Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI
ŽILINSKEJ UNIVERZITY V ŽILINE

Malvér a základné stratégie prevencie a detekcie

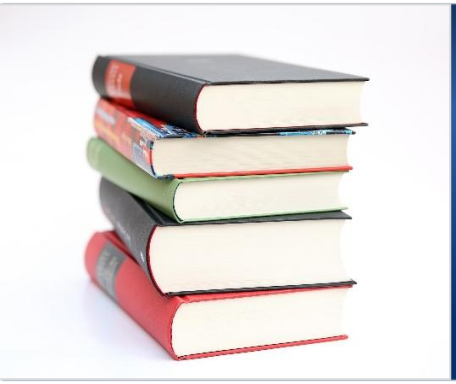
Ochrana koncových zariadení (Blok IV)

Kurz: Špecialista kybernetickej bezečnosti vo verejnej správe

Dalibor Kafka (Pavel Segeč)

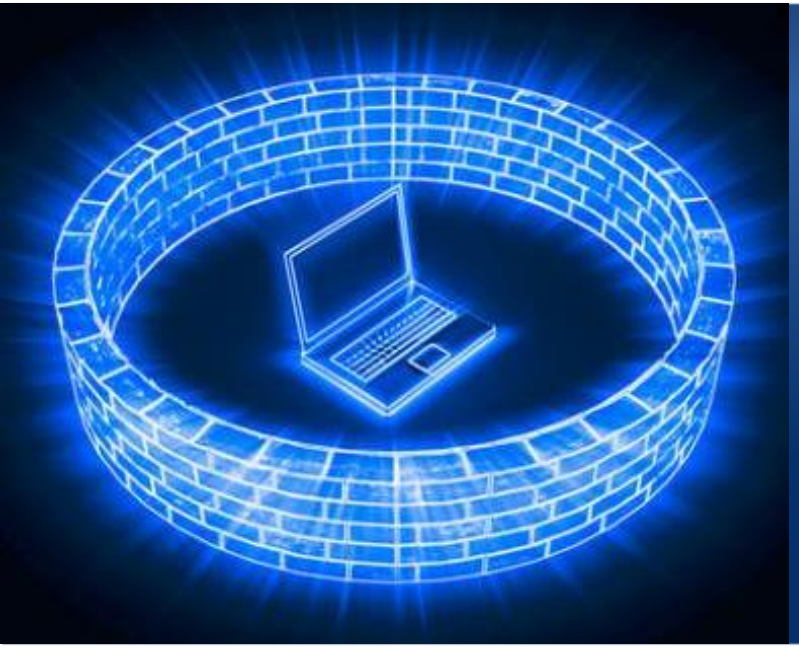
KC KYB UNIZA https://kc.uniza.sk

Dalibor.Kafka@fri.uniza.sk (Pavel.Segec@fri.uniza.sk)



Čo nás čaká ...

- Základné pojmy
- Sieťové hrozby
- Hrozby koncových zariadení - Malware
- Ochrana proti malwaru
- Informácie o hrozbách (Threat Intelligence)



Základné pojmy

Pojmy / definície

- Bežné bezpečnostné slovné spojenia:
  - Asset
    - Akákoľvek hodnota, ktorú vlastní jednotlivec alebo spoločnosť
    - HW, SW, služby, dáta/dokumenty/, ľudia, …
  - Vulnerability (Zraniteľnosť)
    - Slabé stránky systému/siete (nezabezpečený protokol, chyby v kódovaní, slabé politiky atď.)
    - Môže byť zneužité útočníkom
  - Threat (Hrozba)
    - Potenciál zraniteľnosti. Hrozba využíva existujúcu zraniteľnosť konkrétneho aktíva na spôsobenie škody..
    - Potenciálna nebezpečná udalosť
  - Exploit
    - Mechanizmus používaný na využitie zraniteľnosti na ohrozenie aktíva
- Attack (útok)
  - Čin, ktorým sa subjekt pokúša vyhnúť bezpečnostným službám a porušiť bezpečnostnú politiku
  - Vnútri/vonku, Pasívne/Aktívne
- Vektor sieťového útoku
  - cesta alebo iný spôsob, akým sa útočník snaží získať prístup
  - Metóda
- Povrch útoku
  - Celkový súčet zraniteľností v danom systéme, ktoré môže útočný vektor použiť alebo vytvoriť
  - Bezpečnostný cieľ => znížiť povrch útoku

Terms / definitions

- Bežné bezpečnostné slovné spojenia:
  - Risk (Riziko)
    - Potenciál hrozby zneužiť zraniteľnosť aktíva
    - Pravdepodobnosť výskytu udalosti
  - Mitigácia
    - Opatrenia na zníženie závažnosti zraniteľnosti
    - Často označované ako protiopatrenia
  - Risk manažment
    - Proces, ktorý vyvažuje prevádzkové náklady na zabezpečenie ochranných opatrení so ziskami dosiahnutými ochranou aktíva.

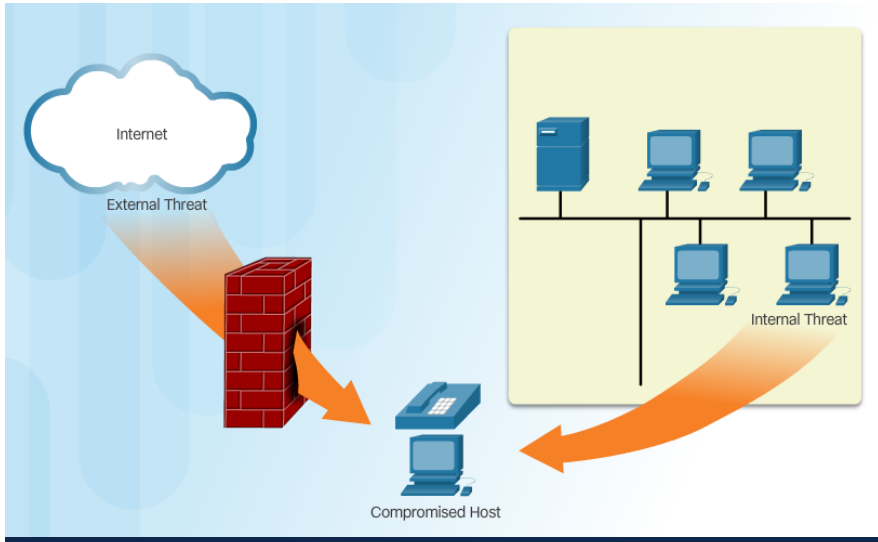
- Ako riadiť riziká (napríklad)
  - Akceptácia rizika
    - Náklady na možnosti riadenia rizík prevyšujú náklady na samotné riziko.
    - Riziko je akceptované, nevyžaduje sa žiadna akcia.
  - Vyhýbanie sa riziku
    - Vyhýbanie sa akémukoľvek vystaveniu sa riziku elimináciou činnosti alebo zariadenia, ktoré predstavuje riziko
    - Stratili sme aj výhody danej činnosti
  - Redukovanie rizika
    - Prijatie opatrení na zníženie/zníženie rizika
    - Vyžaduje si starostlivé vyhodnotenie nákladov na straty, stratégie zmierňovania a výhod získaných z operácie alebo činnosti, ktorá je ohrozená.
  - Presun rizika
    - Riziko sa prenáša na dobrovoľnú tretiu stranu, napríklad na poisťovňu.
    - Poznámka: viac informácií nájdete v téme Kybernetická bezpečnosť

