DECT

MUNI LAW

Národní centrum kompetence pro kyberbezpečnost

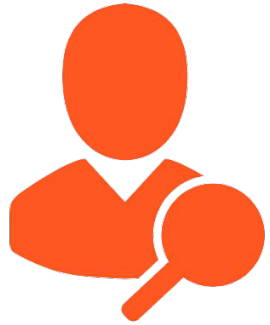
e4j

ORGANIZOVANÁ KYBERKRIMINALITA

VÁCLAV STUPKA

KYBERKRIMINALITA A ORGANIZOVANÝ ZLOČIN

- Kyberkriminalita má poměrně často znaky organizovanosti
- Závisí na charakteru konrkétního trestního jednání
- Míra organizovanosti roste
- "organizace" může být komponentou kyberkriminality stejně jako "cyber" může být komponentou organizovaného zločinu
- Organizovaný zločin využivá prostředky ICT k budování a udržování organizace
- Stále častější vazba mezi tradičními organizovanými sítěmi a hackerskými skupinami
- Vliv terorismu a státních aktérů



ORGANIZOVANÝ ZLOČIN

CO JE ORGANIZOVANÝ ZLOČIN?

- Mezináorodní úmluva proti přeshraničnímu organizovanému zločinu (OSN)
  - Neobsahuje jasnou definici organizovaného zločinu (není shoda, rozhodnutí autorů)
  - Organizovaný zločin = zločin spáchaný organizovanou zločineckou skupinou
  - Organizovaná zločinecká skupina = "Strukturovaná skupina tří a více osob, která existuje po nějakou dobu a jedná s cílem páchání závažnější trestné činnosti zavedené v souladu s touto úmluvou za účelem přímeho nebo nepřímého finančního či materiálního zisku." (Art. 2(a))
- Definice organizovaného zločinu podle UNODC:
  - Trvající kriminální podnik, který racionálně usiluje o zisk z nezákonných činností. Jeho trvající existence je udržována prostřednictvím korupce veřejných činitelů a používání zastrašování, hrozeb nebo síly k ochraně jejích aktivit.

ČESKÉ TRESTNÍ PRÁVO

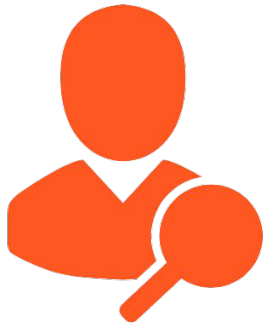
- Podobný přístup jako OSN.
- Organizovaný zločin není definovaný
- §129: ”Organizovaná zločinecká skupina je společenstvím nejméně tří trestně odpovědných osob s vnitřní organizační strukturou, s rozdělením funkcí a dělbou činností, které je zaměřeno na soustavné páchání úmyslné trestné činnosti.”
- Samotná účast na organizované skupině je trestná §361 (zakladatel, účastník, podporovatel)
- Rozdíl mezi organizovanou zločineckou skupinou a organizovanou skupinou (přitěžující okolnost, kvalifikovaná skutková podstata – I §230, 231 apod.)

ORGANIZOAVNÁ KYBERKRIMINALITA

ORGANIZOVANÁ KYBERKRIMINALITA

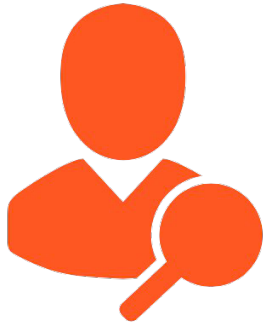
- Organizovaný zločin využívající ICT nástrojů
- Využití tradičních organizovaných skupin při páchání kyberkriminality

- Různé typické aktivity
  - Obchod se zakázaným zbožím na darknetu
  - Podvody, vydírání a praní špinavých peněz
  - Útoky na infrastruktury a data
  - Cybercrime as service

