Riziká na sieti

- Marek Papcun
- Emil Suchánek
- Bohuš Zeman
- Jakub Vengrín

Žiaci SPŠE Hálova 16, Bratislava | V rámci projektu “IB awareness”

Prehliadanie webu

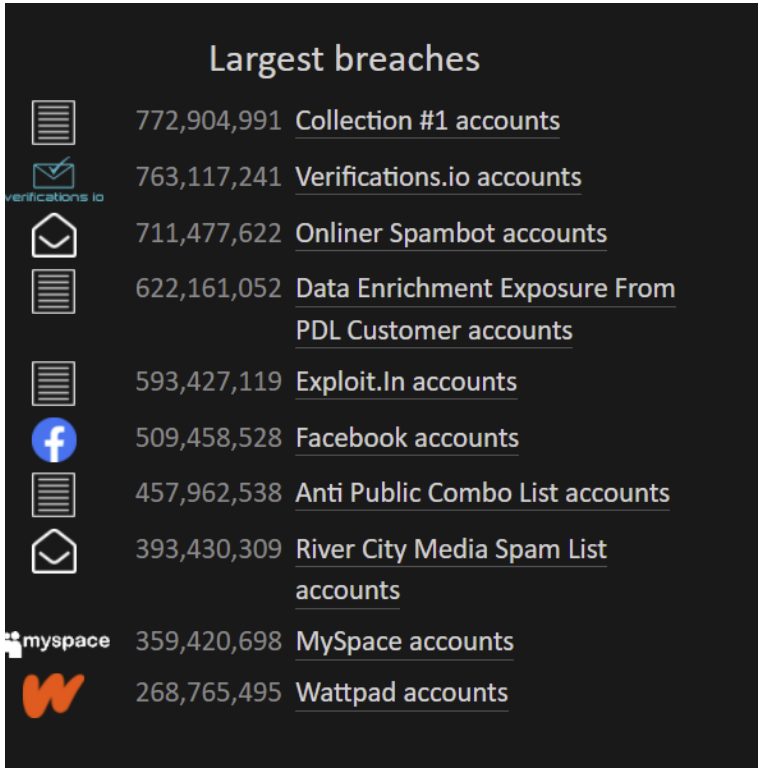
- “Surfovanie”
- “WWW” – World Wide Web
- Text, obrázky, videá, virtuálna realita
- (Inter)aktívny obsah
- Programy/kód, ktorý beží na vašom zariadení

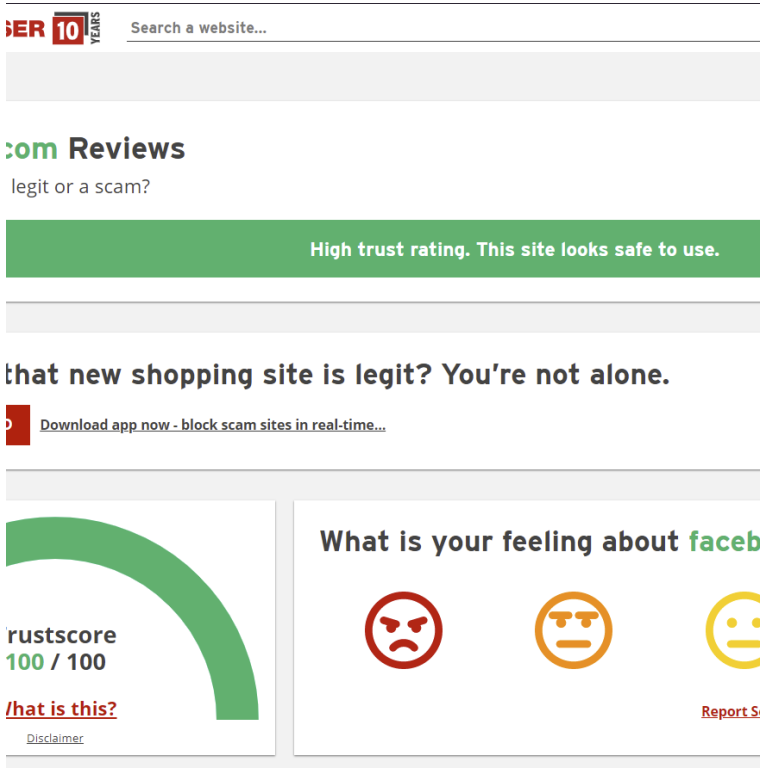
Riziká

- Bezpečnosť
  - Útoky s cielom ukradnúť/zneužiť peniaze, heslá, zariadenie alebo identitu
- Súkromie
  - Sledovanie aktivity
  - Cielené reklamy
- Ovplyvňovanie
  - Šírenie falošných správ
  - Hoaxy