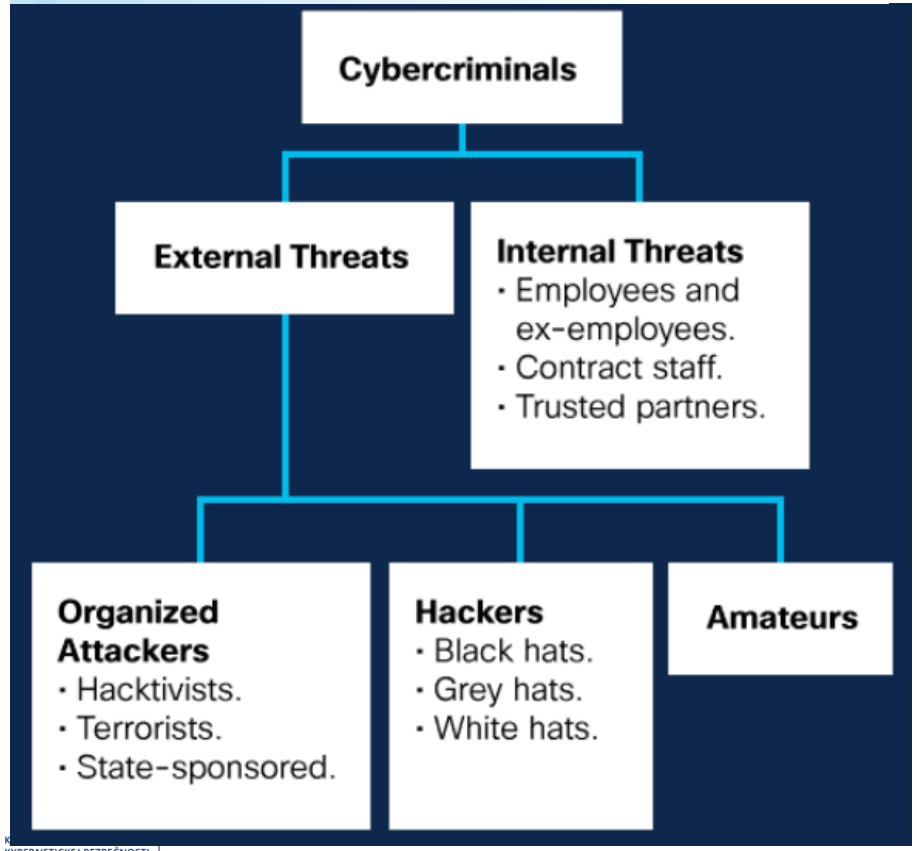
Typy kybernetických hrozieb

- Softvérové útoky
  - Malware, DOS …
- Softvérové chyby
  - Softvérové chyby/chyby, nedostupnosť softvéru, skripty medzi stránkami, nelegálne zdieľanie softvéru
- Sabotáž
  - Preniknutie a kompromitovanie autorizovaného používateľa
    - Databáza, webová stránka, IS…
- Ľudská chyba
  - Nesprávna konfigurácia, neúmyselné zadanie údajov, správanie
- Krádež
  - Ukradnutý hardvér (notebook, počítač, iné zariadenia)
- Poruchy hardvéru
  - Havárie hardvéru (pevný disk a iné komponenty)
- Prerušenie služby
  - Výpadky elektrickej energie.
  - Poškodenie vodou v dôsledku poruchy sprinklerového systému.
- Prírodné katastrofy
  - Silné búrky, ako sú hurikány alebo tornáda, zemetrasenia, záplavy, požiare.

Vnútorné vs. vonkajšie hrozby

- **Interné (vnútorné) hrozby**
  - Zvyčajne vykonávané súčasnými alebo bývalými zamestnancami a inými zmluvnými partnermi
  - Vykonané náhodne alebo úmyselne
    - Nesprávne zaobchádzanie s dôvernými údajmi, pripojenie k infikovaným médiám alebo prístup k škodlivým e-mailom alebo webovým stránkam, zlý úsudok.
    - Podvod, sabotáž, špionáž, krádež majetku...
  - Potenciál väčších škôd ako externých
    - Dôvody: Priamy prístup, interné znalosti (sieť, infraštruktúra, údaje, služby, ľudia, postupy, bezpečnosť...)
  - Získanie hybnej sily
- **Externé hrozby**
  - Outsidery spoločnosti
    - Amatérski alebo skúsení útočníci
  - Snaha získať prístup k interným zdrojom organizácie





Vektor straty dát (príklad aktíva)

- Dáta (informácie) => pravdepodobne najcennejší majetok organizácie
- Strata dát vedie k
  - Poškodeniu značky a strate reputácie alebo dôvery
  - Strate konkurenčnej výhody
  - Strate zákazníkov
  - Strate príjmov, pokutám
  - Súdnym sporom a možnému vyšetrovaniu
  - …
- Vektory straty údajov (únik údajov):
  - E-mail/webmail/sociálne inžinierstvo/instant messaging/sociálne médiá
  - Bezdrôtové zariadenia
  - Nešifrované zariadenia
  - Cloudové úložiská
  - Vymeniteľné médiá
  - Tlačové kópie
  - Nesprávna kontrola prístupu
  - ...

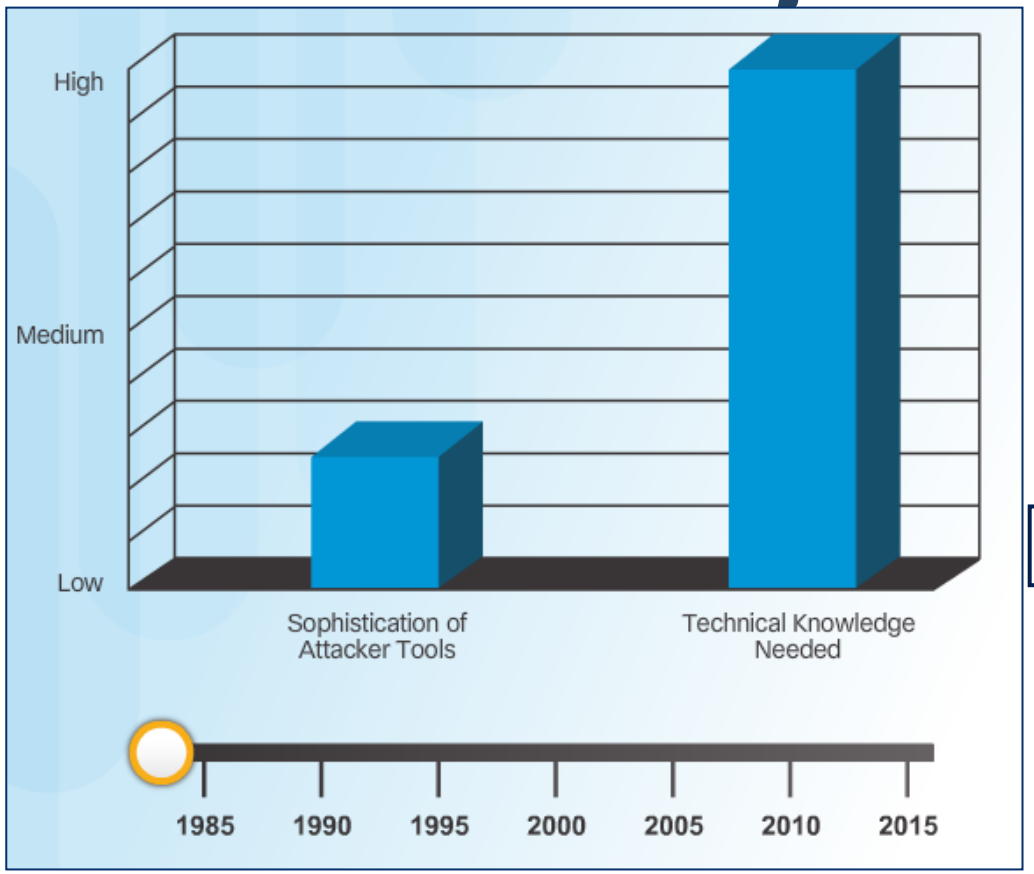
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Sieťové hrozby

