Bezpečnostní incidenty a incident management

Ing. Vladimír Lazecký
vladimir.lazecky@viavis.cz

VIAVIS střežíme podstatné

Malé opakování

- Co je bezpečnost?
- Jak je definována informační bezpečnost?
- Kybernetická bezpečnost?
- Bezpečnost aplikací?

Co je bezpečnostní incident

- Pokus/získání neoprávněného přístupu k systému, aplikaci nebo datům
- Neautorizované užití systému pro zpracování nebo uložení dat
- Neautorizované změny v SW, HW, datech
- Znefunkčnění systému, zamezení poskytování služeb
  - *Zdroj: https://www.ncsc.gov.uk/information/what-cyber-incident*

Bezpečnostní incident – lze zobecnit

- **Bezpečnostní incident** - prolomení **důvěrnosti, dostupnosti nebo integrity**

- Bezpečnost – řízení snížení rizik výskytu incidentu

  - Zahrnuje celý systém:
    - HW, infrastruktura
    - Aplikace
    - Okolní systémy
    - Procesy
    - Lidé…

  - Řízení rizik již v oblasti návrhu systému, aplikací

Bezpečnostní incidenty – různé pohledy a typy

- Typy bezpečnostních incidentů (lze kategorizovat jakkoli):
  - **Neúmyslné**:
    - Technická závada
    - Integrační chyby
    - Chyba v procesu
    - Lidská selhání
    - Kombinace všech možností
    - Ohrožení důvěrnosti, dostupnosti i integrity
    - Obecně mohou vyústit ve **zranitelnost**

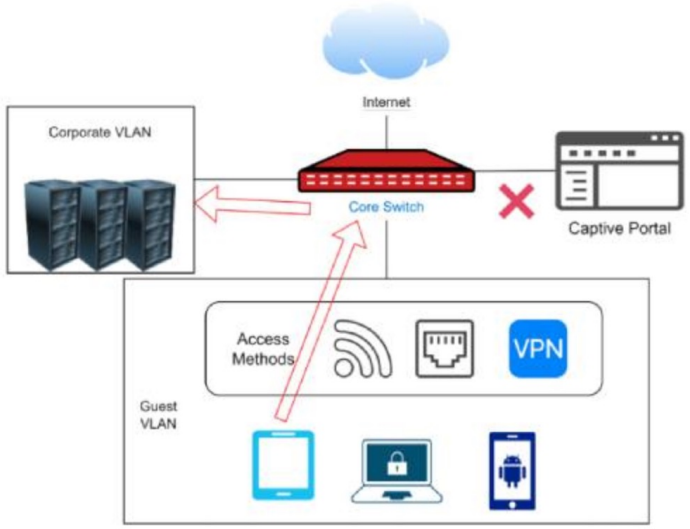
Neúmyslné incidenty

- Cesty ke snižování rizik výskytu:
    - Specifikace bezpečnostních požadavků v etapě návrhu systému
    - Management rizik
    - Testování:
        - Aplikační – funkční, nefunkční, integrační
        - Penetrační testy
    - Definice a optimalizace procesů, testování, audit
    - Vzdělávání a motivace
- Ani důsledným testováním nelze odhalit všechny zranitelnosti

Neúmyslné incidenty – zranitelnost systému

Critical TLStorm 2.0 Bugs Affect Widely-Used Aruba and Avaya Network Switches

May 03, 2022 Ravie Lakshmanan



https://thehackernews.com/2022/05/critical-tlstorm-20-bugs-affect-widely.html

Bezpečnostní incidenty - úmyslné

- **Motivace**:
  - *„Dokázat to“*
  - Využití příležitosti – odhalená zranitelnost
  - Msta – frustrovaný zaměstnanec
  - Business – profitabilita 99%
  - Politické cíle – terorismus, válka
    - Hybridní hrozby
    - Fake news
    - Útoky na infrastrukturu