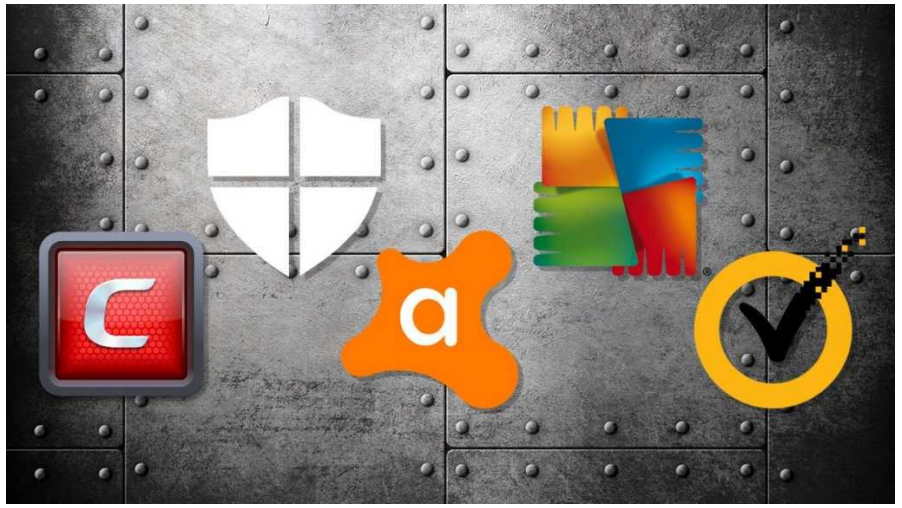
Príklady

- Have i been pwned?
  - https://haveibeenpwned.com/PwnedWebsites
- Scam adviser
  - https://www.scamadviser.com
- Bezpečnosť hesla
  - https://hesla.csirt.upjs.sk

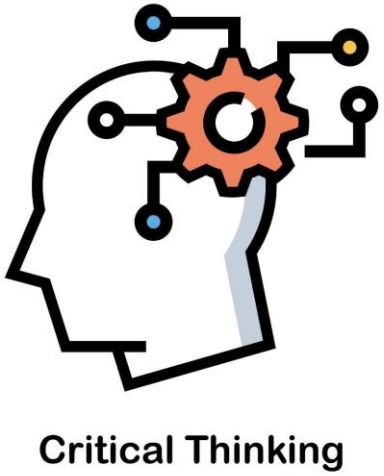




Obrana

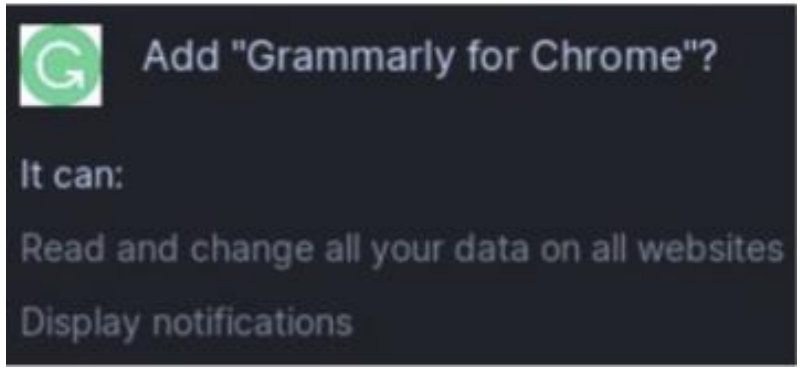


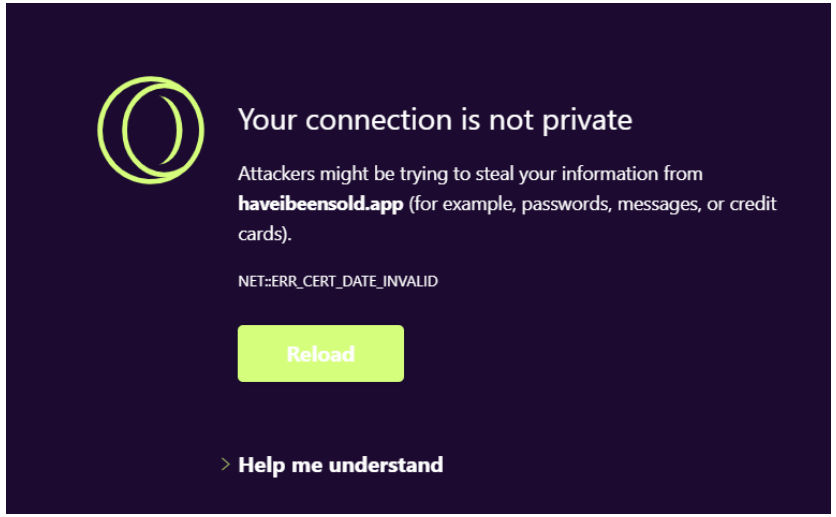
- Technická
  - Nastavenie prehliadača
  - Nástroje
  - Správca hesiel
  - Antivírus
  - Čiastočne účinná
- Používateľská
  - Opatrnosť
  - Kritické myslenie
  - Dodržiavanie pravidiel



