



# 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 cieľom ukradnúť/zneužiť peniaze, heslá, zariadenie alebo identitu
- Súkromie
  - Sledovanie aktivity
  - Cílené 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>

| Largest breaches                                                                    |                                                                                 |
|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
|    | 772,904,991 <a href="#">Collection #1 accounts</a>                              |
|    | 763,117,241 <a href="#">Verifications.io accounts</a>                           |
|    | 711,477,622 <a href="#">Onliner Spambot accounts</a>                            |
|    | 622,161,052 <a href="#">Data Enrichment Exposure From PDL Customer accounts</a> |
|    | 593,427,119 <a href="#">Exploit.In accounts</a>                                 |
|    | 509,458,528 <a href="#">Facebook accounts</a>                                   |
|  | 457,962,538 <a href="#">Anti Public Combo List accounts</a>                     |
|  | 393,430,309 <a href="#">River City Media Spam List accounts</a>                 |
|  | 359,420,698 <a href="#">MySpace accounts</a>                                    |
|  | 268,765,495 <a href="#">Wattpad accounts</a>                                    |



## Ako bezpečné je Vaše heslo?

123456

⚠ Toto je jedno z top 10 najpoužívanějších hesiel.

Počítač ho uhádne za

**menej než sekundu**



### Scamadviser.com Reviews

legit or a scam?

High trust rating. This site looks safe to use.

Is that new shopping site legit? You're not alone.

Download app now - block scam sites in real-time...



rustscore  
100 / 100

[What is this?](#)

[Disclaimer](#)

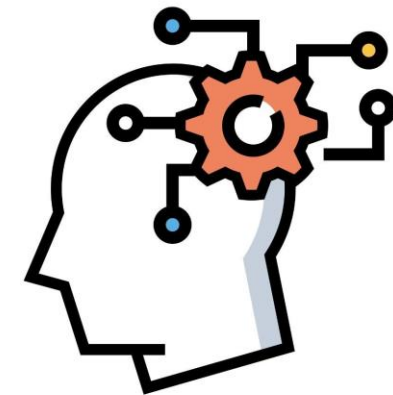
### What is your feeling about facebook



[Report Scam](#)

# Obrana

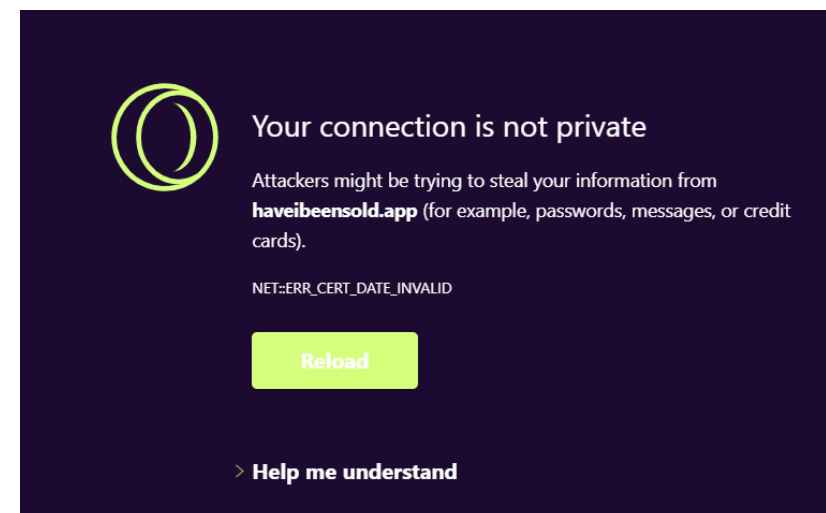
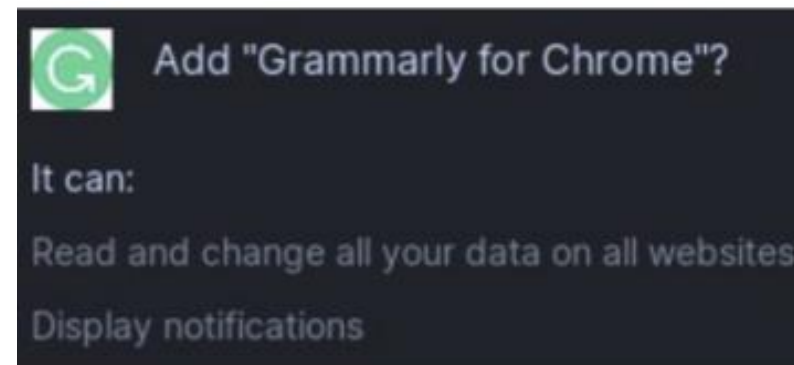
- Technická
  - Nastavenie prehliadača
  - Nástroje
  - Správca hesiel
  - Antivírus
  - Čiastočne účinná
- Používateľská
  - Opatrnosť
  - Kritické myslenie
  - Dodržiavanie pravidiel