Bezpečnostní incidenty - úmyslné

- V čem se liší od neúmyslných:
  - Velikost zdrojů věnovaných na útok
  - Každý systém je nabouratelný, záleží pouze na velkosti úsilí – zdrojů
  - *Lze odhadnout dopad incidentu typu „black out“ v rozsahu 2 týdnů?*
- *Proaktivní incident management incidenty eliminující lze navrhnout jen velmi obtížně (pokud vůbec…)*

Bezpečnostní incidenty - úmyslné

- Podle způsobu provedení:
  - Sociotechniky
  - Technické incidenty
  - Hybridní
  - Kombinace

- Odkud jsou provedeny:
  - Incidenty z vnějšího světa
  - Incidenty z interního prostředí
  - Kombinace obou

Sociotechniky

- Technika stará jako lidstvo samo
- Metody založené na navazování vztahů a využitím důvěřivosti (*všichni to znáte*)
- Využívá se:
  - Nevinná informace
  - Stačí se zeptat
  - Odvracení pozornosti
  - Budování důvěry
  - Žádost o pomoc
  - Soucit, vina, zastrašení
  - Obrácený podraz

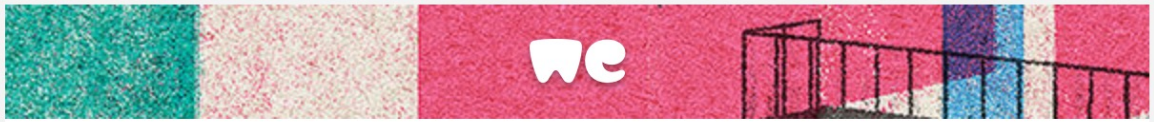
Známé sociotechniky - phishing

TW **We transfer**

Příchozí - VIA

vladimir.lazecky@viavis.cz You have received New files Via We transfer!

Komu: Lazecký Vladimír



vladimir.lazecky@viavis.cz

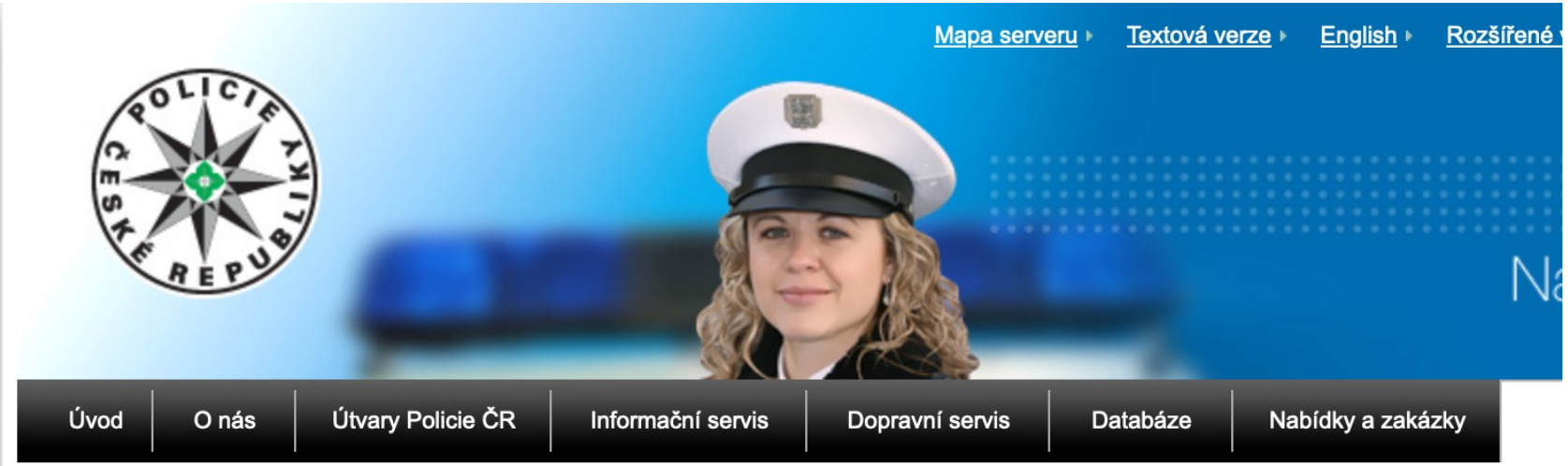
You received New files via WeTransfer

1 file, 372.8 MB in total · Will be deleted on 5th May, 2022

Open files here

VIAVIS střežíme podstatné

Známé sociotechniky - vishing



https://www.policie.cz/clanek/vishing-a-spoofing.aspx

VIAVIS střežíme podstatné

Jak navrhovat systémy odolné proti sociotechnickým útokům?