Nastavenia prehliadaču

- Čo blokovať?
  - Sledovanie a reklamy – adblock,cookies
- Povolenia
  - Zakázať editovanie súborov v PC
- Doplnky:
- Vhodné doplnky – HTTPS Everywhere, Adblock, Privacy badger
- Nevhodné doplnky – Nedôveryhodný alebo neznámy autor, málo používaný, vysoké oprávnenia
- Pozor na súkromie
  - Produktivita vs. súkromie





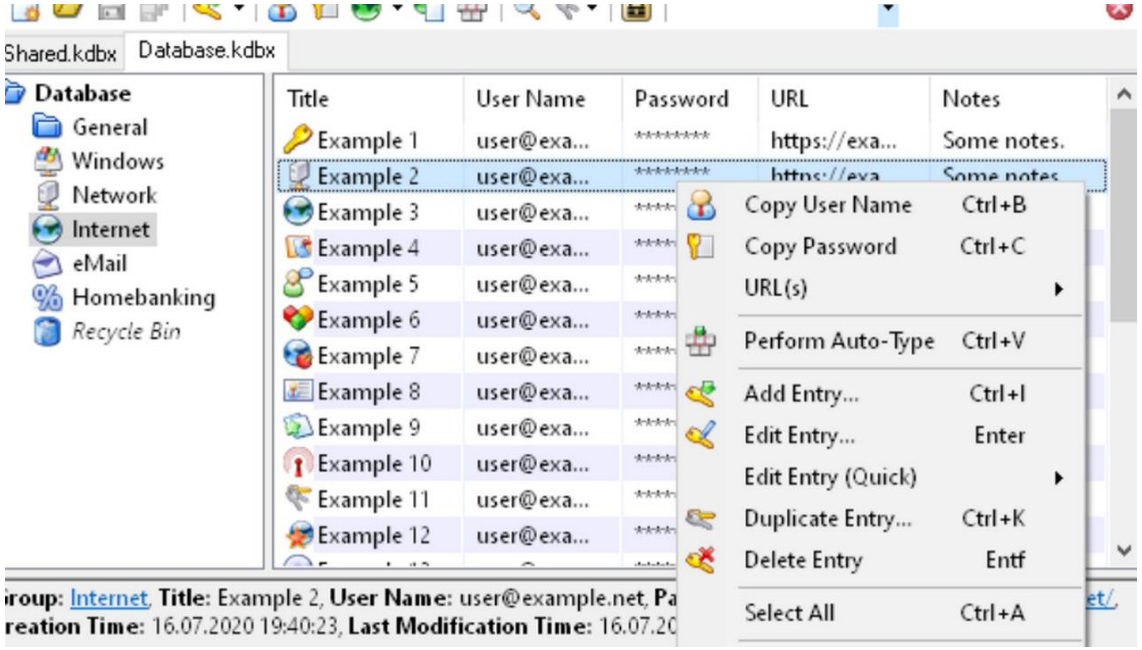
Nástroje

- Správca hesiel
  - 1Password – Platená
  - KeePass – Zadarmo
- 2FA – druhý faktor overenia
  - Niečo som (biometria)
  - Niečo viem (heslo)
  - Niečo mám (zariadenie)

- Antivírus
  - Windows Defender
  - Avast
  - Atď...