Critical Thinking

# 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



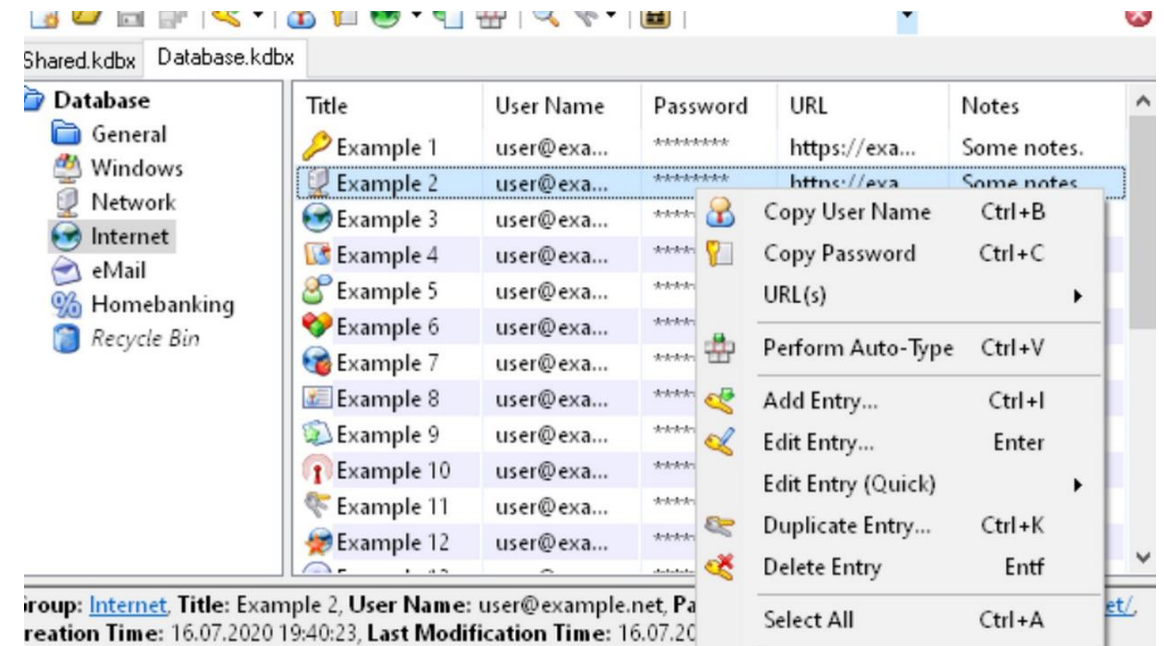


# Nástroje

- Správca hesiel
  - 1Password – Platená
  - KeePass – Zadarmo
- 2FA – druhý faktor overenia
  - Niečo som (biometria)
  - Niečo viem (heslo)
  - Niečo mám (zariadenie)
- Antivírus
  - Windows Defender
  - Avast
  - Atd'...



1Password

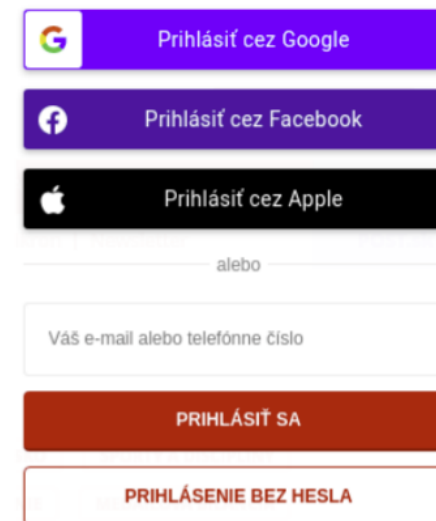


# Emaily

- 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

Images:

- ☐ Always display external images - [Learn more](#)
- ☒ Ask before displaying external images - This option also disables dynamic email.