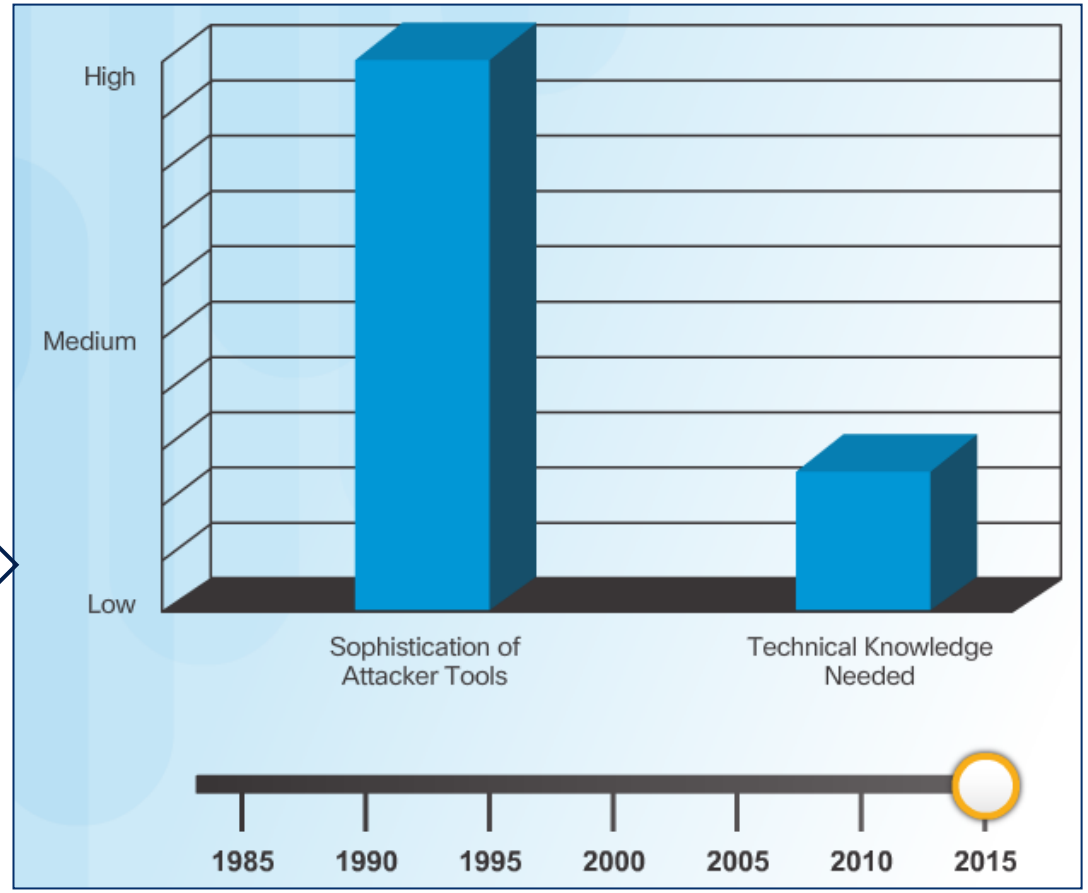
Hacker a evolúcia hackerov

- Hacker
  - Teraz (žijeme v zjednodušenom svete)
    - Zvyčajne sieťový útočník
      - Zneužíva zraniteľnosti
  - Predtým, alebo lepšia definícia
    - Zručný počítačový expert, ktorý využíva svoje technické znalosti na prekonanie problému
- Klasifikácia hackerov (Dobrý, zlý a škaredý - Sergio)
  - White Hat (dobrý)
    - Zručnosti pre dobro
    - Etickí hackeri, penetesteri, skill testeri, výskumníci zraniteľností, administrátori
  - Black Hat (zlý)
    - Neetické zločinci, ktorí úmyselne páchajú krádeže
    - Hackerské útoky za účelom osobného zisku alebo zo zlomyseľných dôvodov
  - Gray Hat
    - Robí neetické veci, ale nie pre zisk
  - Green, Red, Blue Hat
- Moderné hackerské tituly :
  - Script Kiddies (blue)
    - Tínedžeri alebo neskúsení používatelia
    - Používajte vopred pripravené skripty a nástroje (Metasploit)
  - Brokeri zraniteľností (grey)
    - Hľadanie a ohlásenie
  - Hacktivists (grey)
    - Protestovať proti niečomu(anonymous)
  - Kybernetický zločinci (black)
    - Pôsobí z pozadia (Lone volwes)
    - kupuje, predáva a obchoduje s útočnými nástrojmi, zero-day exploit, službami botnetov, bankovými trójskymi koňmi, keyloggermi, súkromnými informáciami, duševným vlastníctvom a oveľa viac.
  - Hackeri sponzorovaní štátom (????)
    - Najnovší typ, veľmi pokročilý
    - Útočníci financovaní vládou (stuxnet)
      - Ale nie sú oficiálne priznaní
    - Zvyšuje sa počet

Hackerské nástroje



Evolúcia



- Jednoduché, svojvoľne vytvorené

- Množstvo predpripravených
- Niektoré veľmi sofistikované s vysokou mierov automatizácie

Kategórie bezpečnostných/útočných nástrojov

- Nástroje a súpravy nástrojov na penetračné testovanie:
  - Lámače hesiel
    - Nazývajú sa aj nástroje na obnovu hesla
    - Ripper, Ophcrack, L0phtCrack, THC Hydra, Rainbow Crack, Meduse
  - Bezdrôtové hackovanie
    - Kismet, Aircrack-ng, KisMAC, Firesheep
  - Skenovanie a hacking siete
    - Sondovanie siete
    - Nmap, SuperScan, Angry IP Scanner, hping3
  - Tvorba paketov
    - Nástroje na testovanie firewallu, generátory paketov
    - Hping, scapy, Socat, Netcat, Nemesis …
  - Sniffery paketov
    - Zachytávanie a analýza
    - Wireshark, tcpdump, Ettercap, Paros, Dsniff, Fiddler, EtherApe. SSLstrip …
  - Detektory rootkitov
    - Kontroly integrity adresárov a súborov
    - AIDE, NetFilter …
- Fuzzery na vyhľadávanie zraniteľností
  - Fuzzing = technika zabezpečenia používaná na odhaľovanie chýb v kóde a bezpečnostných medzier v softvéri, operačných systémoch alebo sieťach
  - Fuzzer, Social Engineering Toolkit (SET), Skipfish, Wapitti, W3af, wfuzz …
- Forenzné
  - techniky počítačového vyšetrovania a analýzy v záujme určenia potenciálnych právnych dôkazov.
  - Kit, Helix, Maltego, Encase
- Debuggery
  - Reverzné inžinierstvo
  - GDB, WinDog, IDA, Imunity Debugger
- Encrypcia
- Zneužívanie zraniteľností
  - Metasploit, Netsparker, Sqlmap, Core Impact
- Skenery zraniteľností
  - Skenovanie sieťovej a systémovej identity
  - OpenVAS, Nessus, Nipper, Secuma PSI
- … mnohé z nich sú založené na *nix

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Penetračné testovanie (offensívna bezpečnosť)

- Pen testing
  - čin hodnotenia bezpečnostných zraniteľností počítačového systému, siete alebo organizácie.
  - Cieľom testu je narušiť systémy, ľudí, procesy a kód, aby sa odhalili zraniteľnosti, ktoré by sa dali zneužiť.
  - Informácie sa používajú na zlepšenie obranyschopnosti systému.

- Fázy
  - **plánovanie**
    - Zhromaždite čo najviac informácií o cieľovom systéme alebo sieti, jej potenciálnych zraniteľnostiach a zneužívaniach, ktoré môžete proti nej použiť.
    - Vykonajte pasívny alebo aktívny prieskum (footprinting) a výskum zraniteľností..
  - **Skenovanie**
    - Aktívny prieskum, ktorý skúma cieľový systém alebo sieť a identifikuje potenciálne slabé miesta
      - v prípade zneužitia mohol útočníkovi poskytnúť prístup.
    - Aktívny prieskum môže zahŕňať:
      - skenovanie portov
      - skenovanie zraniteľností
      - nadviazanie aktívneho pripojenia k cieľu (vyčíslenie)

Penetračné Testovanie

- **Získanie prístupu**
  - Prístup k cieľovému systému a odhaľovanie sieťovej prevádzky,
  - Metódy
    - spustenie exploitu s užitočným zaťažením do systému
    - prelomenie fyzických bariér k aktívam
  - sociálne inžinierstvo
  - zneužívanie zraniteľností webových stránok
  - zneužívanie zraniteľností alebo nesprávnych konfigurácií softvéru a hardvéru
  - prelomenie zabezpečenia kontroly prístupu
  - prelomenie slabej šifrovanej siete Wi-Fi.
- **Udržiavanie prístupu**
  - Zistite, ktoré údaje a systémy sú zraniteľné voči zneužitiu.
  - Dôležité je zostať nepozorovaný, zvyčajne pomocou zadných vrátok, trójskych koní, rootkitov a iných skrytých kanálov na skrytie svojej prítomnosti.
- **Zhromažďovanie údajov**
  - Zhromažďujte údaje, ktoré považujú za cenné
- **Analýza a reportovanie**
  - Poskytnite spätnú väzbu prostredníctvom správy, ktorá odporúča aktualizácie produktov, politík a školení na zlepšenie bezpečnosti organizácie.

Hrozby koncových zariadení - Malware

Rôzne typy Malwaru

- Malware
  - Wiki hovorí: “Malvér alebo škodlivý softvér je akýkoľvek softvér zámerne navrhnutý tak, aby spôsobil poškodenie počítača, servera, klienta alebo počítačovej siete.”
- Najčastejšie kategórie
  - Virus
  - Adware
  - Spyware
  - Worms
  - Trojans
  - Cryptoware/Ransomware
  - Commodity loaders
  - Fileless malware
  - Rootkits
  - Bots
  - iné ….