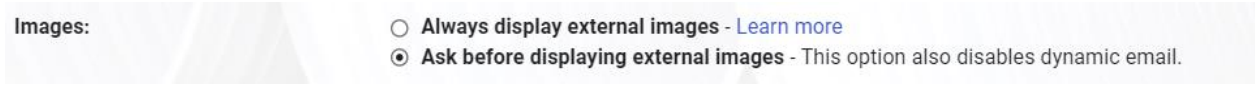
Windows Defender

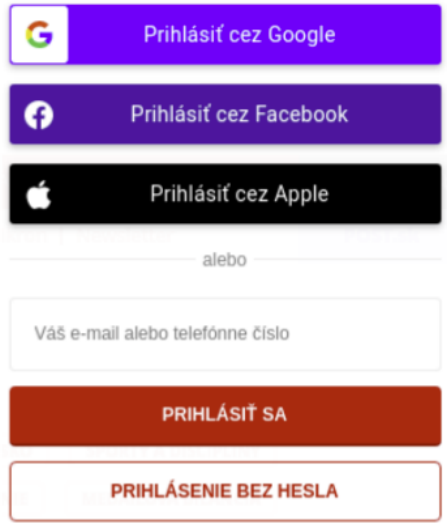
1Password

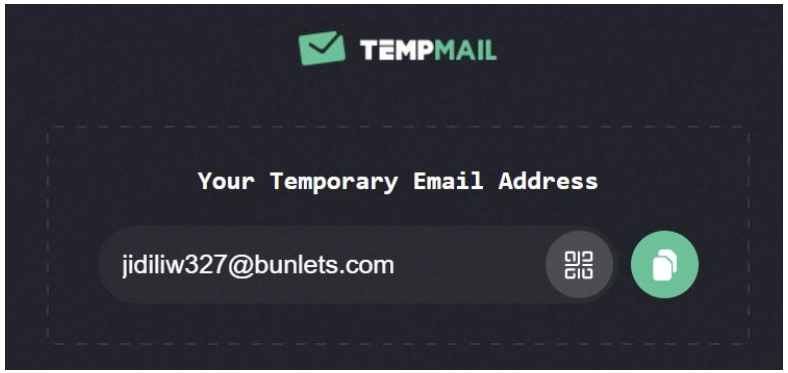


Emaily

- Registrácie:
- Prihlásenie cez Facebook/Google
  - Závislosť na danej službe
- Meno (email) + heslo
  - Potrebný mail – spam, potrebné heslo
- Bez mailu to nejde?
  - Temp mail – Docasný mail
  - https://temp-mail.org/en/
- Email aliasy
  - meno@email.org
  - Meno+alias@email.org
- Sledovanie otvorenia emailu
  - Vloženie 1px obrázku







Odkazy, súbory

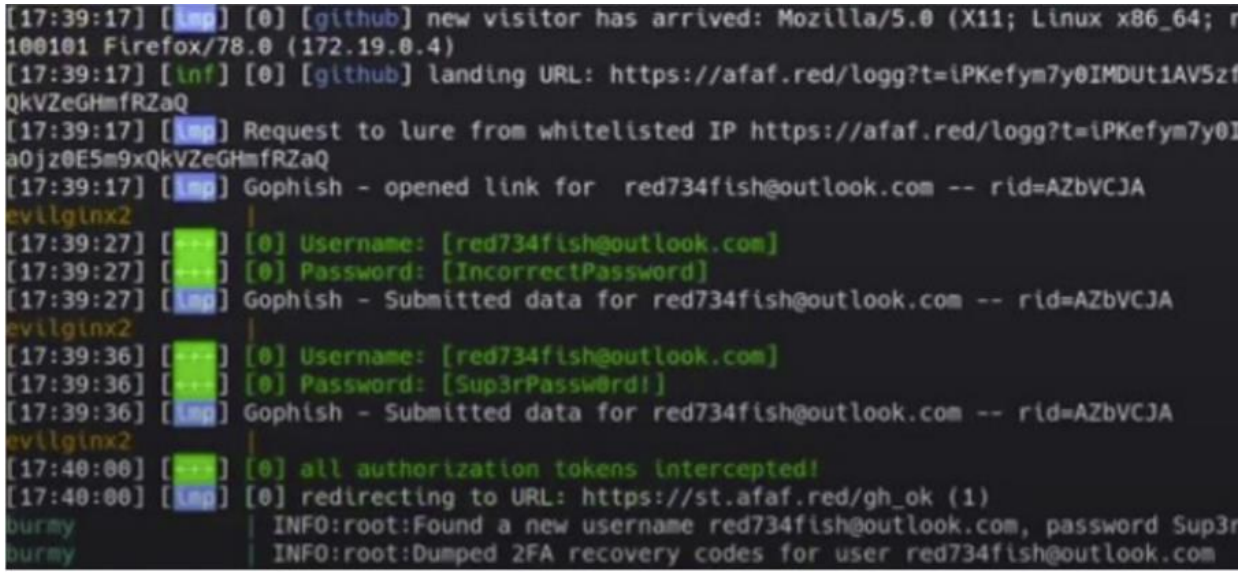
- Nižšia kontrola ako pri mailoch
- Väčšia dôvera používatelov
- Klikanie na liky bez kontroly
- Automatické načítanie/sťahovanie