Buttons for login:

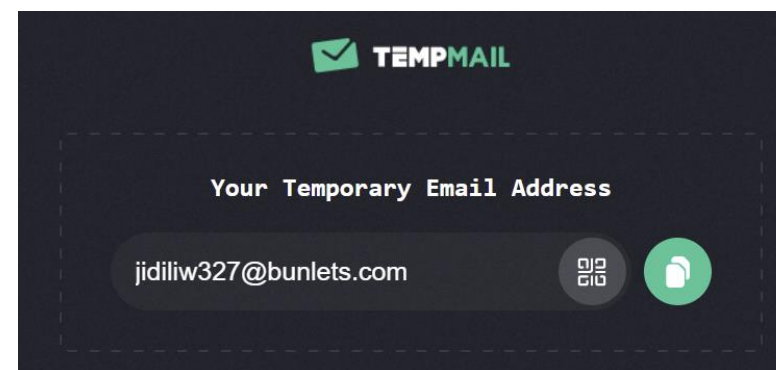
- Prihlásiť cez Google
- Prihlásiť cez Facebook
- Prihlásiť cez Apple

alebo

Váš e-mail alebo telefónne číslo

PRIHLÁSIŤ SA

PRIHLÁSENIE BEZ HESLA





# Odkazy, súbory

---

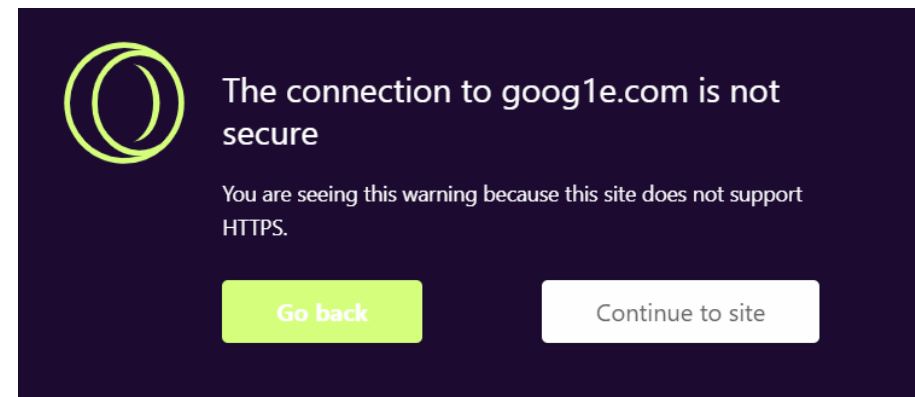
- Nižšia kontrola ako pri mailoch
  - Väčšia dôvera používateľov
  - Klikanie na liky bez kontroly
  - Automatické načítanie/sťahovanie
- 
- Skracovače URL
  - Tinyurl, bit.ly, goo.gl, ...
  - Zakrývajú skutočnú stránku
  - Neklikať, prípadne si pozrieť náhľad
    - “+” na koniec linku