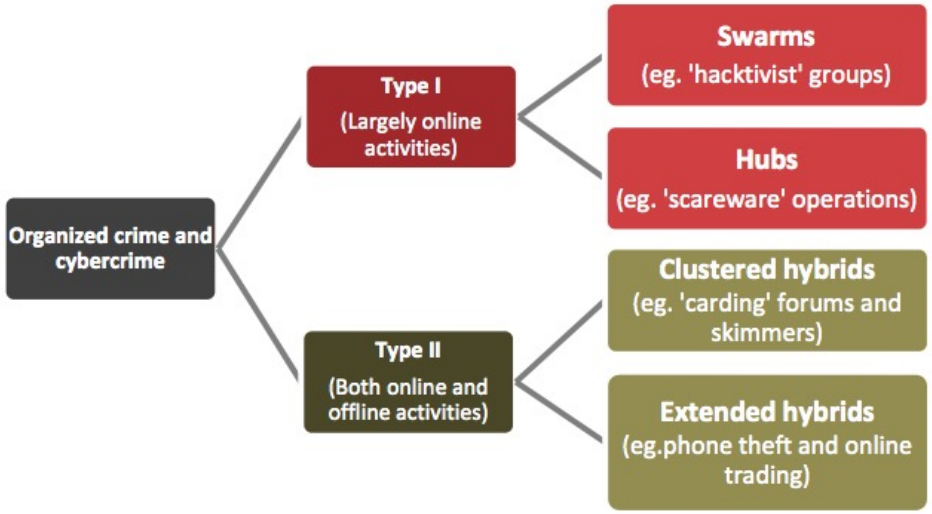


KLASIFIKACE ORGANIZOVANÉ KYBERKRIMINALITY

- Podle úrovně ICT transofrmace
  - Cyber-assisted – především předávání informací, organizace skupiny, vyhledávání obětí
  - Cyber-enabled – například distribuce zakázaného zboží, zakázané pornografie… pomocí internetu
  - Cyber-depended – kyberkriminalita v užším smyslu v rámci organizovaných sločineckých skupin (méně časté)
- Modus operandi
  - Cybercrime against the machine (typická kyberkriminalita – hacking, DoS, apod.)
  - Cybercrime using the machine (online podvody, vydírání apod.)
  - Cybercrime in the machine (zakázaná pornografie, hate speech, zakázaný obsah)
- Skupiny poškozených
  - Jednotlivci
  - Organizace
  - Státy

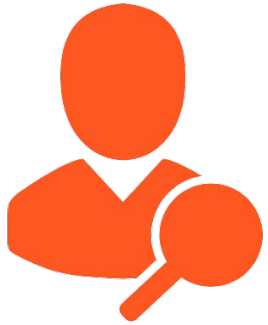


TYPY ZLOČINECKÝCH SKUPIN



Source: BAE Detica/LMU

- Organizované skupiny věnující se kyberkriminalitě a kyberkriminálníci realizující organizovanou trestnou činnost
- Skupiny operující částečně, z většiny nebo zcela online
- Význam geografické, kulturní nebo jazykové blízkosti při formování skupin
- Míra organizovanosti těchto skupin je nižší nebo neznámá
- Častá kvalifikace pro "konvenční" trestné činy



AKTUÁLNÍ VÝZVY

AKTUÁLNÍ VÝZVY

- Průřezové problémy
- Cyber-dependent kriminalita
- Podvody s platebními prostředky
- Zneužívání prostředků darkwebu
- Zneužívání dětí a sexuální kriminalita

PRŮŘEZOVÉ PROBLÉMY

Social engineering

- Covid-19 - nové vektory a nové přístupy
- Intenzivnější využití dezinformačních kampaní
- Sofistikovanější a cílenější phishing
- Poptávka a nabídka CaaS

Kryptoměny

- Kryptoměny často využívané při vydírání
- Podvody při obchodování s kryptoměnami
- Krádeže kryptoměn

Kategorizace

- Stále neexistuje klasifikace kyberkriminality - nemožnost vedení a sdílení statistik a dat

Going dark

- Organizované skupiny využívají šifrovacích nástrojů, bulletproof služeb apod., které znemožňují idnetifikaci

CYBER DEPENDENT KRIMINALITA

Ransomware

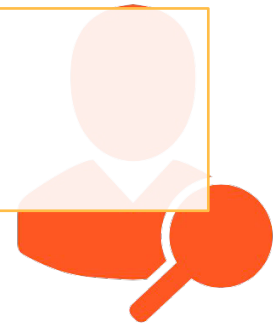
- Čím dál sofistikovanější a cílenější - zapojení velkých organizovaných skupin
- Stále častější hrozba zveřejněním dat
- Supply-chain ransomware, delayed ransomware
- Širší spolupráce mezi různými skupinami, vyšší investice a výdělky

Malware

- Stále sofistikovanější, APT
- Trojské koně na sběr dat
- Schopnost skrývání do legitimních zpráv
- Commodity malware, MaaS, AaaS

Silný potenciál DDoS útoků

- Stabilní intenzita útoků
- Stoupající sofistikovanost - automatizace
- Často poskytovány jak cílené útoky CaaS
- Rozvoj využití IoT



PODVODY S PLATEBNÍMI PROSTŘEDKY

SIM swapping

- Nástroj pro získání identity
- Cílem je obejít 2FA
- Rovněž SMiShing
- Velmi cílené útoky

BEC

- Nejčastěji CEO fraud, nebo invoice fraud
- Vysoce cílené útoky
- Využití pandemické situace a home office
- častěji mířené na menší společnosti

Podvody s online investicemi

- Stále častější sofitikovné podvody (kryptoměny, akcie, komodity - get rich quich scheme)
- Poměrně široké zapojení organizovaných sítí (falešné společnosti, call centra, apod)
- Využití dezinofrmačních sítí, pandemické situace, aktuálního dění