Vírusy

- Škodlivý kód pripojený k spustiteľným a často legitímnym súborom
  - Vyžaduje sa na spustenie hostiteľského programu
- Väčšina z nich vyžaduje aktiváciu používateľa
  - Otvoriť súbor, otvoriť prílohy pošty ...
- Môže začať okamžite alebo chvíľu zostať neaktívny
- Viacero typov
  - Nepoškodzujúce, deštruktívne…
  - Môžu sa snažiť o propagáciu samého seba
    - Iné spôsoby propagácie
      - USB, CDs, DVDs, sieťové zdieľanie a emailová komunikácia (najčastejšie)

Adware/Spyware

- Adware
  - Softvér, ktorý zobrazuje reklamy, na zariadení používateľa.
  - Adware generuje svojim vývojárom príjmy (googleADS)
  - škodlivý adware môže sledovať správanie používateľov a slúžiť ako brána pre nebezpečnejší malware.
  - Android.MobiDash, Android.HiddenAds

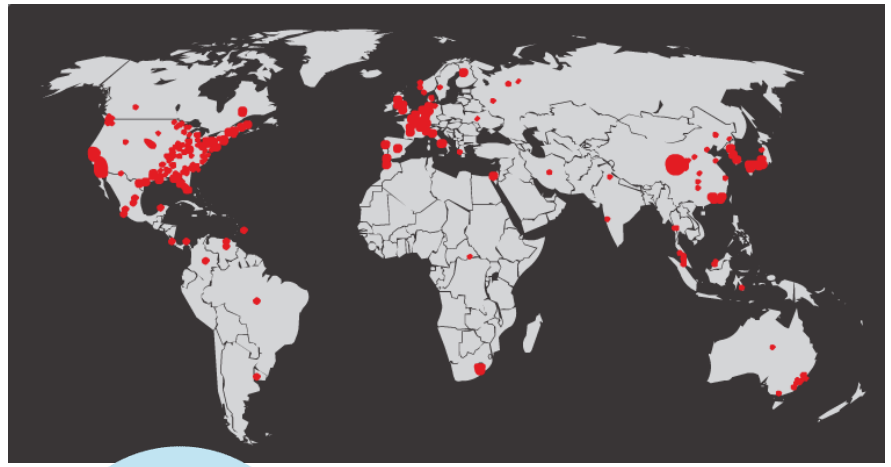
- Spyware
  - Škodlivý softvér, ktorý tajne zhromažďuje informácie o zariadení používateľa.
  - Často sa inštaluje cez klamlivé reklamy, infikované e-mailové prílohy, bežne používané aplikácie
  - Lumma, Redline, Pegasus

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

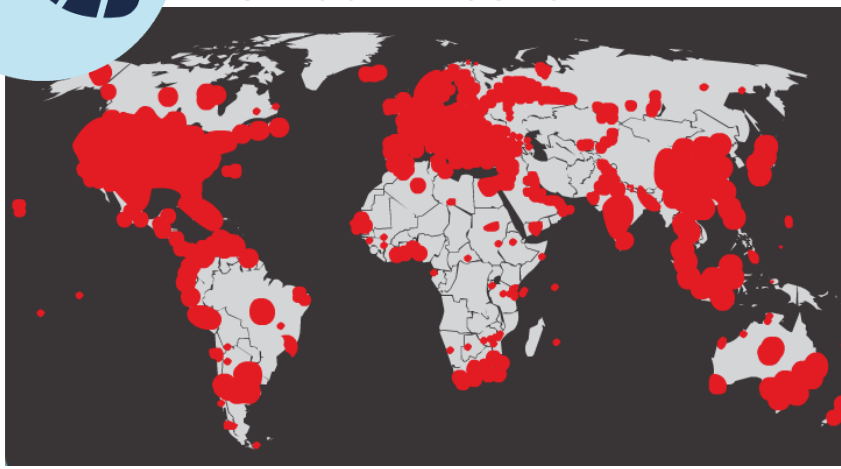
Worm

- … hra
- Ale aj škodlivý kód, ktorý sa nezávisle replikuje
  - Zneužíva zraniteľnosti v sieťach
    - A šíri sa rýchlo
  - Nepotrebuje hostujúci program
  - Komponenty:
    - Umožnenie zraniteľnosti (jej zneužitie)
    - Propagačný mechanismus
    - Payload
- Uskutočnili niektoré z najničivejších útokov v histórii
  - Sql Slammer, ILOVEYOU, Code Red, Melisa, MyDoom, Conflicker,
    - Poznámka: *Vyzeral, že už neexistuje ale vrátil sa*
  - Shai-Halud *(zraniteľnosť NPM),* LitterDrifter *(použitý pri útoku na ukrajinské štátne služby)* RasberyRobin/EchoBot (šírený cez USB a cieľom sú IOT zariadenia)