# Možnosti útoku

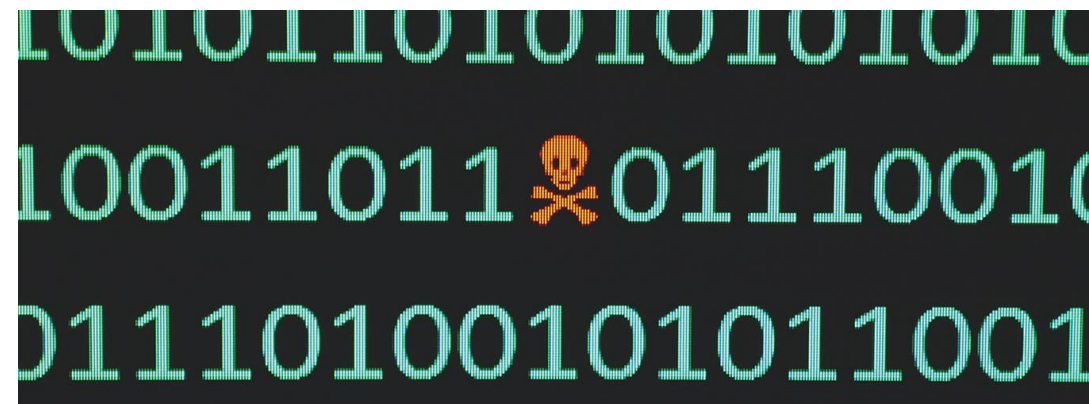
- Podvodnícka stránka - Phishing
  - Krádež prihlasovacích údajov
  - Bankových údajov
  - Ručné vyplňanie ale aj copy-paste
- Podobné stránky – Typosquatting
  - Podobné URL
  - Goog1e.com
  - Gmail.sk
  - Skwikipedia.org

```
[17:39:17] [Imp] [0] [github] new visitor has arrived: Mozilla/5.0 (X11; Linux x86_64; r
100101 Firefox/78.0 (172.19.0.4)
[17:39:17] [Inf] [0] [github] landing URL: https://afaf.red/logg?t=iPKefym7y0IMDUt1AV5zf
QkVZeGHmFRZaQ
[17:39:17] [Imp] Request to lure from whitelisted IP https://afaf.red/logg?t=iPKefym7y0I
a0Jz0E5m9xQkVZeGHmFRZaQ
[17:39:17] [Imp] Gophish - opened link for red734fish@outlook.com -- rid=AZbVCJA
evilginx2
[17:39:27] [Imp] [0] Username: [red734fish@outlook.com]
[17:39:27] [Imp] [0] Password: [IncorrectPassword]
[17:39:27] [Imp] Gophish - Submitted data for red734fish@outlook.com -- rid=AZbVCJA
evilginx2
[17:39:36] [Imp] [0] Username: [red734fish@outlook.com]
[17:39:36] [Imp] [0] Password: [Sup3rPassw0rd!]
[17:39:36] [Imp] Gophish - Submitted data for red734fish@outlook.com -- rid=AZbVCJA
evilginx2
[17:40:00] [Imp] [0] all authorization tokens intercepted!
[17:40:00] [Imp] [0] redirecting to URL: https://st.afaf.red/gh_ok (1)
buray INFO:root:Found a new username red734fish@outlook.com, password Sup3r
buray INFO:root:Dumped 2FA recovery codes for user red734fish@outlook.com
```