- **Nápady?**
  - *Kde je hranice možností?*
  - *Jak specifikovat požadavky na systémy/aplikace?*
  - *Stopy?*

Technické útoky na důvěrnost informace

- **Cíle**:
  - Získat cennou informaci
  - Získat neoprávněný přístup do systému
  - Informaci zcizit tak, aby útočník nezanechal stopy (*problém*)

- **Zopakujme – informaci lze získat vždy, záleží pouze na množství investovaného úsilí**

Technické útoky na důvěrnost informace

- Překážky pro útočníka:
  - Zjistit, kde daná informace je (*architektura systému, distribuce dat*)
  - Získat neoprávněný přístup do systému (*autentizace, autorizace*)
  - Logistika dat – jak informaci dostat ze systému ven (*logování, nastavení práv*)
  - Časový tlak (*expirace přístupů, bezpečnostní procesy, monitoring*)
  - Stopy – zvláště elektronické stopy (*analýza stop, uchovávání, log management*)
- Inspirace pro bezpečnostní požadavky

- Sofistikovaný útok musí být velmi pečlivě naplánován

- Podstatnou roli hraje časové hledisko a generování stop – šance pro obranu

Technické útoky na důvěrnost informace

- Prolomení autentizace – útočník řeší:
  - Zjištění identity uživatele s dostatečnými přístupovými právy
  - Prolomení přístupové bariéry – nejčastěji hesla
  - Čas útoku – dva stejní uživatelé
  - Důvěryhodnost provedené operace
- Zjištění identity:
  - „Hrubou silou“ – rozeslání podvodných mailů – „phishing“, někdo se ozve
  - Scanováním provozu – pokud má přístup k síti
  - Podvržením přihlašovací stránky
  - Má-li útočník Login, dá se hádat heslo - cracking
  - POZOR – časté útoky na mobilní zařízení (tablety, mobily, notebooky)
  - Kritický problém – mobilní zařízení jsou díry do systému

Technické útoky na důvěrnost informace

- Odposlechy provozu
  - Podmínka:
    - Přístup k nižším vrstvám přenosu (fyzická, linková, datová vrstva)
    - Přístup ke komunikačním serverům
  - Maily – otevřená korespondence lze:
    - Podvrhnout odesílatele
    - Změnit obsah
    - Odposlechnout zprávy – jde o datový tok
    - **Veřejné mailové služby NEJSOU BEZPEČNÉ**
  - **Bezpečný mail – podepisování, šifrování, silná ochrana klíče**

Šifrování dat – jak to funguje – malá odbočka

- Co to je šifrování:
  - **Z otevřených dat udělat data, která si může přečíst jen ten, komu to povolím**
- Analogie
  - Data – listina
  - Šifrování – trezor
  - **Kdo má přístup – ten, kdo má klíč**

Šifrování dat – jak to funguje

- Šifrování:
  - Algoritmus – matematický postup – je obvykle znám
    - Otevřenost algoritmu není na závadu
    - Crystal box x Black box
  - Klíč – informace, která vstupuje do algoritmu – číslo, řetězec znaků
    - Všichni známe ZIP – klíč je heslo, které zadáváte
    - Kdo ovládá klíč, ovládá přístup k datům
    - Je důležitá délka klíče – čím delší, tím obtížnější prolomení šifry