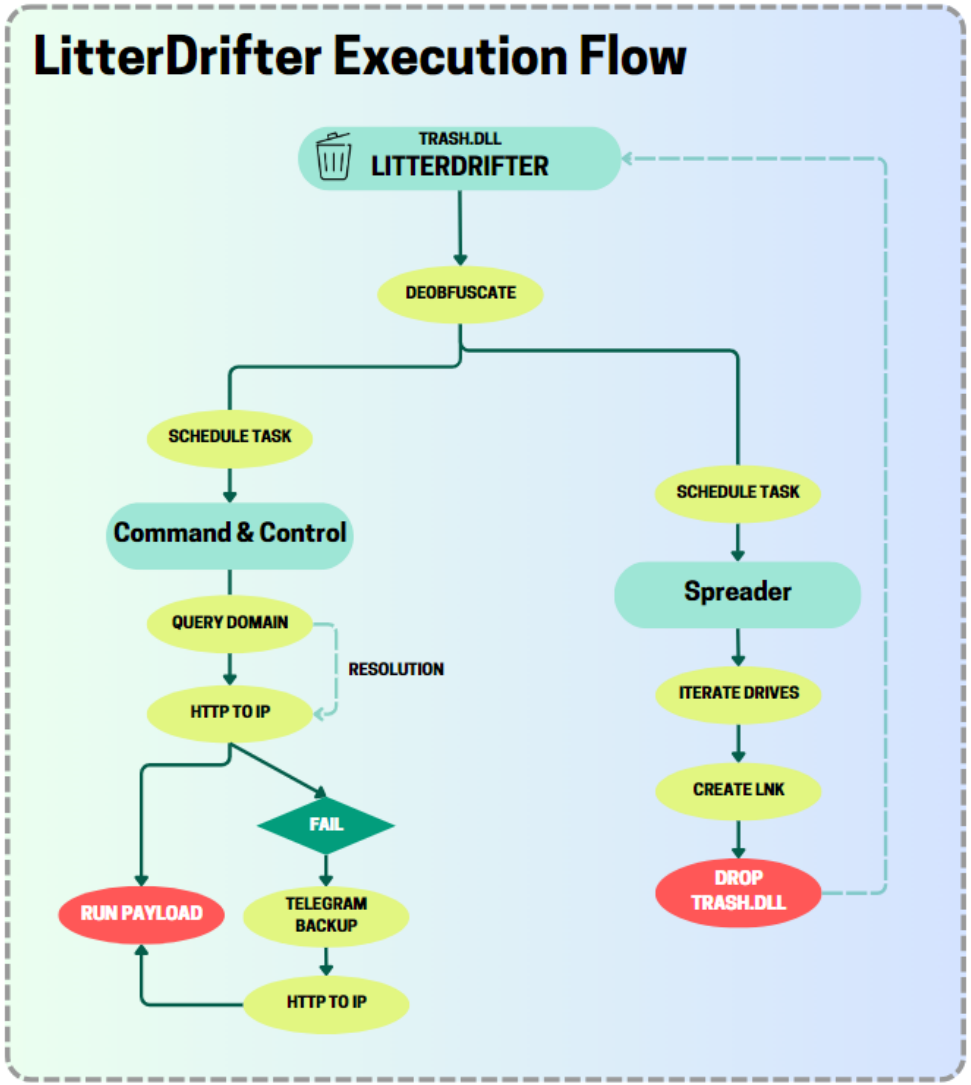
Iniciálna Code Red Worm infekcia

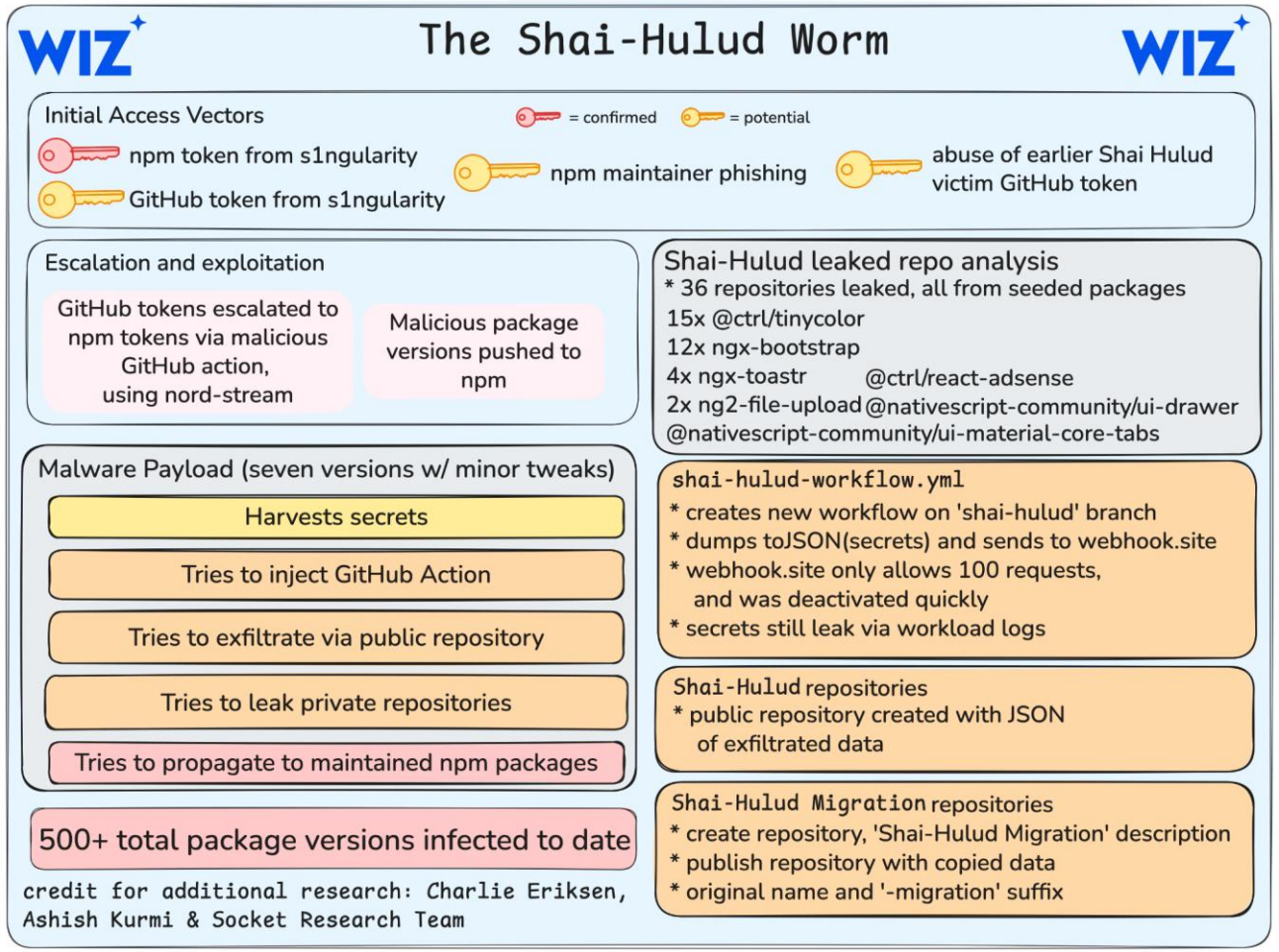


Code Red Worm
19 hodín neskôr



Worm





Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Trojský kôň(pamätáte si mytológiu?)

- Wiki: *škodlivý program, ktorý sa falošne prezentuje ako bežný, neškodný program alebo nástroj, aby presvedčil obeť k jeho inštalácii.*
- Pripojené k spustiteľným súborom alebo používa sociálne inžinierstvo
  - Online hry, freeware, emailové prílohy
  - Vykonáva škodlivé operácie pod rúškom požadovanej funkcie
    - Zneužíva privilégiá používateľa, ktorý ho spúšťa
- Mnoho moderných formulárov funguje ako Backdoor
  - Kontaktuje ovládač a umožňuje neoprávnený prístup
- Vo všeobecnosti
  - Nepokúša sa vložiť do iných súborov ani sa šíriť
- Ťažšie odhaliteľné
  - Hľadajte vysoké využitie procesora

Klasifikácie (podľa poškodenia):

- Security software disabler TH
  - Vypnúť antivírus
- Transfer pre vzdialený prístup (RAT)
- Transfer pre odosielanie údajov
  - Odosiela súkromné alebo citlivé údaje
- Deštruktívne TH
- Dropper
  - Sťahuje a inštaluje malware
- Proxy TH
  - Umožňuje z infikovaného zariadenia spraviť proxy server
- FTP TH
  - Umožňuje neoprávnený prenos súborov
- DoS TH
  - Spomaluje alebo zastavuje sieťové aktivity

Cryptoware/Ransomware

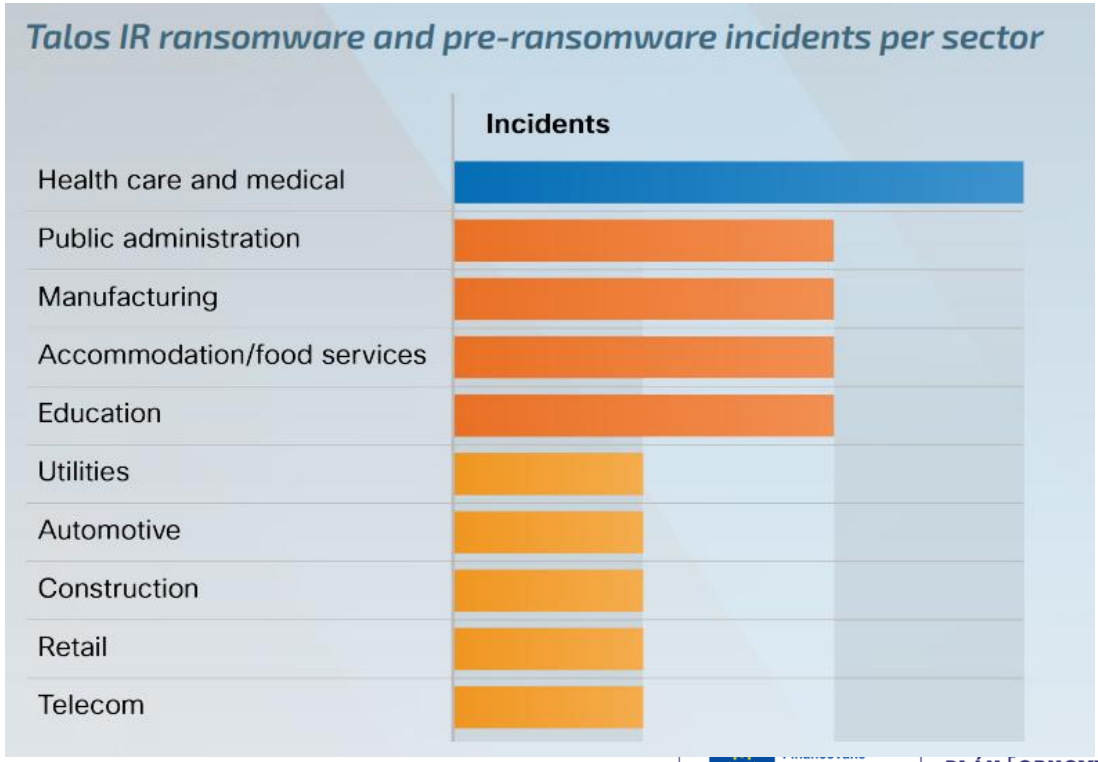
- Zablokuje prístup k infikovanému počítačovému systému alebo súborom
  - Screen-Locker
- Kľúčové charakteristiky ransomvéru:
  - Šifrovanie údajov
  - Požiadavky na výkupné
  - Dvojité a trojité vydieranie: zahŕňa ďalšie hrozby (únik ukradnutých údajov online, požiadavka na platbu atď.)
  - Rýchle nasadenie: Môže sa rýchlo šíriťVyskakovacie správy:
    - Obetiam sa zobrazujú vyskakovacie správy požadujúce platbu za odomknutie ich súborov.
  - Manipulácia so súbormi: presunutie, premenovanie alebo zmena povolení
- Ransomware hrozby:
  - LockBit: Známy pre svoje rýchle šírenie v rámci organizácií a funguje ako Ransomware-as-a-Service (RaaS).
    - 2019-2024 + 9.2025 versia 5.0
  - Presun všetkých na RaaS
  - Najpoužívanejšie sú – Qilin, Akira, Play, Safepay, Dragonforce
  - Staršie
    - Cryptolocker, WannaCry