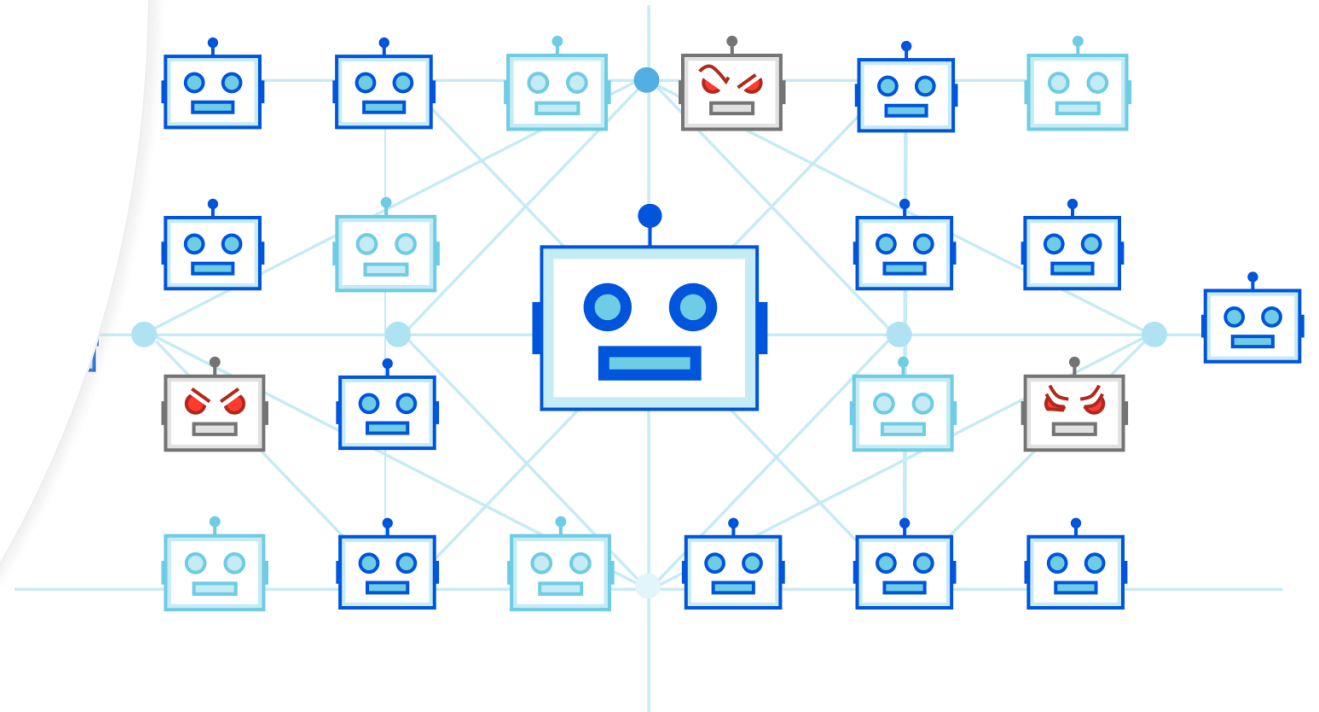
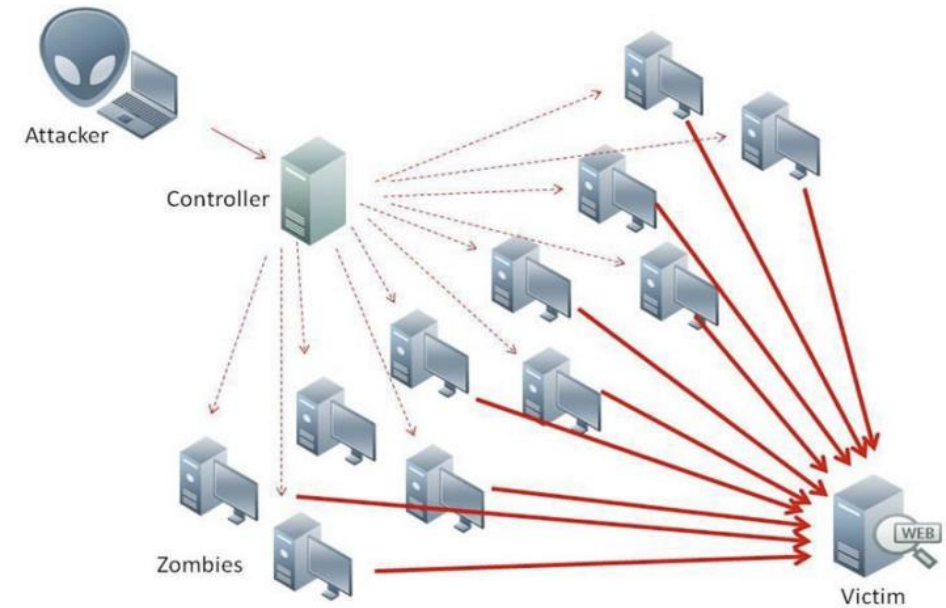
# Malvér

- 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
  - Atd'...



# Bot/Botnet

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





# Advér

- Kód/program, ktorý automaticky zobrazuje alebo sťahuje reklamy
- Väčšina advér programov existujú na podporu tvorca 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



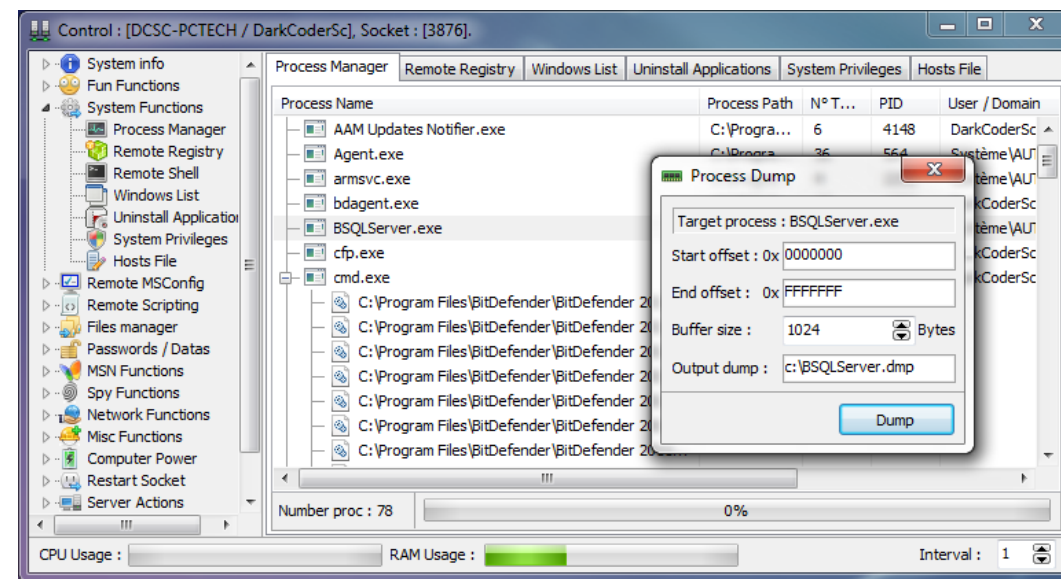
# Ransomware

- 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 zaplacení výkupného súborý/systém neodšifrujú, môže sa stať že príde aj ku kompletnému zmazaniu všetkých súborov



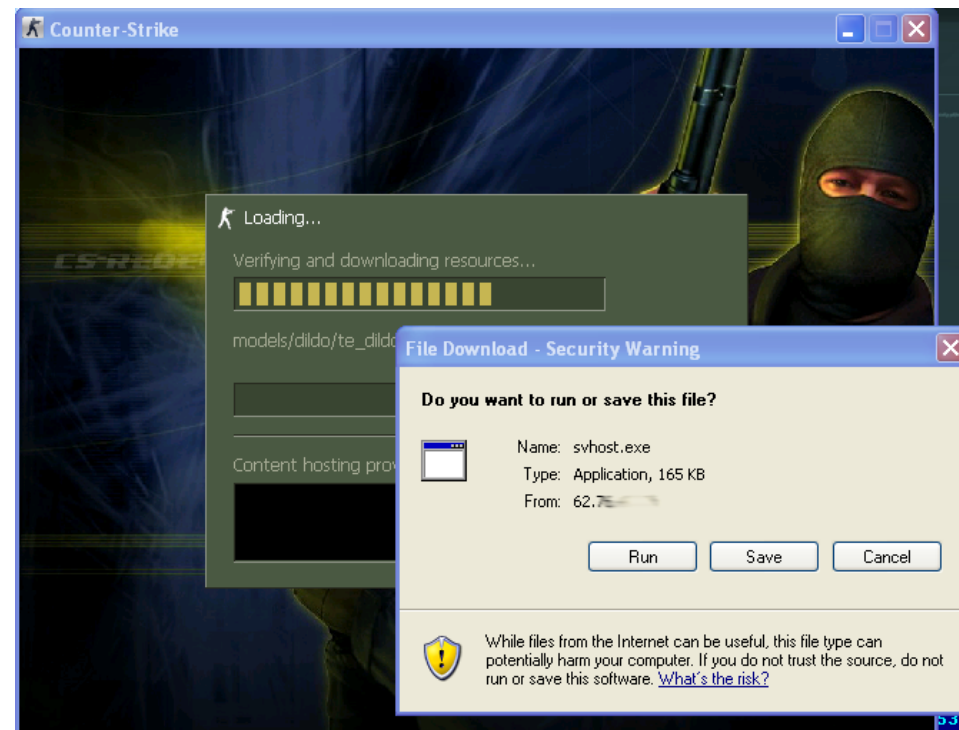
# RAT – Vzdialené ovládanie PC

- Útočník dostane plný prístup ku kontrole PC
- Môže prehliadať vaše súbory zo svojho PC
- Dokonca má prístup k ovládaniu 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 registrácii 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?