Šifrování dat – jak to funguje

- Symetrické:
  - Šifrování i dešifrování se provádí stejným klíčem
  - Příjemce i odesílatel musí mít stejný klíč
  - Lze využít – pokud šifruji sám pro sebe
- Známé technologie: AES, Blowfish, DES, GOST, IDEA, RC2, RC5, Tripple DES
- Výhody:
  - Jsou méně náročné na výpočetní výkon
- Nevýhody
  - Slabina – jak bezpečně doručit klíč protistraně? (Heslo přes SMS…)

Šifrování dat – jak to funguje

- Asymetrické šifrování
  - Pracuje s dvojicí klíčů – jedním se šifruje, druhým dešifruje
  - Jiný název – veřejný a soukromý klíč
  - Šifruje se veřejným klíčem protistrany
  - Dešifruje vlastním soukromým klíčem
  - Veřejný klíč:
    - Jednosměrná operace šifrování
    - Lze poslat otevřeným mailem
  - Soukromý klíč:
    - Dešifrování
    - Nutná silná ochrana
  - Asymetrická kryptografie se používá i v el. podpisu

Šifrování dat – jak to funguje

- Jak se šifrují sdílená data pro více uživatelů?
  - Symetricky – nutno všem rozeslat klíč
    - Komplikovaný řetězec důvěry
  - Asymetricky – jeden soubor musí být zašifrován pro každého uživatele zvlášť
    - Roste nárok na výpočetní výkon a množství dat

  - Používá se kombinace obou metod:
    - Vygeneruje se jednorázový symetrický klíč
    - Tímto klíčem se zašifrují data
    - Asymetricky se pro každého uživatele zašifruje symetrický klíč

Šifrování dat – jak to funguje

- Proč vám tím pletu hlavu?
  - **Klíč je v klíči ☺**
  - Kdo ovládá klíč – má přístup k šifrovaným datům
  - Pokud cloud nabízí šifrování – ptejte se jak?
  - Kde se generují klíče?
  - Kdo je má pod kontrolou?

Šifrování dat – jak se dá šifrování prolomit

- Každá technologie je prolomitelná, záleží pouze na zdrojích útočníka
- Šifrovací algoritmy jsou obvykle navrženy tak, že jejich prolomení je problém – nedostatek výpočetního výkonu
- Pokud nelze algoritmus prolomit – útočník jej obejde:
  - Získá klíč
  - Získá zprávu ještě před jejím zašifrováním
  - Získá zprávu po jejím dešifrování

Šifrování dat – jak se dá šifrování prolomit

- Získání klíče:
  - Krádež počítače – klíč je uložen na disku a chráněn pouze heslem
  - Zadní vrátka v SW – kde probíhají kryptografické operace
- Chyba v softwarových implementacích

- Jak číst zprávy, že NSA prolomila šifrovanou komunikaci?
  - Získala klíč ☺

Technické útoky na důvěrnost

- Mobilní zařízení – tablety, mobily
  - Největší riziko – otevírají přístup do interních sítí
  - Útoky:
    - Trojský kůň – SW otevírající přístup
    - SW odesílající data
    - SW odesílající přístupové kódy
    - Odesílání geolokačních záznamů
  - Zdroje útoků:
    - Neautorizovaný SW
    - Využití zranitelností

Technické útoky na důvěrnost

Data breaches

- Isle of Wight children's details sent out in email gaffe (90)
- Hilliard City Schools evaluating protocols after leaking the names of students (4,200)
- Nespresso data leak in South Africa (unknown)
- State Bar breach exposed thousands more confidential records than original estimates (322,525)
- A security lapse exposed India's CISF personnel files and health records (unknown)
- Japanese medical online consultation site leaking consumer-submitted images of symptoms (12,000)
- Hotel WiFi across MENA compromised and exposing private data (unknown)
- CareOregon Advantage files notice of recent data breach (10,467)
- Christie Clinic, CSI Laboratories report breaches (unknown)
- Personal Data of 820,000 NYC Students Exposed (820,000)
- Names and addresses of 620 FSB officers published in data breach (620)

https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-march-2022-3-99-million-records-breached