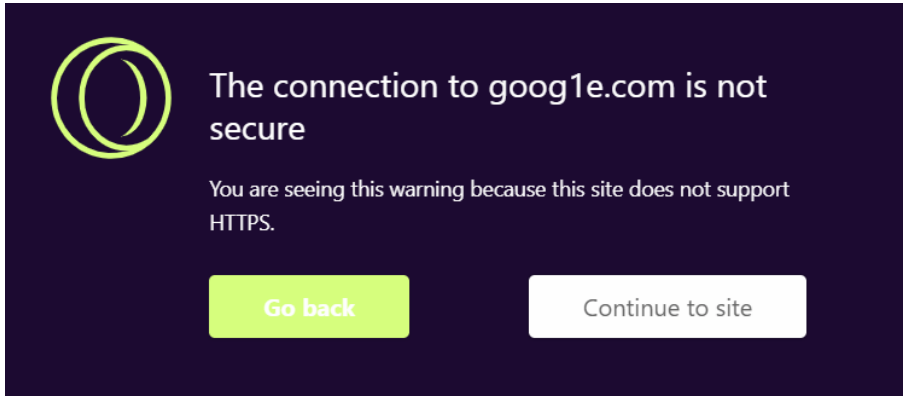
- Skracovače URL
- Tinyurl, bit.ly, goo.gl, ...
- Zakrývajú skutočnú stránku
- Neklikať, prípadne si pozrieť náhlad
  - “+” na koniec linku

Možnosti útoku

- Podvodnícka stránka - Phishing
  - Krádež prihlasovacích údajov
  - Bankových údajov
  - Ručné vypĺňanie ale aj copy-paste

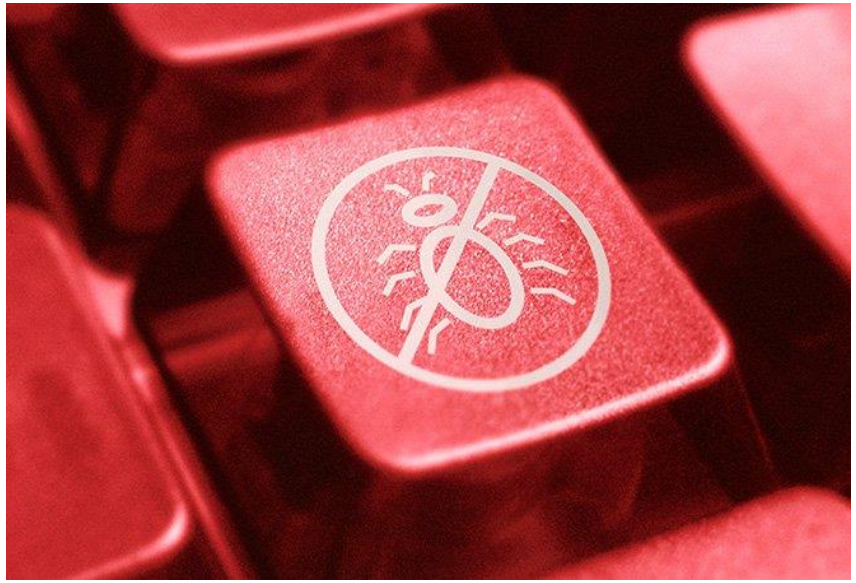
- Podobné stránky – Typosquatting
  - Podobné URL
  - Goog1e.com
  - Gmail.sk
  - Skwikipedia.org