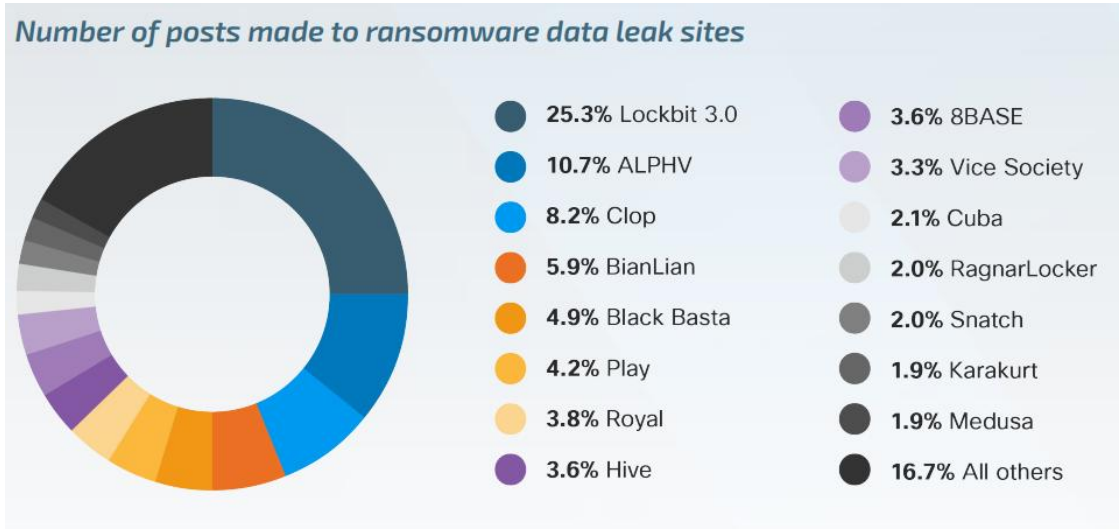
Are you victim? Check: https://www.nomoreransom.org/sk/index.html

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

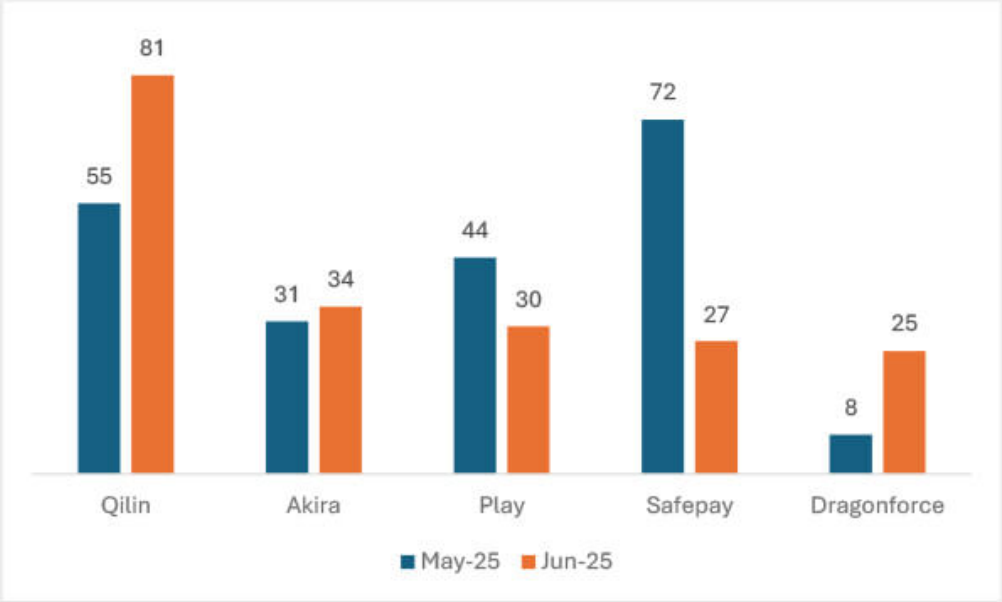
Ransomware attacks

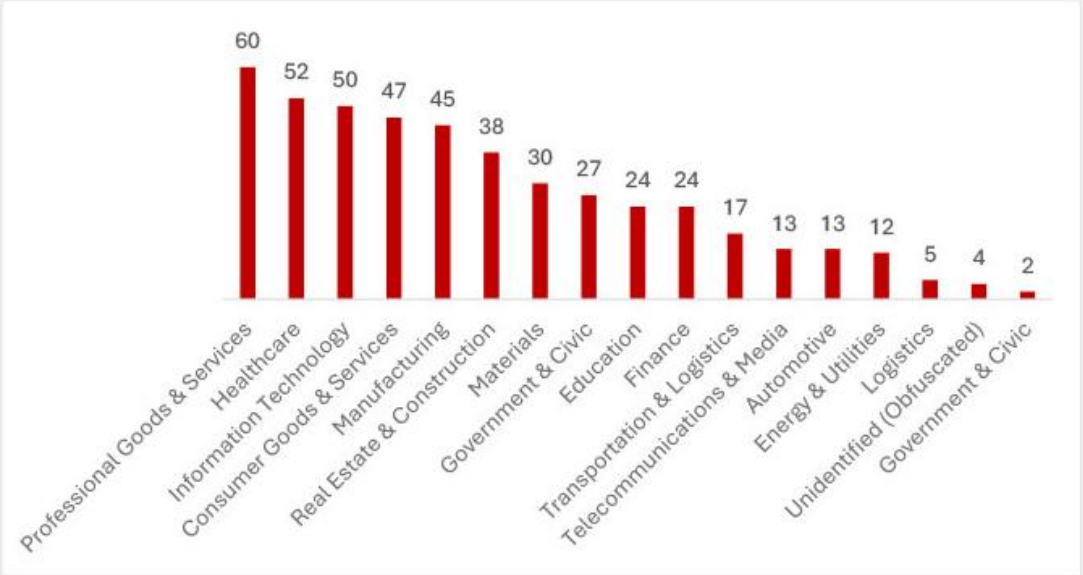
- 20% zo všetkých aktívít
- Pravidelné zmeny názvov (unikajúce zdrojové kódy)
- Začali využívať Zero-day zraniteľnosti

