**Slovenská technická univerzita v Bratislave**

Fakulta informatiky a informačných technológií

Ilkovičova 3, 842 19 Bratislava 4

Princípy informačnej bezpečnosti

Špecifikácia projektu

Peter Plevko

2020/2021

Téma projektu

# Škodlivý kód, jeho formy a identifikácia (Windows, Android)

Ako už z názvu vyplýva v mojej téme sa budem zaoberať škodlivým kódom alebo po anglicky malicious software. V tejto špecifikácii by som chcel bližšie informovať o čom budem vlastne písať a napísať aj nejaký ten harmonogram ako plánujem toto zadanie počas semestra vypracovávať. V zadaní plánujem bližšie rozviesť čo je to ten malware, kedy vznikol na čo sa používa a aké sú jeho typy, tieto typy aj bližšie rozvediem spomeniem čo je to trojský kôň ďalej čo je to internetový červ a pod. Mojou úlohou je samozrejme aj naprogramovať jednoduchý škodlivý kód toto plánujem vykonať v programovacom jazyku python 3.8.0 a môj škodlivý softvér bude keylogger čo je vlastne program na zistenie hesla. Toto heslo zisťuje pomocou toho že zaznamenáva stlačene klávesy a následne z nich vytvorí heslo. Tento malware sa používa na nedovolený prístup do počítačov alebo hocikde kde sa používa heslo. Ďalej pomocou antivírusov skúsim nájsť tento môj malware v počítací. Porovnám 10 najlepších bezplatných antivírusov a zistím aké majú výhody nevýhody ktorý je najlepší a pripadne ci sa oplatí si antivírus zaplatiť alebo stačí mat aj takýto antivírus ktorý je voľne dostupný. Pozriem sa aj na históriu vírusov to znamená kedy vznikol prvý vírus a za akým účelom samozrejme sa pozriem aj nato aká veľká vzdialenosť sa v tejto disciplíne prekonala, ako ďaleko sme sa posunuli od prvého vírusu až k tým súčasným. Pozriem sa aj na dobu súčasnú na najväčšie problém ktoré vírusy spôsobili a kto za týmito činmi stal. Pozriem sa aj na históriu antivírusov ktorý bol prvý ako ďaleko sme sa posunuli a odpoviem aj na otázku ci antivírusové firmy nevytvárajú vírusy za účelom svojho obohacovania sa. Odpoviem aj na otázku aký je rozdiel medzi Bugom a vírusom pretože obidve spôsobujú problém a padnutia systému.

# 1 Progres report

V prvom progres reporte zanalyzujem aké sú typy vírusov na čo sa používajú a aké sú nebezpečne. Popíšem aj históriu vírusov kedy vznikol prvý vírus za akým účelom a ako sme sa zato dobu posunuli vpred aj čo sa týka vytvárania vírusou aj obrany proti nim. Samozrejme pozriem sa aj nato ako sa proti nim brániť a zanalyzujem najlepšie voľne dostupne antivírusové programy a ich výhody a nevýhody.

# 2 Progres report

Naprogramujem veľmi jednoduchý malware v pythone key logger vytvorím aj samoreplikujúci sa vírus takzvaný creeper avšak iba jednoduchú verziu. Naštrukturujem word urobím obsah pomaly už dokončujem zadanie.

# Ciele projektu

Nadobudnúť ucelene vedomosti v oblasti počítačových vírusov a naprogramovať jednoduchý malware. Popísať typy a históriu malware ako aj antivírusových systémov. Zodpovedať otázku ktorý voľne dostupný antivírusový program je najlepší.

## Zoznam základných použitých prameňov

1. GRIMES, Roger A., 2020, 9 types of malware and how to recognize them. *CSO Online* [online]. 17 November 2020. [Accessed 27 February 2021]. Available from: <https://www.csoonline.com/article/2615925/security-your-quick-guide-to-malware-types.html>
2. Malware - Wikipedia, [no date]. [online], [Accessed 27 February 2021]. Available from: <https://en.wikipedia.org/wiki/Malware>
3. Best Free Antivirus in 2021, [no date]. *Best Free Antivirus Software 2021* [online], [Accessed 27 February 2021]. Available from: <https://www.antivirusguide.com/free-antivirus/?lp=default&utm_source=google>
4. Analýza existujúcich typov škodlivého kódu na vybranej platforme. Literatúra: Michael Sikorski and Andrew Honig. Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software. No Starch Press, San Francisco, CA, USA, 1st edition, 2012.
5. 11 real and famous cases of malware attacks, [no date]. *Gatefy* [online], [Accessed 27 February 2021]. Available from: https://gatefy.com/blog/real-and-famous-cases-malware-attacks/