TECH TALK

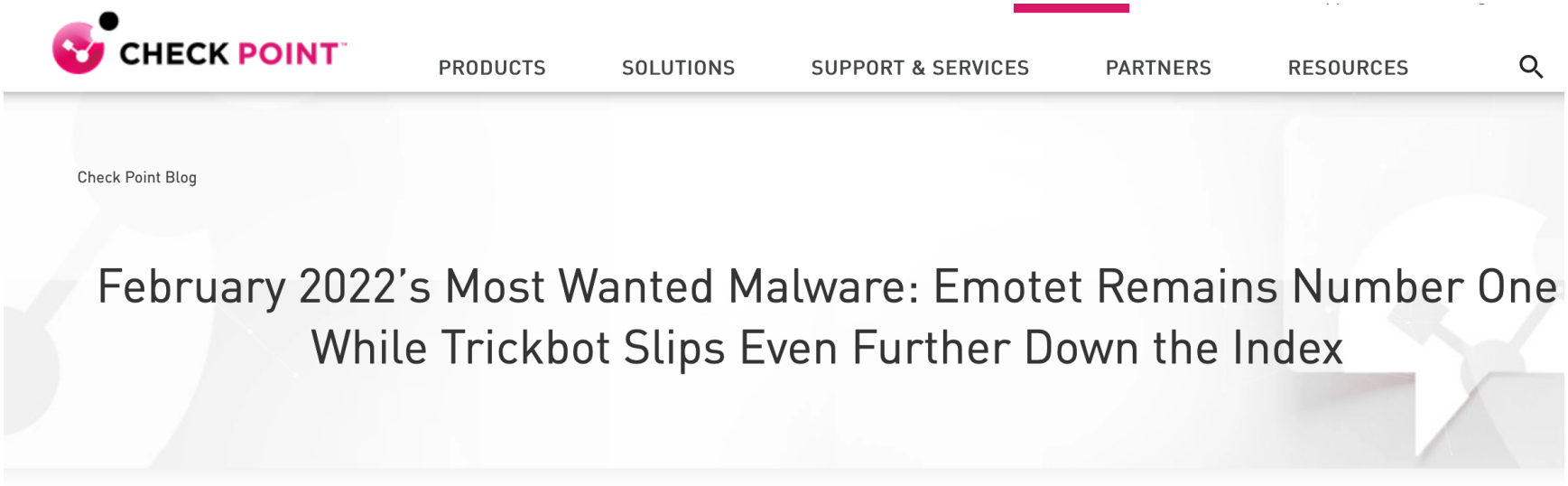
Metadata: a hacker's best friend

In this blog post, we are going to explore the dangers and risks of the tip of a very huge iceberg of sensitive information companies are exposing: the metadata of a document.