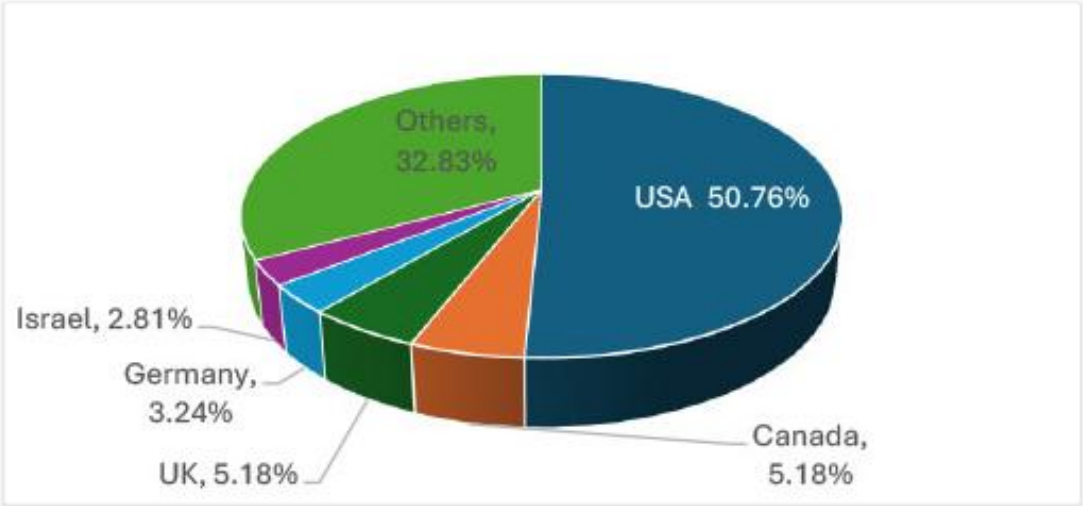




Ransomware

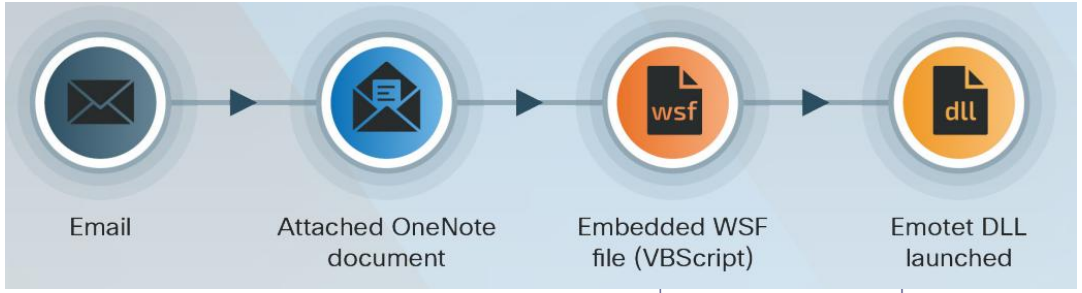


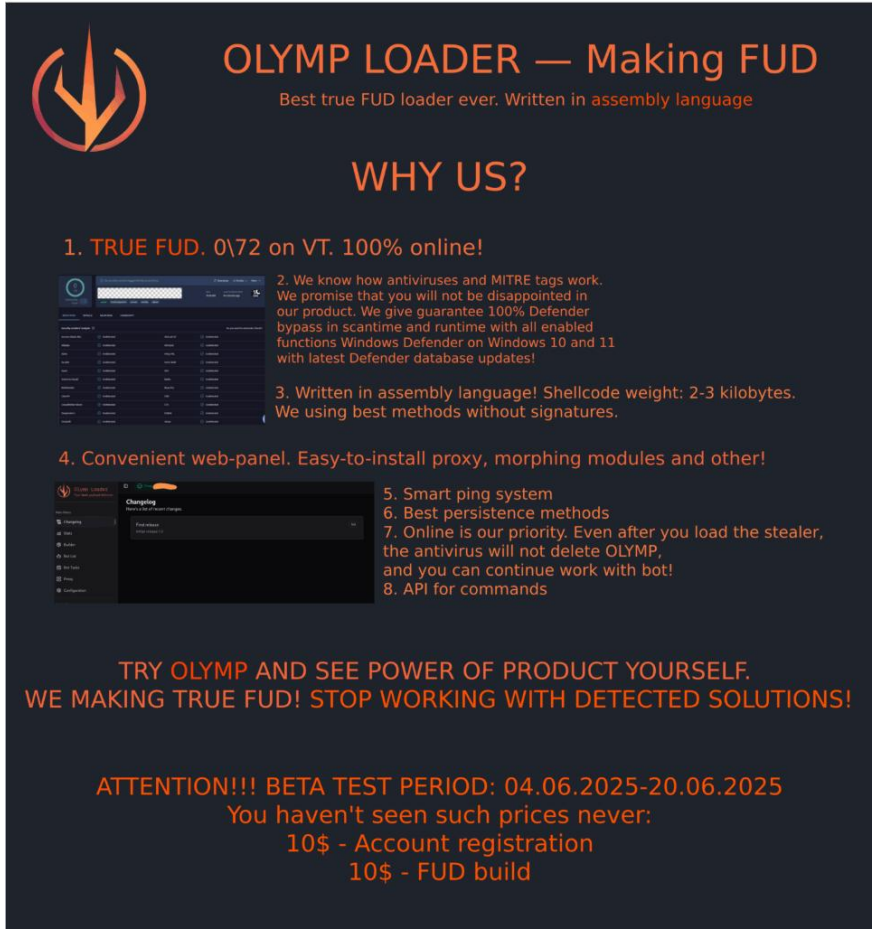


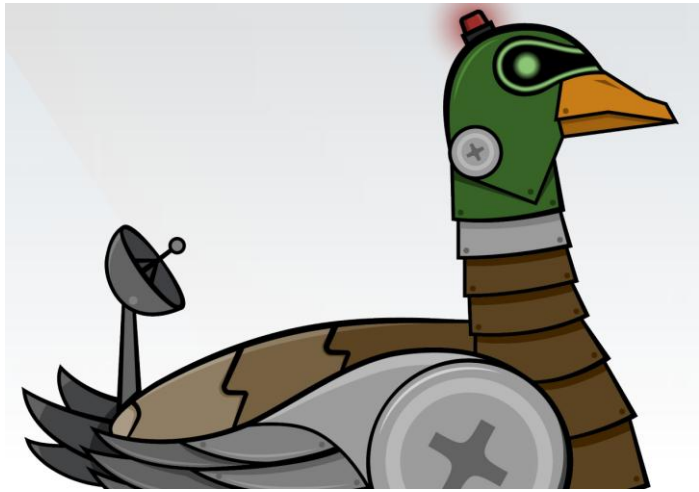


Commodity Loaders

- Typ malvéru používaného na nasadenie ďalších škodlivých dát do systému obete.
  - často šírený cez emaily ale aj nebezpečné stránky, phishing a iné
- Hlavné charakteristiky:
  - Iniciálna infekcia:
    - Často začína ako trójsky kôň (správa sa ako bežná aplikácia).
  - Druhá etapa malwaru:
    - Akonáhle je systém napadnutý => stiahne a spustí ďalší malware (ransomware alebo spyware).
  - Komerčná dostupnosť:
    - Často sa predávaj, vďaka čomu sú ľahko dostupné. (Telegram)
  - Globálny dopad:
    - Sú neustálou hrozbou s významným globálnym dopadom, ktorá ovplyvňuje rôzne odvetvia a organizácie.
- Examples: Olymp loader, IcedID, Emmenhtal, QakBot.







Other malware

- Rootkity
  - Navrhnuté na úpravu operačného systému a umožnenie privilegovaného prístupu
    - Umožňujú prístup k počítaču (root)
  - Často maskujú jeho existenciu
- Backdoor
  - Poskytujú vzdialený prístup k systému obchádzajúc bežné overovanie
  - Príklad: Netbus, Back Office
- Logické bomby
  - Čakajú na spúšťač, ako je napríklad zadaný dátum alebo položka v databáze, aby spustili škodlivý kód
- File-less malware
  - škodlivý kód, ktorý beží v pamäti počítača (RAM) namiesto toho, aby sa zapísal na pevný disk
    - Aplikuje sa cez CLI/ PowerShell/ WMI
- Scareware/Rogueware
  - Šokuje alebo vyvoláva úzkosť.
  - Zavádza vás a vyvoláva dojem, že ste napadnutí hackermi/infikovaní.
    - sociálne inžinierstvo
- Cryptojacking
  - Slúži na ťaženie kryptomien
- ….

Ochrana proti malwaru

Ochrana proti vírusom

Prevencia:

- Používanie dôveryhodného antivírusového a antimalvérového softvéru s heuristickou analýzou
- Pravidelné aktualizácie OS a aplikácií
- Zákaz automatického spúšťania médií (USB, sieťové disky)
- Digitálne podpisovanie interného softvéru

Detekcia a reakcia:

- Centrálne monitorovanie antivírusových udalostí (SIEM)
- Karanténa a analýza infikovaných súborov
- Obnova systémov z čistých záloh

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Ochrana proti Adware

Prevencia:

- Inštalácia softvéru len z overených zdrojov
- Blokovanie neautorizovaných rozšírení prehliadača
- Politika obmedzujúca práva používateľov na inštalácie
- Používanie DNS filtrov a web proxy

Detekcia a odstránenie:

- Monitoring sieťového prenosu (reklamné domény, presmerovania)
- Kontrola plánovača úloh a spúšťacích skriptov

Ochrana proti Spyware

Prevencia:

- Zakázanie neautorizovaných doplnkov a aplikácií
- Pravidelný audit oprávnení (kamera, mikrofón, clipboard)
- Implementácia DLP systému
- Šifrovanie disku a citlivých dát

Detekcia:

- Behaviorálna analýza procesov
- EDR agenti na koncových zariadeniach

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Ochrana proti červom (Worms)

Prevencia:

- Segmentácia sietí a oddelenie zón (LAN, DMZ, OT)
- Blokovanie nepotrebných portov a protokolov
- Silné autentifikačné politiky pre zdieľané zdroje
- Automatické záplaty zraniteľností

Detekcia:

- IDS/IPS systém – detekcia sieťovej replikácie
- Monitorovanie sieťového správania

Ochrana proti Trójskym koňom

Prevencia:

- Aplikačný whitelisting (AppLocker, SRP)
- Overovanie digitálnych podpisov spustiteľných súborov
- Sandboxovanie príloh a neznámych aplikácií
- Používanie princípu least privilege

Detekcia:

- EDR analýza neobvyklých procesov
- DNS monitoring na C2 domény

Ochrana proti Cryptoware / Ransomware

Prevencia:

- Offline zálohy a test obnovy (immutable backups)
- Behaviorálne detektory proti šifrovaniu
- Obmedzenie prístupu k zdieľaným priečinkom
- Blokovanie makier a skriptov z internetu
- Viacúrovňová autentifikácia (MFA)

Reakcia:

- Okamžité odpojenie infikovaných zariadení
- Obnova systému z bezpečných záloh

Ochrana proti Commodity Loaders

Prevencia:

- Kontrola e-mailových príloh (PDF, ZIP, ISO, MSI)
- Kontrola reputácie spustiteľných súborov
- Sandbox v e-mailových bránach
- Kontrola spúšťacích procesov

Detekcia:

- Analýza logov na opakované sťahovanie payloadov
- Monitorovanie komunikácie s cloud hostingmi

Ochrana proti Fileless Malware

Prevencia:

- Zakázanie PowerShellu, WMI a skriptovania pre bežných používateľov
- AppLocker pravidlá pre PowerShell a .NET
- Pravidelné čistenie cache a plánovača úloh
- Použitie EDR systémov s in-memory analýzou

