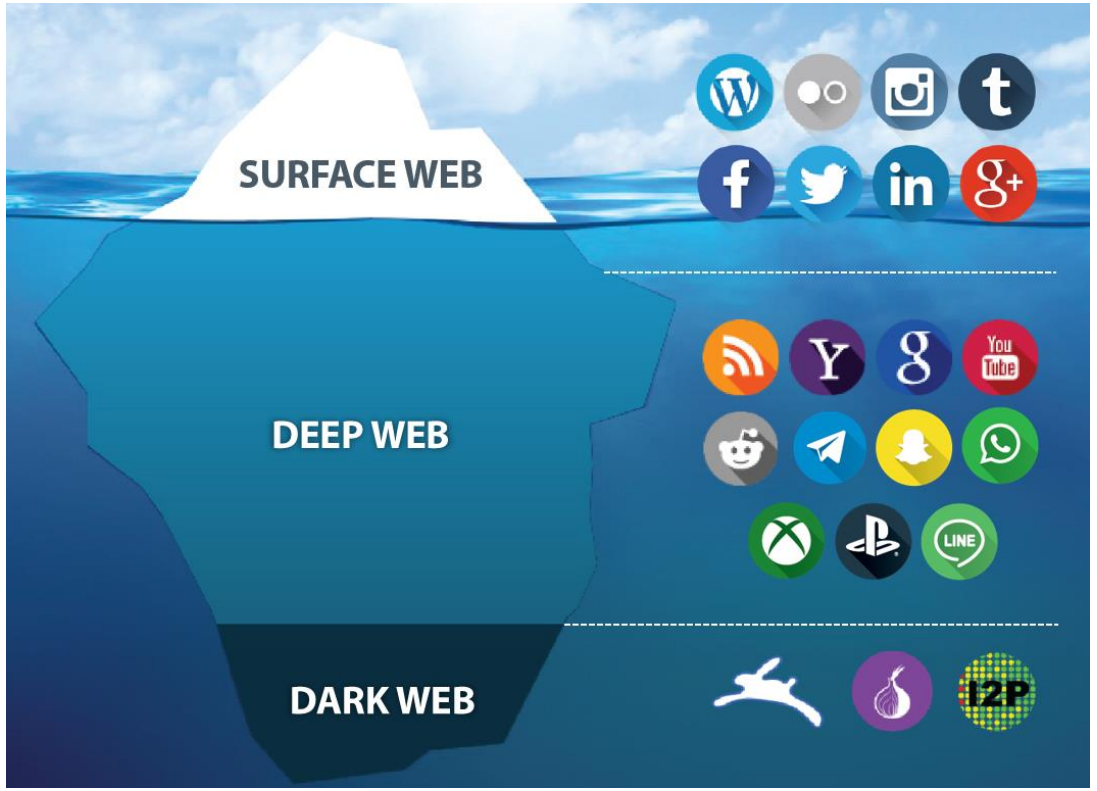
OSINT jako nedílná součást kybernetické bezpečnosti

- Vědět, co se ví:
  - Co komunikuji sám o sobě
  - Co komunikuje okolí
- Bezpečnostní analytika
  - Detekce hrozeb a míry rizika
- Protiopatření:
  - „Potlačení“ rizikového obsahu
  - Odstranění zranitelností



Co může OSINT odhalit

- **Otevřený internet**
  - Technické zranitelnosti, metadata
  - Rizikové vazby, kontakty
  - Trolí kampaně
  - PR útoky…
- **DeepWeb, DarkNet**
  - Úniky dat, metadat, dokumentů
  - Kompromitovaná zařízení
  - ZeroDays Vulnerabilities
  - Kompromitované identity
  - Rizikové vazby…



OSINT – vazby, souvislosti na DarkNetu

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

DarkNet – tržiště profilů

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.

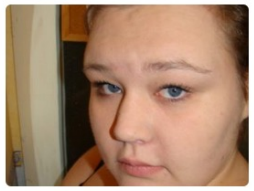
$5.00

Add to cart

Agnieszka Kl.

$3.00

Add to cart



Aleksandra Bo.

$4.00

Add to cart

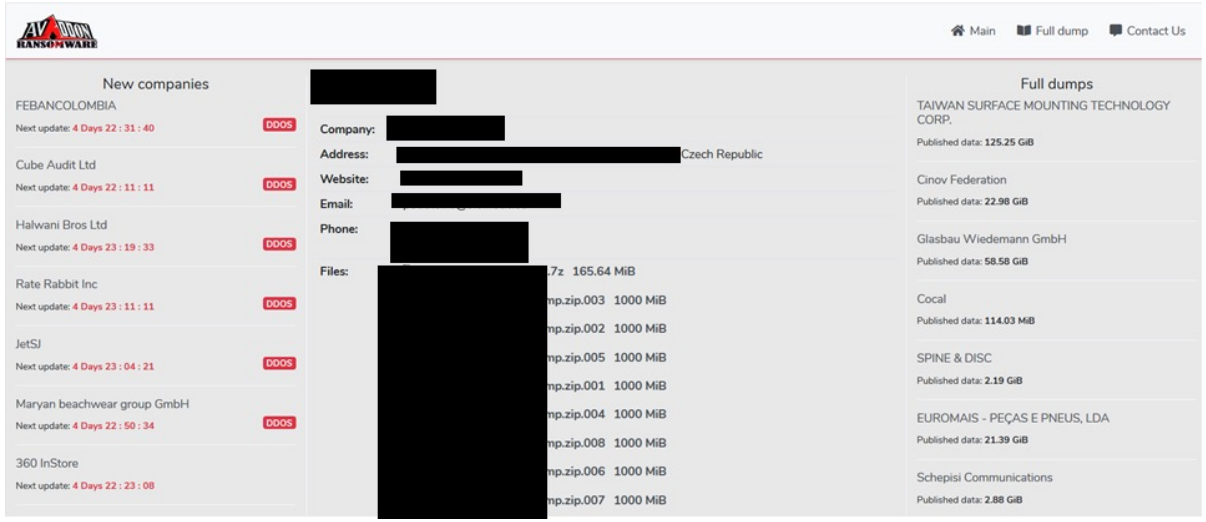
Aleksandra Sn.

$6.00

Add to cart

Zkušenosti klientů

- **Nejčastější zranitelnosti:**
  - Zranitelné systémy (aktualizace, metadata, Zero Days Vulnerabilities…)
  - Kompromitované uživatelské identity
  - Rizikové vazby – osobní, firemní
  - Uniklá data, včetně úniků od třetích stran
  - Mediální obraz, detekce trollů
  - Rizikové profily na sociálních sítích



Shrnutí

- Útoky jsou dostupnější laikům
- OSINT – předpoklad pro úspěšný útok

- **Nepřitahovat pozornost**
  - Sledovat zranitelnosti
  - Odstraňovat je
  - Nekomunikovat je

- **OSINT jako nezbytná součást kyber bezpečnosti**

Kdo si udělal na sebe/organizaci profesionální OSINT?

Prostor pro vaše dotazy…

Děkujeme za pozornost

Za tým VIAVIS a.s.

- Vladimír Lazecký