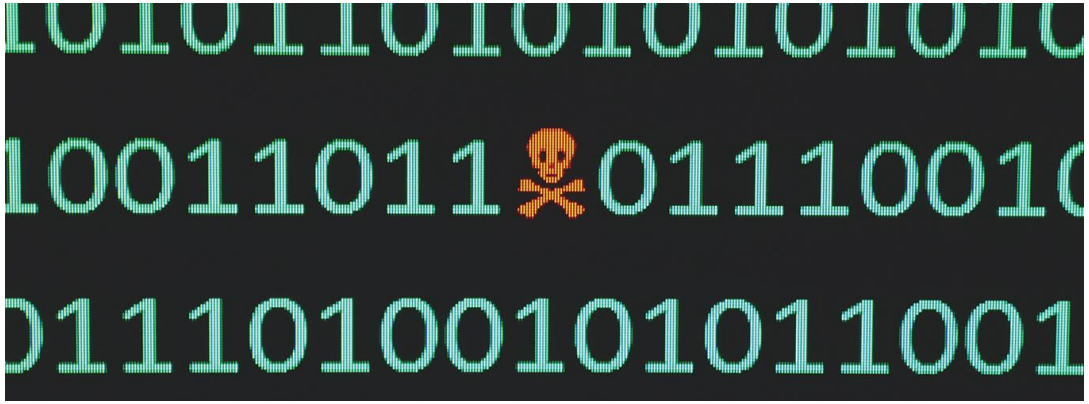




Malvér

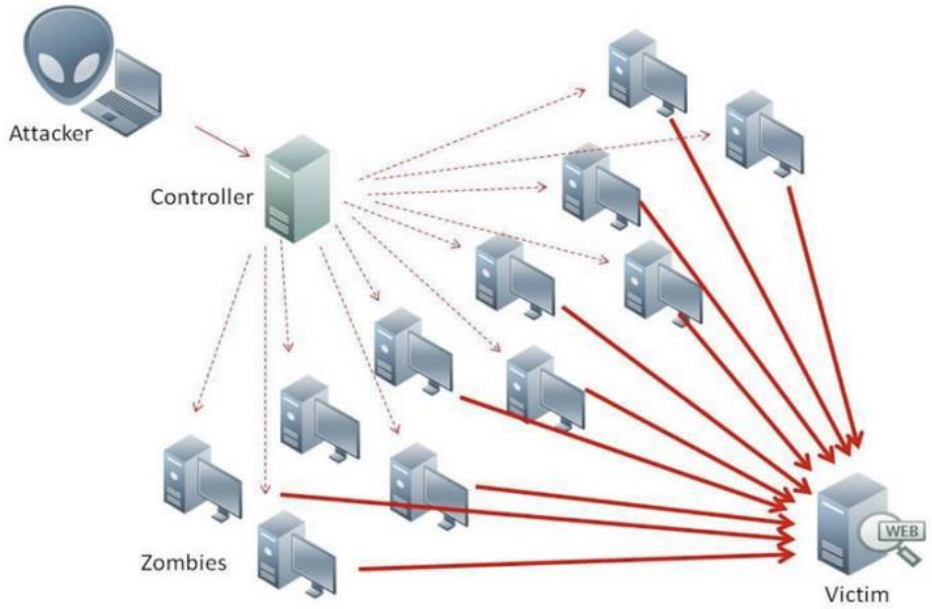
- Zlomyselný kód, program
- Poškodí alebo zablokuje a ukradne informácie z počítaču
- Najčastejšie infikovanie malwarom je práve cez internet
  - Sťahovanie pochybných súborov
  - Navštevovanie neoficiálnych/neoverených stránok
  - Atď...

