KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

CYBER THREAT INTELLIGENCE

A JEHO MIESTO V ANALÝZE SPRAVODAJSKÝCH A POLITICKÝCH INFORMÁCIÍ

DEFINÍCIE

- **MITRE (2021):** CTI je zhromažďovanie, vyhodnocovanie a šírenie informácií o hrozbách, ktoré sú akcieschopné a pomáhajú organizáciám robiť rozhodnutia o ochrane digitálnych systémov
- **Rid (2020):** CTI je proces, v ktorom sa surové dáta o kybernetických hrozbách premieňajú na spravodajsky hodnotné informácie, ktoré majú politický, ekonomický alebo vojenský rozmer
- **ENISA (2020):** CTI je štruktúrovaná, spracovaná a kontextualizovaná informácia o potenciálnych alebo aktuálnych kybernetických hrozbách, využiteľná na strategickej aj taktickej úrovni
- spoločný znak všetkých definícií: nejde len o dáta, ale o dáta spracované do kontextu, ktoré umožňujú konať.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

VÝVOJ CTI

- Prvé fázy (1990-2000)
  - kybernetická bezpečnosť bola orientovaná skôr na technickú prevenciu (firewally, antivírusy)
  - „Inteligencia“ znamenala predovšetkým zdieľanie zoznamov škodlivých IP adries a vírusových podpisov
- Posun po roku 2010
  - nástup sofistikovaných útokov (APT – Advanced Persistent Threats)
  - útočníci boli často štátni aktéri (Rusko, Čína, Irán, Severná Kórea)
  - vznik potreby rozlišovať strategické, taktické a technické vrstvy informácií

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

VÝVOJ CTI

- Súčasnosť
  - CTI je súčasťou geopolitiky: sledujú sa nielen technické hrozby, ale aj informačné a kognitívne kampane
  - prepojenie CTI s OSINT a politicko-spravodajskou analýzou (napr. voľby, dezinformácie, hybridné hrozby)
  - komerčné firmy (FireEye/Mandiant, Recorded Future, CrowdStrike) dodávajú CTI vládnym aj súkromným aktérom

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

VÝZNAM CTI

- **prevencia útokov:** CTI pomáha rozpoznať vzorce správania aktérov a predpovedať útoky
- **rozhodovanie:** strategická CTI dáva podklady politikom a manažérom (napr. o hrozbách pre kritickú infraštruktúru)
- **kontextualizácia dát:** dáta bez kontextu sú zahlcujúce – CTI pomáha pochopiť kto, prečo a ako útočí
- **geopolitický rozmer:** CTI je dnes nástrojom medzinárodnej politiky a diplomacie (napr. atribúcia útokov, sankcie)
- **synergia s inými spravodajskými disciplínami:** OSINT, HUMINT a CTI sa čoraz viac prelínajú

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

TYPY CTI A ICH VYUŽITIE

1. STRATEGICKÁ CTI

- **Definícia:** dlhodobé analýzy trendov, aktérov a geopolitických kontextov.
- **Publikum:** politické vedenie štátu, bezpečnostní stratégovia, vrcholový manažment.
- **Obsah:**
  - motivácie aktérov (štáty, APT skupiny, hacktivisti),
  - trendy v kybernetických hrozbách,
  - možné scenáre (napr. kybernetické útoky počas volieb).
- **Príklad:** správa NATO StratCom o ruských informačných a kybernetických aktivitách v Európe

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

TYPY CTI A ICH VYUŽITIE

2. TAKTICKÁ CTI

- **Definícia:** analýza taktik, techník a procedúr (TTPs) útočníkov.
- **Publikum:** bezpečnostní analytici, spravodajské tímy.
- **Obsah:**
  - aké metódy používa útočník (spear-phishing, exploit, malvér)
  - ktoré sektory sú cieľom,
  - aké sú odporúčané protiopatrenia.
- **Príklad:** MITRE ATT&CK framework – databáza známych taktik a techník kybernetických útokov.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

TYPY CTI A ICH VYUŽITIE

3. OPERATÍVNA CTI

- **Definícia:** informácie o konkrétnych kampaniach a plánovaných útokoch.
- **Publikum:** kybernetické tímy (SOC, CERT/CSIRT).
- **Obsah:**
  - kto je cieľom,
  - aké nástroje sú aktuálne nasadené,
  - indikátory kompromitácie (IoCs).
- **Príklad:** správa o phishingovej kampani zameranej na diplomatické misie v strednej Európe.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