MARTIN CARNOGURSKY
25 JUL 2017 • 18 MIN READ

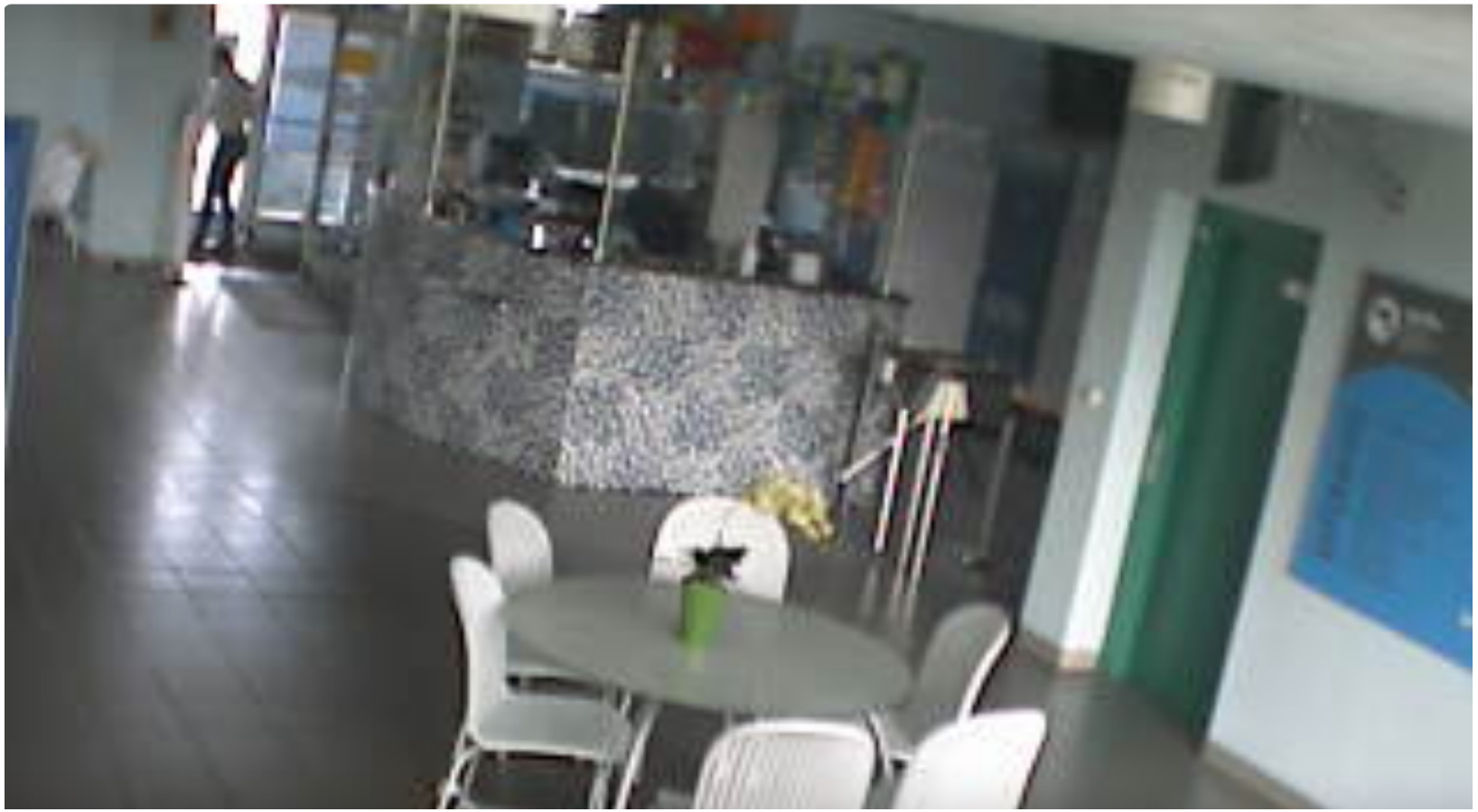
https://blog.sweepatic.com/metadata-hackers-best-friend/