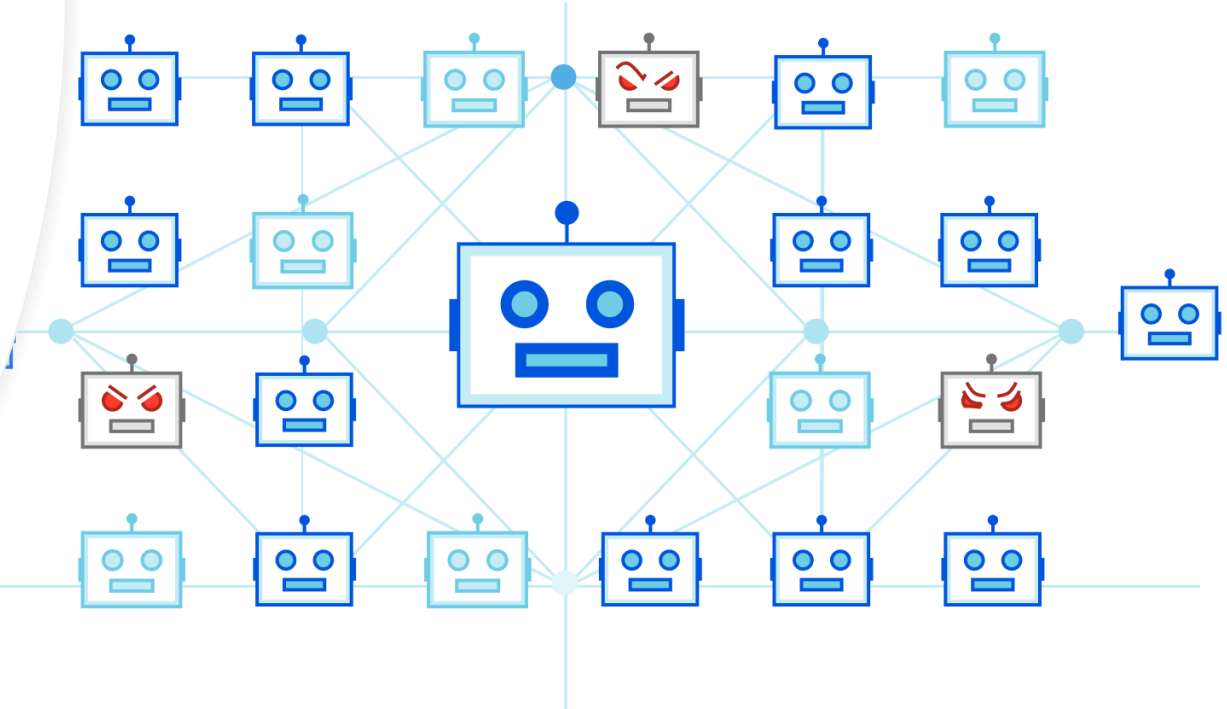




Bot/Botnet

- Vykonávanie útoku pomocou viacerých počítačov naraz
- „Botnet“ – sieť nakazených počítačov ktoré ďalej vysielajú útok
- Je náročné vystopovať páchatela kedže počítače z ktorých útok vychádza sú často na inom mieste ako páchateľ
- Všetky počítače sú nakazené jednotným vírusom





Advér

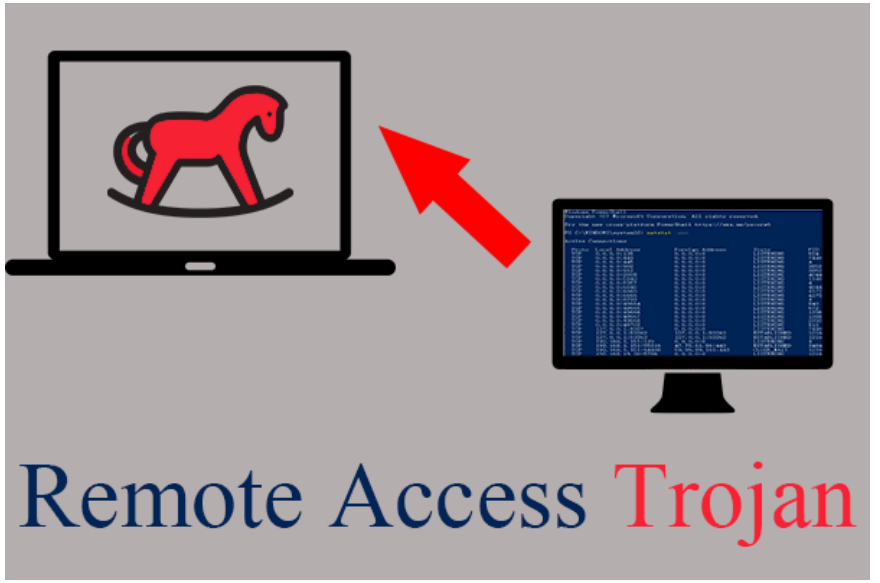
- Kód/program, ktorý automaticky zobrazuje alebo sťahuje reklamy
- Väčšina advér programov existujú na podporu tvorcu aby pokryl náklady
- Existujú ale aj škodlivé programy slúžiace výhradne na zaplnenie počítaču reklamou
- Útočník môže tieto reklamy využiť aj na speňaženie sám pre seba