TYPY CTI A ICH VYUŽITIE

4. TECHNICKÁ CTI

- **Definícia:** najnižšia, technická úroveň – konkrétne dátové ukazovatele hrozby.
- **Publikum:** IT bezpečnostné tímy, administrátori.
- **Obsah:**
    - IP adresy, URL adresy, domény, hash súbory, digitálne certifikáty, ktoré treba blokovať.
- **Príklad:** databáza hashov ransomvéru Conti publikovaná bezpečnostnou firmou

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

PREPOJENIE MEDZI ÚROVŇAMI

- strategická CTI odpovedá „prečo a kto“
- taktická CTI vysvetľuje „ako“
- operatívna CTI ukazuje „kedy a kde“
- technická CTI dáva konkrétne „čo“

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

PRÍPADOVÉ ŠTÚDIE

1. STRATEGICKÁ CTI – APT28 (Fancy Bear)

- **Aktér:** ruská skupina napojená na GRU.
- **Dlhodobé ciele:** ovplyvňovanie volieb, špionáž proti NATO a EÚ.
- **Známky správania:** koordinované kampane, kombinácia kyberútokov a dezinformácií.
- **Strategický význam:** predstavuje dlhodobú hrozbu pre demokratické inštitúcie a medzinárodnú stabilitu.
- **Zdroj:** FireEye (2014), „APT28: A Window into Russia's Cyber Espionage Operations?

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

PRÍPADOVÉ ŠTÚDIE

2. TAKTICKÁ CTI – spear-phishing proti NATO (2015)

- **Metóda:** spear-phishing e-maily posielané zamestnancom NATO a európskych ministerstiev.
- **Techniky:** škodlivé prílohy (Word dokumenty s makrami), sociálne inžinierstvo (emaily vydávajúce sa za oficiálne oznámenia).
- **Cieľ:** získanie prihlasovacích údajov a prístup do interných sietí.
- **Použiteľnosť:** pomáha bezpečnostným tímom identifikovať typické techniky APT skupín.
- **Zdroj:** FireEye, ESET, MITRE ATT&CK framework.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

PRÍPADOVÉ ŠTÚDIE

3. OPERATÍVNA CTI – phishingová kampaň proti diplomatickým misiám v Európe (2019)

- **Zistenie:** OSINT a CTI analýza zachytila konkrétne e-maily rozposielané diplomatickým úradom v Poľsku, Česku a Slovensku.
- **Obsah:** emaily obsahovali odkazy na falošné prihlasovacie portály.
- **Indikátory kompromitácie (IoCs):** zoznam podvodných domén, e-mailových adries a nástrojov.
- **Výstup:** CERT tímy vydali varovanie a odporúčania.
- **Zdroj:** CERT-EU incident report (2019).

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

PRÍPADOVÉ ŠTÚDIE

4. TECHNICKÁ CTI – ransomvér Conti (2021–2022)

- **Obsah:** konkrétne hash hodnoty škodlivých súborov, IP adresy serverov používaných na C2 (command & control), a URL adresy na distribúciu.
- **Použitie:** tieto indikátory sa okamžite nasadzujú do firewallov a antivírusov.
- **Výstup:** „blocklist“, ktorý zabraňuje šíreniu ransomvéru.
- **Zdroj:** CISA (Cybersecurity & Infrastructure Security Agency, USA) – advisories on Conti ransomware.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

CTI AKO SÚČASŤ INFORMAČNEJ BEZPEČNOSTI

- CTI v rámci kybernetickej/informačnej bezpečnosti
  - kybernetická bezpečnosť = technická ochrana systémov a sietí
  - informačná bezpečnosť = širší koncept zahŕňajúci nielen technické, ale aj organizačné, ľudské a strategické aspekty
  - CTI = most medzi týmito dvoma – poskytuje kontext k hrozbám a umožňuje proaktívnu obranu.
- Prepojenie CTI s ďalšími vrstvami
  - prevencia: CTI identifikuje trendy a prediktívne faktory (napr. rastúce phishingové kampane)
  - detekcia: technická CTI poskytuje IoCs, ktoré sa nasadzujú do detekčných systémov (IDS/IPS, SIEM)
  - reakcia: operatívna CTI pomáha incident response tímom reagovať rýchlejšie
  - obnova: strategická CTI ukazuje, ako minimalizovať budúce riziká.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