Technické útoky na důvěrnost



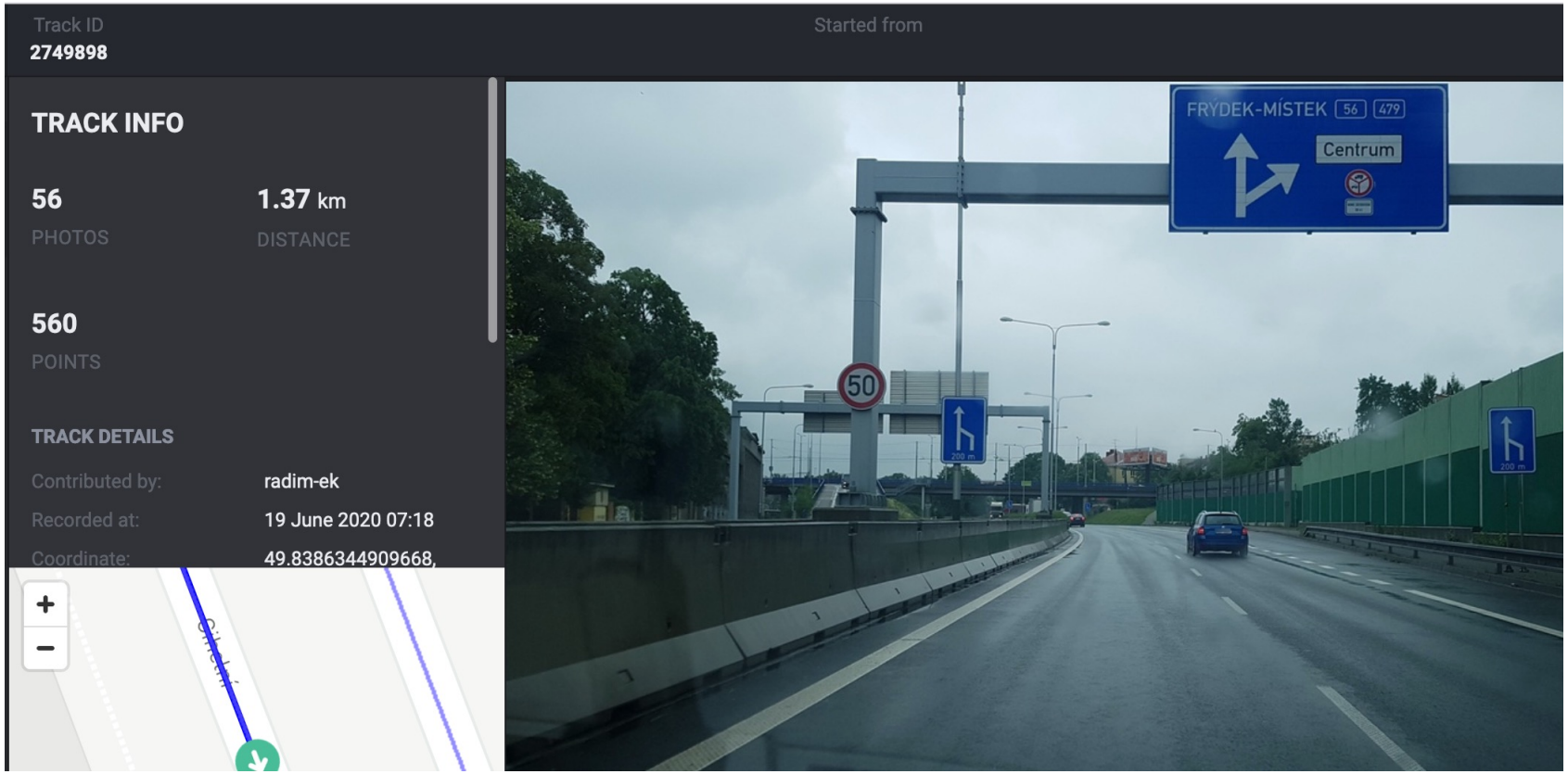
https://blog.checkpoint.com/2022/03/09/february-2022s-most-wanted-malware-emotet-remains-number-one-while-trickbot-slips-even-further-down-the-index/

Útoky na důvěrnost



https://www.insecam.org/en/view/204260/

Útoky na důvěrnost



https://kartaview.org/details/2749898/51/track-info

Technické útoky na důvěrnost

– Jak se lze bránit?

  – Požadavky na systémy?

  – Požadavky na aplikace?

  – Provoz?

Technické útoky na dostupnost

- **Útok na dostupnost služby – vyřazení služby z provozu:**
  - Webových serverů
  - Informačních systémů
  - Systémů kritické infrastruktury…
  - Osobních zařízení
  - Aplikací

- *Jak byste to udělali?*

Technické útoky na dostupnost

- **DoS (Denial of Service) Attack - odmítnutí služby**
  - Přehlcení požadavky - pád nebo nedostupnosti systému

- **DDoS (Distribued Denial of Service)**
  - Útok z většího množství počítačů najednou
  - Často je tento útok veden bez vědomí majitelů útočících počítačů