Detekcia:

- Monitoring skriptových aktivít (Sysmon, Event ID 4104/4688)
- Detekcia anomálneho využitia pamäte alebo process injection

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Ochrana proti Rootkits a Botom

Rootkits:

- Secure Boot a TPM integritné kontroly
- Antivírus s kernel-level detekciou
- Kontrola systémových ovládačov a hashov
- Re-inštalácia OS po náleze

Boti a botnety:

- Detekcia anomálií v DNS a sieťovej komunikácii
- Ochrana proti C2 komunikácii (sinkhole, threat intel)
- Rotácia hesiel a API tokenov

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Security Awareness vo firmách

- Pravidelné školenia o phishingu a sociálnom inžinierstve
- Simulované phishingové kampane pre zamestnancov
- Politika bezpečného používania e-mailov a webu
- Dôraz na zodpovednosť každého používateľa
- Interné hlásenie podozrivých incidentov (report button)

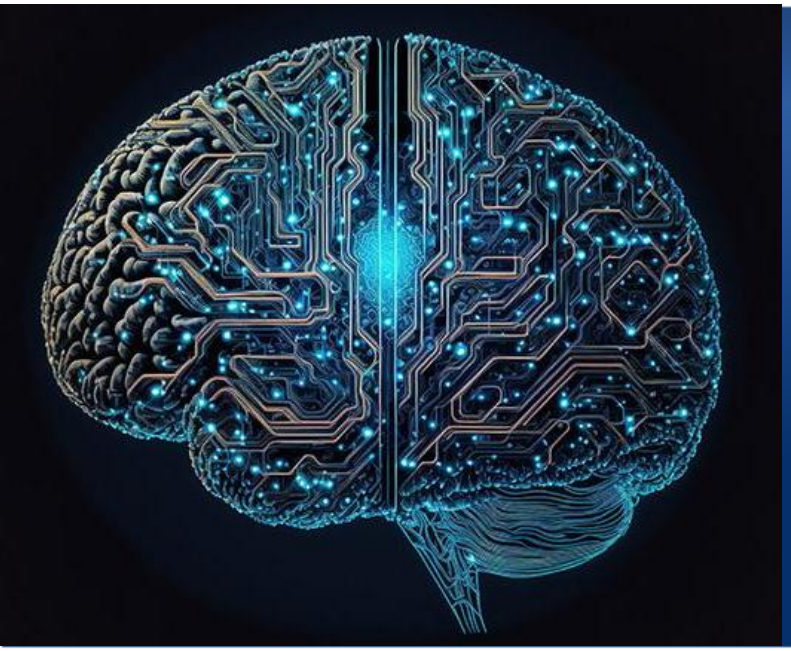
Security Awareness vo firmách

- Dvojfaktorová autentifikácia na všetkých kritických systémoch
- Silné heslá a pravidelná rotácia
- Uzamykanie pracovnej stanice pri odchode
- Opatrnosť pri prenášaní dát na USB a cloude
- Firemná kultúra bezpečnosti – 'Security First' prístup

Odstránenie malware

- Vo všeobecnosti
  - Robte si pravidelné zálohy
  - Snažte sa zabrániť aby sa malvér dostal na koncové zariadenia
  - Na úrovni siete:
    - Definovanie sieťového perimetra
    - Definovanie segmentácie
    - Používanie bezpečnostných zariadení
  - Monitorovanie
  - Pripravte sa na incident (incident manažment)

- Odpojte infikované počítače od všetkých sieťových pripojení,
- Zvážte vypnutie všetkých Core zariadení,
- Resetujte prihlasovacie údaje, ale overte si, či sa tým nezamykáte,
- Bezpečne vymažte infikované zariadenia a preinštalujte operačný system,
- Pred obnovením zo zálohy overte, či neobsahuje žiadny škodlivý softvér,
- Pripojte zariadenia k čistej sieti,
- Nainštalujte, aktualizujte a spustite antivírusový softvér,
- Znova sa pripojte k sieti a monitorujte sieťovú prevádzku.



Informácie o hrozbách (Threat Intelligence)

Zdroje informácií => Spravodajské informácie o hrozbách

- Informácie o hrozbách
  - Proces zhromažďovania, analýzy a interpretácie informácií o súčasných alebo potenciálnych hrozbách pre digitálnu bezpečnosť organizácie
  - Vybavuje organizácie vedomosťami, ktoré potrebujú na pochopenie a obranu pred kybernetickými hrozbami
- Tri základné charakteristiky
  - Relevantné
    - Prispôsobené špecifickej hrozbe organizácie
      - Príklad: Ak moja organizácia nepoužíva macOS, zraniteľnosti systému macOS pre mňa nie sú relevantné
  - Akčné
    - Musí poskytovať jasné a konkrétne informácie, ktoré môžu usmerňovať rozhodovanie a bezpečnostné opatrenia, ako je identifikácia zraniteľností alebo konfigurácia obranných opatrení
  - Kontextové
    - Poskytuje informácie o tom, kto, čo, prečo a ako predstavuje hrozbu, a pomáha organizáciám pochopiť motívy, taktiky a potenciálne dopady škodlivých aktérov.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Zdroje informácií o hrozbách a výskumu

```
Malware File - "studiox-link-standalone-v20.03.8-stable.exe"
        sha256 6a6c28f5666b12beecd56a3d1d517e409b5d6866c03f9be44ddd9efffa90f1e0
        sha1 eb019ad1c73ee69195c3fc84ebf44e95c147bef8
        md5 3a104b73bb96dfed288097e9dc0a11a8
DNS requests
        domain log.studiox.link
        domain my.studiox.link
        domain  _sips._tcp.studiox.link
        domain sip.studiox.link
Connections
        ip 198.51.100.248
        ip 203.0.113.82
```

- Množstvo zdrojov:
  - Interné a externé, verejné alebo súkromné
- Verejné
  - Spravodajské informácie z otvorených zdrojov (OSINT)
    - CVE - Slovník bežných zraniteľností a expozícií (CVE)
      - https://cve.mitre.org/cve/
      - Spravuje nezisková organizácia MITRE Corporation
      - Každý záznam CVE obsahuje
        - štandardné identifikačné číslo, stručný popis bezpečnostnej zraniteľnosti a všetky dôležité odkazy na súvisiace správy o zraniteľnostiach.
    - CVSS (Common Vulnerability Scoring System)
      - Štandardizovaný systém hodnotenia používaný na určenie závažnosti zraniteľností v kybernetickej bezpečnosti
    - MITRE ATT&CK® https://attack.mitre.org/
      - globálne dostupná vedomostná základňa o taktikách a technikách nepriateľa založená na pozorovaniach z reálneho sveta
    - Projekt MISP: https://www.misp-project.org/
- Ostatné => Platformy a nástroje pre spravodajstvo o hrozbách
  - Indikátor kompromitácie: časti forenzných údajov, ktoré identifikujú potenciálne škodlivú aktivitu v systéme alebo sieti
    - Nezvyčajná odchádzajúca sieťová prevádzka, anomálie v aktivite privilegovaných používateľských účtov, geografické nezrovnalosti, iné varovné signály prihlásenia, nárast objemu čítania databázy, veľkosti odpovedí HTML, veľký počet požiadaviek na ten istý súbor, nezhodná prevádzka portov a aplikácií, podozrivé zmeny v registri alebo systémových súboroch, anomálie požiadaviek DNS
    - Pomáha odhaliť kompromitáciu
  - Indikátor útoku: informácie o útoku

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Zdroje informácií a výskum hrozieb

- Súkromné služby zamerané na spravodajstvo o hrozbách
  - Ďalšie zdroje (Cisco Talos, FireEye, Fortinet FortiguardLabs…)
- Niekoľko bezpečnostných organizácií a fór zameraných na bezpečnosť
  - SANS (SysAdmin, Audit, Network Security) www.sans.org, CERT (Computer Emergency Response Team): www.cert.org, MITRE www.mitre.org, FIST (Forum of Incident Response Teams): https://www.first.org/, ISC2 (International Information Systems Security Certification Consorcium): https://www.isc2.org
- Správy o kybernetickej bezpečnosti
  - Napríklad Cisco
- Bezpečnostné blogy a podcasty

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Ďakujem za pozornosť

Malvér a základné stratégie prevencie a detekcie

Ochrana koncových zariadení (Blok IV)

Kurz: Špecialista kybernetickej bezečnosti vo verejnej správe

Dalibor Kafka (Pavel Segeč)

KC KYB UNIZA, https://kc.uniza.sk

Dalibor.Kafka@fri.uniza.sk
(Pavel.Segec@fri.uniza.sk)