CTI AKO SÚČASŤ INFORMAČNEJ BEZPEČNOSTI

- CTI a kognitívny priestor
  - kybernetické hrozby sú čoraz viac prepojené s informačnými a psychologickými operáciami
  - príklad: únik dát → následne ich použitie v dezinformačnej kampani (hack & leak)
  - CTI preto sleduje nielen technické útoky, ale aj narratívne kampane spojené s útočníkmi
- Praktický význam pre politickú komunikáciu
  - politické inštitúcie (parlamenty, vlády, think-tanky) sú terčmi kybernetických aj informačných útokov
  - CTI poskytuje včasné varovania, ktoré môžu chrániť integritu volieb, politických rozhodnutí alebo diplomatických vzťahov
  - prepojenie s OSINT: verejné dáta dopĺňajú technické indikátory, čím vzniká komplexný obraz

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

CTI V POLITICKOM A SPRAVODAJSKOM KONTEXTE

- POLITICKÁ DIMENZIA CTI
  - CTI už nie je len technickou disciplínou – dnes je súčasťou geopolitického súperenia
  - kybernetické hrozby sú často štátom podporované (APT skupiny viazané na Rusko, Čínu, Irán, Severnú Kóreu)
  - CTI pomáha mapovať atribúciu útokov (kto stojí za nimi) – čo má priame dôsledky pre diplomaciu, sankcie a bezpečnostné politiky
  - CTI tak dáva politikom a novinárom mapu hrozieb, ktorá je kľúčová pri ochrane dôvery verejnosti
- SPRAVODAJSKÁ DIMENZIA CTI
  - CTI je prepojené s klasickými spravodajskými disciplínami (SIGINT, HUMINT, OSINT)
  - rozširuje spravodajské kapacity o digitálny rozmer – sleduje aktivity v kyberpriestore a na dark webe
  - politické a vojenské spravodajské služby používajú CTI ako doplnok k predikcii hrozieb

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

LIMITY CTI

- Dostupnosť dát
- Rýchlosť zastarávania
- Interpretácia a atribúcia
- Falošná istota

Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

ETICKÉ OTÁZKY CTI

- Súkromie a monitoring
- Zverejňovanie informácií
- Politizácia CTI
- Komercializácia CTI

Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

BUNDESTAG HACK (2015)

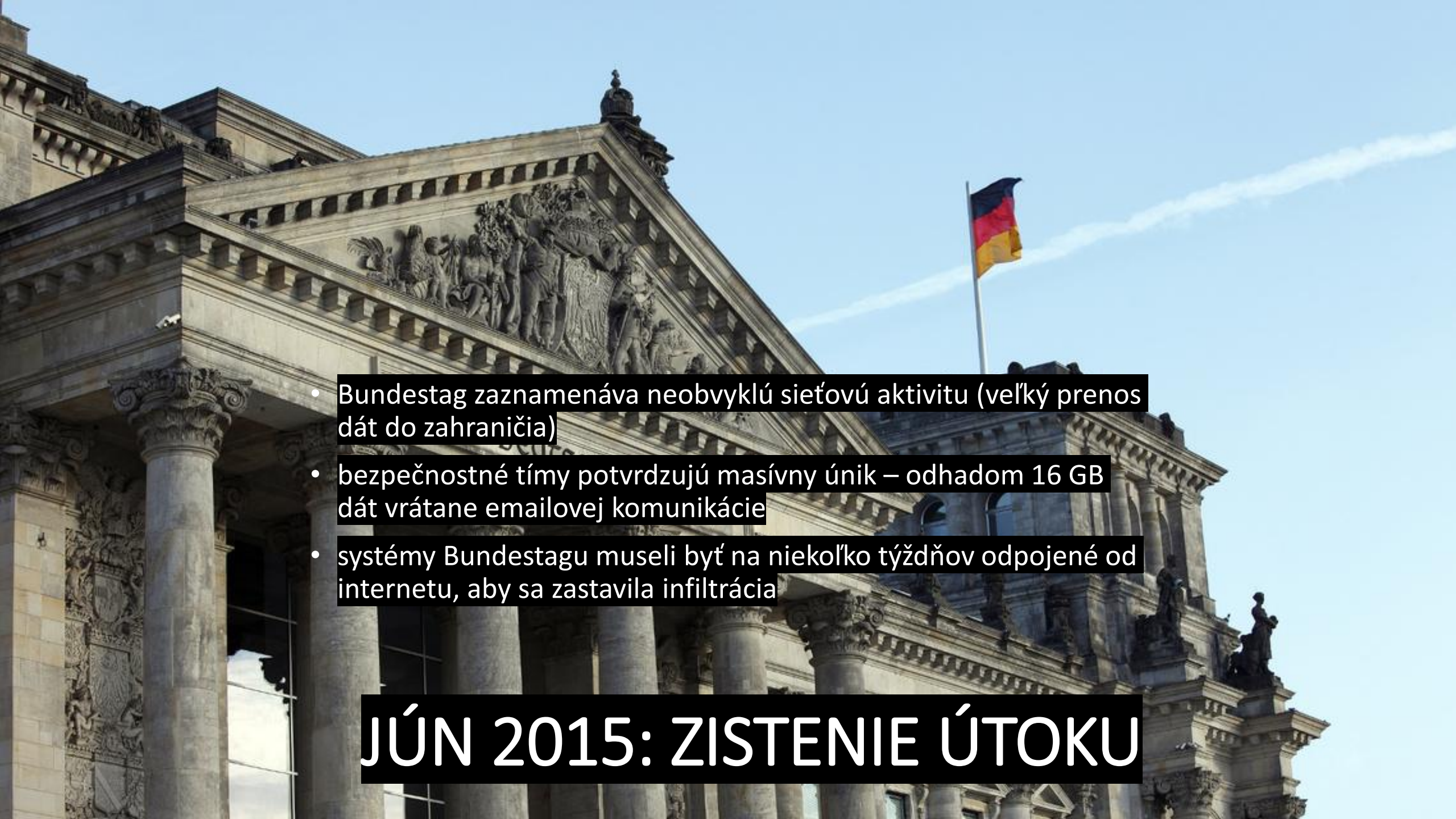
- Máj 2015: Kyberútok na nemecký parlament (Bundestag)
- Útočníci získali prístup k IT infraštruktúre a odcudzili odhadom 16 GB dát, vrátane emailov poslancov
- Incident sa považuje za najväčší kybernetický útok na nemecké politické inštitúcie