Technické útoky na dostupnost

– Ransomware

Ransomware

- Threat actors leak data from Scottish Association for Mental Health (unknown)
- Ransomware gang leak 190GB of alleged Samsung data, source code (unknown)
- Pennsylvania-based Fleetwood Area School District hit by ransomware (unknown)
- Ubisoft says it experienced a 'cyber security incident', LAPSUS$ group claims credit for attack (unknown)
- PracticeMax discloses security incident (165,698)
- Wagstaff, Inc. hit by ransomware (unknown)
- TransUnion hackers demand R224-million ransom (unknown)
- Wheeling Health Right victim of ransomware attack (unknown)
- New Jersey Brain and Spine notifies those affected by ransomware (92,453)
- Argentina'ssenatereveals that its website was hit by ransomware (unknown)
- Microsoft confirms it was hacked by Lapsus$ extortion group (unknown)
- Hundreds of companies potentially hit by Okta hack (unknown)
- Oklahoma City Indian Clinic impacted by Suncrypt's ransomware attack (20,000)

https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-march-2022-3-99-million-records-breached

Technické útoky na dostupnost

- **Obsazení přenosové kapacity** - velmi účinná metoda, útočník vytvoří takový provoz, který plně vytíží přístupovou cestu
- **Přivlastnění systémových zdrojů** – maximálně spotřebovat limitované zdroje oběti
- **Zneužití chyb v programech** – tam, kde správci zanedbávají záplatování
- **Napadení DNS a systémů směrování paketů** - na DNS serverech dojde ke změnám záznamů o IP adresách –veškerý provoz je měněn ve prospěch útočníka nebo žádosti vedou do „slepé uličky“
- **Útok na klíčové DNS servery -** nefunkčnost znamená ztrátu většiny internetového i e-mailového provozu
- **DDoS** - nebezpečnost se násobí tím, že jsou vedeny z různých směrů, využívají metody obsazení přenosové kapacity
  - Je velmi obtížné zastavit útočníka, působí z mnoha směrů
  - Útok vyžaduje značné technologické znalosti
  - Problém distribuce útočných nástrojů a koordinace jejich aktivity

Technické útoky na dostupnost

- Obrana před DoS útoky není snadná – nestačí jedno opatření (technické řešení):
  - Implementace bezpečnostních záplat
  - Pravidla na perimetru internetu – např. první paket z jakékoliv IP adresy není vpuštěn (odfiltruje DDoS)
  - Aktivace služby filtrující všechny UDP
  - Vypnutí nepoužívaných nebo nepotřebných služeb
  - Architektura se záložními zdroji - rozložení zátěže

Technické útoky na dostupnost

CISA.g

Alerts and Tips Resources Industrial Control Systems

National Cyber Awareness System > Alerts > Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure

Alert (AA22-110A)

Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure

Original release date: April 20, 2022

Print Tweet Send Share

https://www.cisa.gov/uscert/ncas/alerts/aa22-110a

Technické útoky na integritu

- Cílem útoků – změnit informaci během přenosu, zpracování, archivace
- Internet je veřejný prostor – odposlech a změna provozu je možná
- Princip – jedna z možností
  - Provoz je neoprávněně přesměrován
  - Na útočníkem ovládaném serveru je změněn
  - Jsou změněna „metadata“
  - Provoz je odeslán k adresátovi
  - Provoz – datový tok, odposlech nelze z přijaté zprávy zjistit

  - Úprava zasílaných dokumentů - faktury

https://www.nccoe.nist.gov/sites/default/files/legacy-files/data-integrity-project-description-final.pdf

Technické prostředky ochrany

- Existuje množství sofistikovaných prostředků:
  - Antiviry
  - Firewally
  - Scanování a hodnocení provozu – SIEM
  - DLP systémy
  - Monitoring využití zdrojů
  - Systémy řízení provozu
  - Kamerové systémy

  - Zásadní problém – množství logů a zdroje na jejich analýzu

Hybridní hrozby

- Vícerozměrné a komplexní hrozby

Máte nějaké dotazy?

Děkuji za pozornost

Ing. Vladimír Lazecký