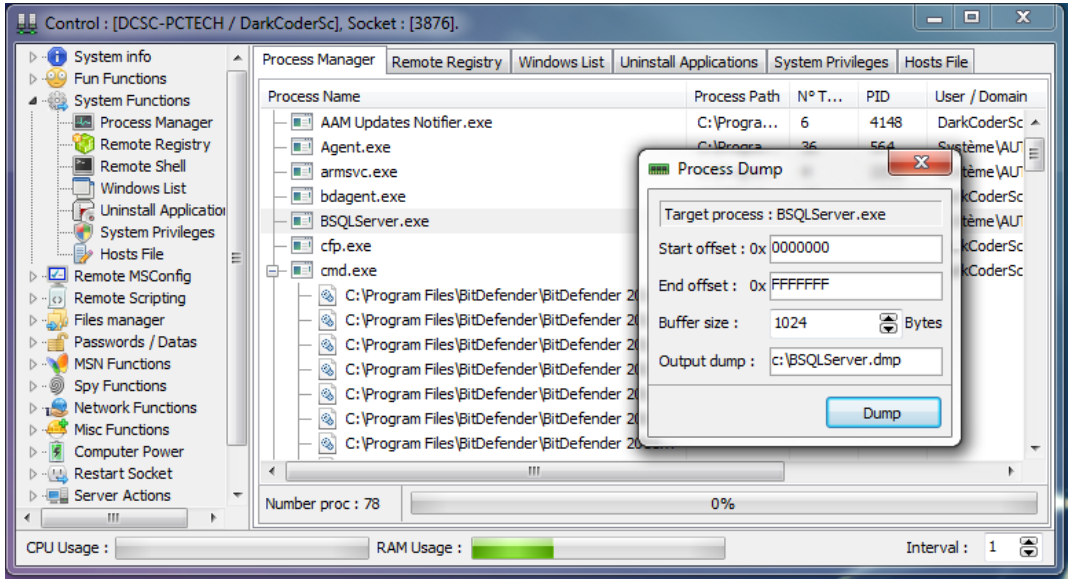
Ransomware

- Škodlivý softvér, ktorý zablokuje alebo zašifruje počítačový systém
- Od obete sa následovne požaduje vyplatenie výkupného
- Jednoduchý ransomware zablokuje iba systém a je pomerne jednoduché ho odblokovať aj bez vyplatenia výkupného
- Niektoré druhy ransomwaru ale aj po zaplatení výkupného súbory/systém neodšifrujú, môže sa stať že príde aj ku kompletnému zmazaniu všetkých súborov

RAT – Vzdialené ovládanie PC

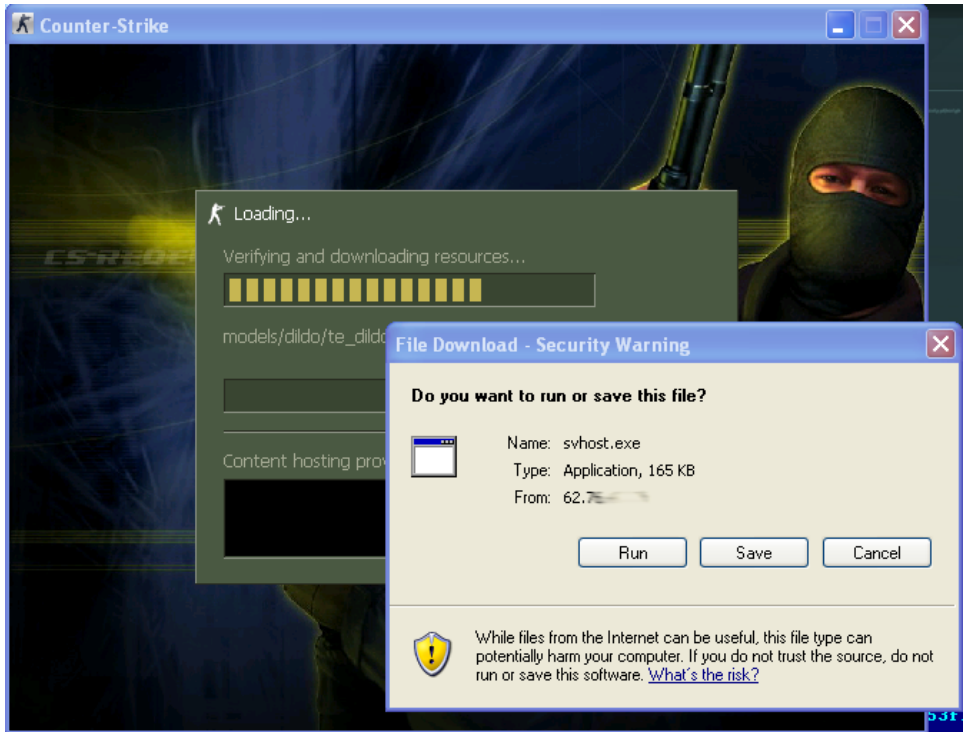
- Útočník dostane plný prístup ku kontrole PC
- Môže prehliadať vaše súbory zo svojho PC
- Dokonca má prístup k ovládaní myši a klávesnice
- Útok je smerovaný väčšinou na cenné údaje ako bankovníctvo, prihlasovacie údaje alebo dokonca aj identita
- V niektorých prípadoch útočník doslova pred očami obete preberie kontrolu nad PC a zabráni obeti prístup (Softvér ukradne)





Trojský kôň

- Škodlivý kód/program, ktorý sa tvári ako užitočný program
- Pochádza z podvodných/pirátskych stránok
- Jeho útoky bývajú rôzne:
  - Kradnutie dát
  - Šifrovanie súborov
  - Zahlcovanie disku súbormi výhodnými pre útočníka
- Jedná sa o najnebezpečnejší druh malvéru



Quiz na záver

1. Čo znamená skratka „WWW“?
2. Vymenujte aspoň 2 riziká prehliadania na internete.
3. Ktorá časť obrany je dôležitejšia? Technická alebo používateľská?
4. Vysvetlite čo to je druhý faktor overenia.
5. Ktorú službu je dobré využiť pri registrácií na krátke používanie?
6. Vysvetlite rozdiel medzi phishing a typosquatting útokom.
7. Čo znamená „Botnet“?
8. Čím je typický ransomware?
9. Prečo sú odkazy otvárané na telefóne nebezpečnejšie ako na PC?
10. Ako sa volá najnebezpečnejší druh malvéru?