- útočníci rozposielajú spear-phishing e-maily poslancom a zamestnancom Bundestagu
- e-maily obsahujú link na škodlivý server → po kliknutí sa inštaluje malvér (RAT)
- malvér umožňuje útočníkom vzdialený prístup a postupné šírenie v sieti

APRÍL - MÁJ 2015: ZAČIATOK ÚTOKU

- útočníci získavajú administrátorské prístupy
- infikujú viaceré interné servery a pracovné stanice
- dochádza k laterálnemu pohybu po sieti a hromadnému odčerpávaniu dát

MÁJ - JÚN 2015: INFILTRÁCA/ŠÍRENIE

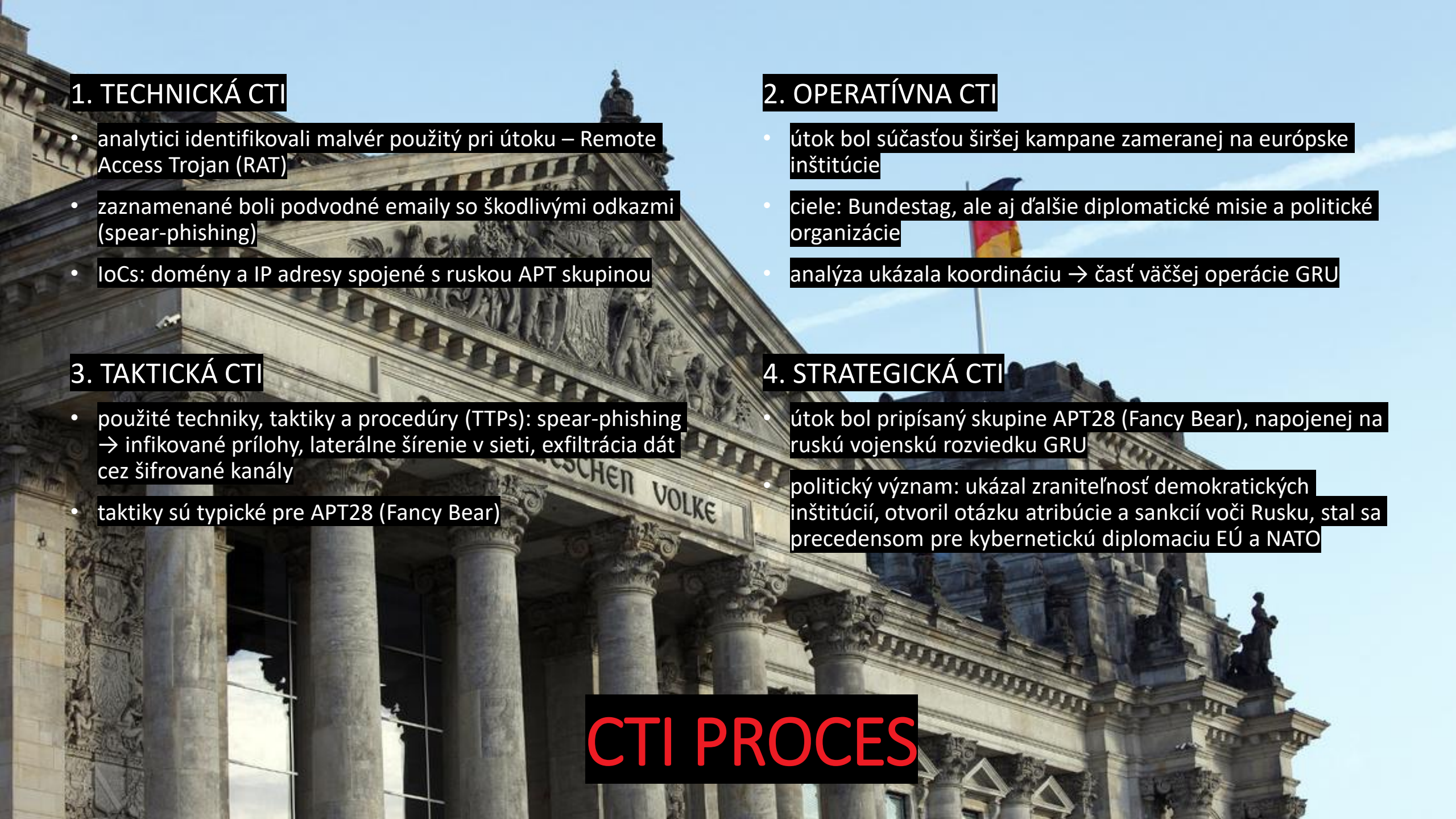


- Bundestag zaznamenáva neobvyklú sieťovú aktivitu (veľký prenos dát do zahraničia)
- bezpečnostné tímy potvrdzujú masívny únik – odhadom 16 GB dát vrátane emailovej komunikácie
- systémy Bundestagu museli byť na niekoľko týždňov odpojené od internetu, aby sa zastavila infiltrácia

JÚN 2015: ZISTENIE ÚTOKU

- nemecké úrady spolu s CTI firmami analyzujú útok
- identifikované TTPs sú charakteristické pre APT28 (Fancy Bear), skupinu spojenú s GRU
- CTI správy ukazujú prepojenie na iné útoky proti európskym inštitúciám.

2016 – 2017: ANALÝZA A ATRIBÚCIA



1. TECHNICKÁ CTI

- analytici identifikovali malvér použitý pri útoku – Remote Access Trojan (RAT)
- zaznamenané boli podvodné emaily so škodlivými odkazmi (spear-phishing)