Card-not-present

- Hlavně carding a e-skimming
- Zaměření na menší I větší obchodníky, falešné eshopy
- Často obchodované související osobní údaje
- Rovněž ATM black-boxing

ZNEUŽÍVÁNÍ DARKWEBU

Online tržiště

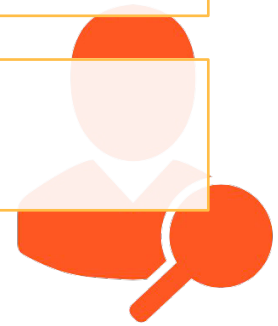
- Vysoká volatilita – hacking nebo exit scams
- Zatím žádný velký hráč typu Silkroad nebo Sheep Marketplace
- DarknetTrust – nový typ služby – ověřování důvěryhodnosti vendor na různých tržištích
- Rozvoj vyhledávačů a rozcestníků

Větší zacílení na bezpečnost a anonymitu

- Implementace bezpečnostních standardů a technologií
- Wallet-less a user-less tržiště
- Reputační a navigační systémy
- Etiketa a morální pravidla – vyloučení exponovaných oblastí
- Nové komunikační nástroje
- Rozvoj decentralizovaných tržišt, TOR stále hraje prim
- Na druhou stranu rozvoj clearweb aktivit

Zboží

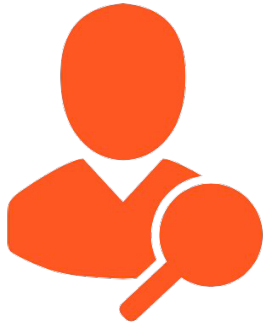
- Stále vice se nabízí na tržištích digitální zboží a služby (data, přístupy, CaaS)
- Často se obchoduje s identitami (imigranti, falešné účty, společnosti, etc.)
- Rozvoj trhu se zbožím díky pandemii



BOJ S ORGANIZOVANOU KYBERKRIMINALITOU

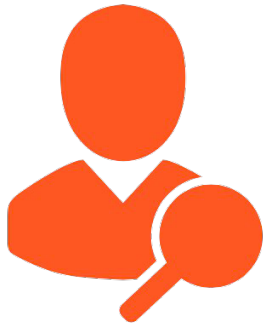
HLAVNÍ NÁSTROJE

- Silnější orgány činné v trestním řízení
- Spolupráce
- Technická řešení
- Vzdělávání a informovanost



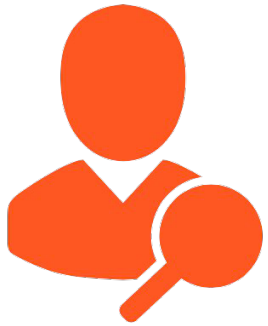
SILNĚJŠÍ ORGÁNY

- Posilování personálních kapacit, odbornosti a povědomí
  - Vzdělávání nespecializovaných příslušníků
  - Posilování kapacit specializovaných jednotek
  - Zaměření na vzdělávání i státních zástupců a soudců
  - Technické vybavování
- Dlouhodobý monitoring známých vektorů a hrozeb
  - V rámci prevence
  - Za využití agentů a utajovaných operací
  - Spolupráce se zpravodajskými službami



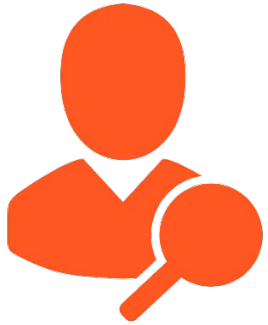
SPOLUPRÁCE

- Především mezinárodní
  - Předávání informací (z monitoringu, o hrozbách, o postupech apod)
  - Poskytování technické spolupráce
  - Poskytování součinnosti
  - Společné vyšetřovací týmy
- Se soukromým sektorem a dalšími OVM



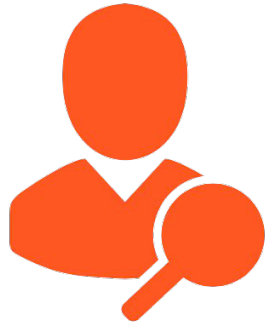
TECHNICKÁ ŘEŠENÍ

- Scanování clear webu i dark webu
- AI a big data analýza
- Jazyková analýza, obrazová analýza apod.
- Nástroje pro efektivní transfer elektronických důkazů
- Nástroje pro identifikaci osob



VZDĚLÁVÁNÍ A INFORMOVANOST

- Vzdělávací kampaně národních a mezinárodních institucí
  - Europol – no more ransom, money muling
  - UNODC – Counterfeit – Don't buy into organized crime
  - INTERPOL - #stopillicittrade
  - OSN – Blue Heart Campaign
  - apod.
- Vzdělávání v rámci systému školství ohledně bezpečného chování na internetu



DÍKY ZA POZORNOST

STUPKA@NC3.CZ