- IoCs: domény a IP adresy spojené s ruskou APT skupinou

2. OPERATÍVNA CTI

- útok bol súčasťou širšej kampane zameranej na európske inštitúcie
- ciele: Bundestag, ale aj ďalšie diplomatické misie a politické organizácie
- analýza ukázala koordináciu → časť väčšej operácie GRU

3. TAKTICKÁ CTI

- použité techniky, taktiky a procedúry (TTPs): spear-phishing → infikované prílohy, laterálne šírenie v sieti, exfiltrácia dát cez šifrované kanály
- taktiky sú typické pre APT28 (Fancy Bear)

4. STRATEGICKÁ CTI

- útok bol pripísaný skupine APT28 (Fancy Bear), napojenej na ruskú vojenskú rozviedku GRU
- politický význam: ukázal zraniteľnosť demokratických inštitúcií, otvoril otázku atribúcie a sankcií voči Rusku, stal sa precedensom pre kybernetickú diplomaciu EÚ a NATO

CTI PROCES

2018 – 2020: POLITICKÉ DÔSLEDKY

- nemecké úrady oficiálne obviňujú Rusko z útoku
- v máji 2020 EÚ a Nemecko uvalili sankcie na dôstojníka GRU Dmitrija Badina, identifikovaného ako jedného z aktérov

AKTIVITA – diskusia

Vláda má CTI informácie o plánovanom útoku na energetickú infraštruktúru. Zverejní ich, alebo ich utají? Diskusia o dôsledkoch.

CTI by malo byť čo najotvorenejšie (verejné správy), alebo skôr elitné (pre úzke kruhy expertov)?

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY