Univerzita Mateja Bela v Banskej Bystrici

Fakulta prírodných vied

Martin Marič

Počítačová kriminalita

Úvod k informatike

Katedra informatiky

Banská Bystrica, 05.10.2015

Obsah

ZOZNAM OBRÁZKOV, TABULIEK A GRAFOV

REGISTER POJMOV

Úvod

V minulom storočí si ľudia prestavovali pod pojmom „kriminalita“ trestné právo a trestnú činnosť páchanú fyzicky alebo psychicky. S rozvojom informačných technológií sa objavujú nie len pozitívne faktory, ako bleskové spracovanie dát, urýchlenie činností a ľudských aktivít, ale objavujú sa aj negatívne faktory, ako neoprávnené získavanie financií, zneužívanie osobných údajov vo svoj prospech a zámerné napádanie počítačov „tretími stranami“. Tak vznikol špecifický typ kriminality nazývaný „počítačová kriminalita.“

Tento typ kriminality páchajú ľudia, ktorí sú vysoko inteligentní a technicky zdatní, preto je takmer nemožné vystopovať ich. Každá krajina má rozdielnu legislatívu, ktorá upravuje práve počítačovú kriminalitu.

Predmetom tejto práce je oboznámiť verejnosť s týmto druhom kriminality a zamerať sa na rôzne aktivity spojené s týmto druhom kriminality, ako napríklad „*hackovanie*“, „*spam*“, „*cracking*“, „*keyloggerstvo*“. Táto práca je zameraná hlavne na problematiku malvéru a jeho rôzne formy, z ktorých najznámejšie sú podrobnejšie rozpísané v jednotlivých podkapitolách. Táto práca zachytáva aj históriu počítačovej kriminality v minulom storočí, kedy sa technológie len začali vyvíjať a postupne sa dostávali do rúk širšej verejnosti.

Metodika, ktorá bola aplikovaná pri vypracovaní tejto práce sa nazýva „metóda zhromažďovania informácií“. Pre lepšiu predstavivosť jednotlivých druhov kriminality, táto práca využíva niekoľko obrázkov a tabuliek.

Túto tému práce som si vybral práve z dôvodu, že znalosť počítačovej kriminality ako celku je menej populárna a chcel som tento problém rozobrať do menších detailov a poukázať tak na rozširovanie sa a stále pribúdanie nových nebezpečenstiev spolu s vývojom nových technológii v súčasnosti. Ďalším dôvodom je môj osobný záujem o túto tému.

1. Počítačová kriminalita

Predtým, než sa pustíme do problematiky počítačovej kriminality, musíme si najprv osvojiť základné pojmy. Táto kapitola stručne charakterizuje počítačovú kriminalitu a najznámejšie druhy počítačovej kriminality.

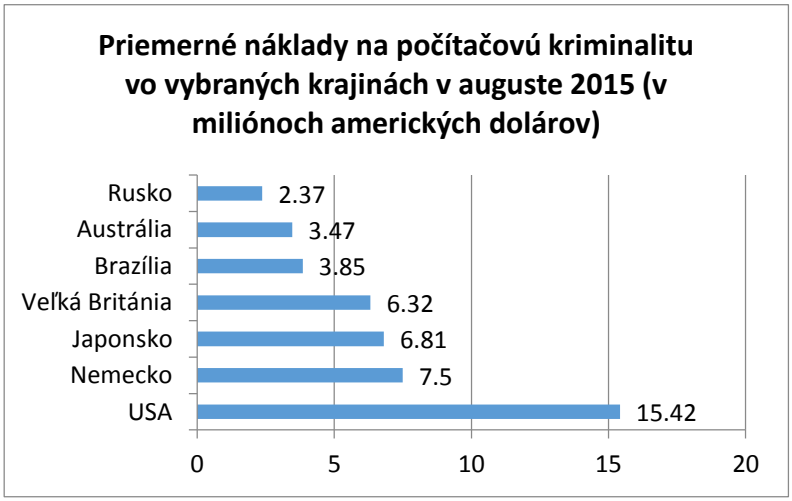
Počítačová kriminalita je pojem vo všeobecnosti používaný pre popísanie aktivity, pri ktorej sú informačné systémy a siete nástrojom, cieľom alebo miestom páchania kriminálnych činov.

Počítačovú kriminalitu, páchanú prostredníctvom komunikačných sietí a informačných a komunikačných systémov, odlišujeme od klasickej kriminality radom osobitných charakteristík a zvláštnosťami.

Najdôležitejšia skutočnosť v oblasti počítačovej kriminality je tá, že trestný čin môže byť spáchaný v priebehu niekoľkých sekúnd bez toho, aby sa páchateľ nachádzal na mieste spáchania trestného činu a poškodený tento čin zaregistroval.

Trestná činnosť páchaná pomocou počítačov alebo počítačových sietí, ale aj trestná činnosť páchaná na počítačoch, programovom vybavení a dátach, ktoré sú uložené v počítačových systémoch predstavuje obrovské straty a často presahuje hranice jedného štátu, čím sa stáva medzinárodnou trestnou činnosťou.

Každá krajina má pre oblasť počítačovej kriminality prijatú vlastnú legislatívu a rozdielne reaguje na rýchlosť rozvoja tohto problému. V Európe sa za lídra v počítačových opatreniach proti tomuto druhu kriminality považovalo Švédsko. V roku 1973 prijalo zákon, ktorý klasifikoval za trestný čin neautorizované získanie dát uložené v počítačoch.



Graf 1: Priemerné náklady na počítačovú kriminalitu [6]

Pokuty a trestné sadzby vymerané za tento druh trestných činov sú rozdielne v každej krajine. Vo Francúzsku sa neoprávnený zásah do autorizovaného spracovania údajov trestá od 1 do 3 rokov väzenia a jednorazovou pokutou vo výške 20 000 až 50 000€. V Austrálii je za opakovaný spam pokuta až do výšky 1,1 milióna austrálskych dolárov, čo je v prepočte približne 718 000€. [1]

1.1. Druhy počítačovej kriminality

Úlohou tejto podkapitoly je rozdeliť počítačovú kriminalitu na základné a najznámejšie druhy, resp. formy, s ktorými sa môže stretnúť každý, kto je pripojený k internetu.

Malvér – je všeobecné označenie škodlivého softvéru. Patrí sem viacero druhov škodlivého softvéru, ako napríklad: počítačový vírus, internetový červ, trójsky kôň, ale aj „*hoax*[1]*“* alebo „*spyware*[2]*“*. Malvér je rozsiahly pojem, preto mu bude venovaná osobitná kapitola v tejto práci.

Spam – je nevyžiadaná a hromadne rozosielaná správa prakticky rovnakého obsahu. Ide o zneužívanie elektronickej komunikácie, najmä e-mailu. Zväčša je používaný ako reklama, hoci za krátku históriu elektronickej komunikácie bol spam použitý aj z iných dôvodov. Existuje veľa rôznych médií, ktoré sú spamermi zneužívané. Môže to byť napríklad spomínaný e-mail, instantné zasielanie správ (napríklad ICQ), skupiny *„Usenet“*,[3] krátke textové správy.

Hackerstvo – je termín odvodený od anglického slova „hack“, čo znamená „rozseknúť“. Používa sa na označenie rozseknutia programátorského problému. Predstavuje buď elegantné a jednoduché riešenie predtým neriešiteľného rébusu alebo naopak, nie veľmi elegantný a mnohokrát nepochopiteľný spôsob jeho riešenia. Pre tento druhý uvedený prípad sa v odbornej hackerskej brandži používa skôr pomenovanie „*kludge*[4]“. Voľný preklad tohto termínu znamená nájdenie nemotorného, okýpteného, ohavného, neodpovedajúceho, ale dosť dobrého riešenia. Je zaujímavé, že slovo „kludge“ vošlo aj do anglického slovníka a do

[1] Hoax je predovšetkým prostredníctvom internetu elektronicky šírená správa (najmä e-mailová), ktorá napriek svojej nezmyselnosti vyzýva na to, aby bola preposielaná ďalším používateľom systému. [8]

[2] Spyware (z angl. špehovací tovar) alebo spajvér je počítačový program, ktorý sa bez vedomia užívateľa pokúša „vyšpehovať“ citlivé dáta z počítača (napr. heslá).

[3] Usenet (User's Network) - sústava vzájomne prepojených uzlov, ktoré si medzi sebou predávali sieťové novinky. Vznikla spolu so vznikom internetu. Časom sa z nej stala virtuálna sieť, resp. služba poskytovaná v rámci iných sietí. [7]

[4] Kludge - skratka prebratá z anglických slov: clumsy, lame, ugly, dumb, but good enough

slovenčiny sa prekladá ako „čierna skrinka“ alebo „účinná improvizácia“. Vo všetkých druhoch médií sa slovo počítačový pirát nesprávne spája s pojmom „hacker“. Hackerstvo je noblesa spojená s modifikáciou programových kódov alebo s nájdením netradičných riešení. Svetoznámi hackeri nie sú nadšení, že ich aktivity sú zlučované s delikvenciou. V počítačovej praxi sa hackerstvo často spája skôr s informačnou bezpečnosťou, pretože hackeri testujú úroveň zabezpečenia a ochrany informačných systémov, a po zistení slabín to oznámia spoločnosti, ktorej patrí predmetný informačný systém, bez vykonania akýchkoľvek deštruktívnych, prípadne finančných aktivít zo strany hackera. Takýto typ hackera sa nazýva aj „etický hacker“. Tento pojem lepšie priblížil jeden z najznámejších etických hackerov Anatoly Kozlow slovami: *„V biznise je etický hacker tiež známy ako „biely klobúk“ alebo „nositeľ“ bieleho klobúka, na rozdiel od „čiernych klobúkov“, ktoré „nosia“ ľudia ako Kevin Mitnick alebo hackeri „Anonymous“. Oficiálna definícia etického hackera je v podstate IT profesionál, ktorý má nejakú špeciálnu sadu zručností a nesie nejaké nástroje, a používa tieto nástroje a zručnosti k tomu, aby prenikol do systémov spoločnosti s jej súhlasom, alebo súhlasom zákazníka. Etický hacker pomáha organizáciám interného auditu s cieľom zladiť niektoré zdroje.“* [2]

Obrázok 1: Logo skupiny hackerov "Biele klobúky"

Cracking – je anglický termín, ktorý sa prekladá ako „tvorenie trhlín alebo prasklín“. V informatickom svete však slovo cracker označuje počítačového piráta, ktorý preniká do informačných systémov s cieľom škodiť, ale súčasne mať z toho aj nejaký prospech, a to buď v podobe finančného obohatenia sa alebo získania dôverných údajov. Crackeri sa obvykle zameriavajú na veľké spoločnosti, pretože tieto sú potenciálnym zdrojom „veľkých peňazí“. Počítačový pirát (cracker) hľadá možnosť vytvorenia „praskliny“ v programovom vybavení alebo aplikácii, aby sa buď dostal k údajom alebo mohol zmeniť fungovanie samotného programu. Neobmedzuje sa iba na prelomenie ochrany počítača a preštudovanie funkčnosti programov, ale často ho zaujímajú tajné bezpečnostné

Obrázok 2: Generátor sériových čísel (keygen)

kódy. Úlohou crackera je nájdenie sériového kľúča pre registráciu softvéru, následne vytvoriť algoritmus pre generovanie sériových kľúčov pre daný softvér, ktorý sa nazýva „*keygen*[5]“. Posledným krokom je odstránenie rôznych parametrov ochrán softvéru, ako napríklad obmedzenie počtu používateľov alebo obmedzenie funkčnosti.

2. Malvér

Táto kapitola rozoberá pojem „malvér“ a vysvetľuje všetky pojmy s ním spojené. Objasňuje, čo vlastne tento pojem znamená a taktiež zachytáva jeho počiatky v 20. storočí, kde sa zaznamenal prvýkrát. Taktiež podrobne rozoberá rôzne druhy malvéru a ako sa im brániť.

Slovo malvér vzniklo ako novotvar zložením z dvoch anglických slov „malicious“ a „software“, čo v preklade znamená „zlomyseľný a zákerný softvér alebo program“ a označuje sa ním škodlivý program alebo jeho časť.

2.1. Druhy malvéru

Na svete existuje viacero druhov malvéru. Tieto jednotlivé druhy vznikali postupne, ako sa rozvíjal svet malvéru. Nie všetky škodlivé programy alebo ich časti nazývame „počítačový vírus“, i keď je tento pojem v spoločnosti veľmi rozšírený.

Táto podkapitola slúži na podrobnejšie rozpísanie najznámejších druhov malvéru.

Ide o pomenovanie pre všetky druhy škodlivého softvéru, napríklad:

- Počítačový vírus,
- Počítačový červ,
- Trójsky kôň,
- Keylogger,
- Spyware,
- Adware.

[5] Keygen – je pomenovanie zložené z dvoch anglických slov „key“ a „generator“, čo znamená generátor kľúčov.

Tabuľka 1: TOP 3 najnebezpečnejších malvérov sveta

Názov malvéru	Popis malvéru
ZEUS	Tento malvér nenesie svoje meno len pre zastrašenie. Skutočne ho môžeme porovnať so Zeusom, kráľom bohov. Zeus vo svojej podobe je tak silný malvér, že dokáže spôsobiť nepredstaviteľné škody v jeho schopnosti krádeži informácií a útoku na bankové a finančné inštitúcie po celom svete. Prvýkrát bol zaznamenaný v roku 2007, no od tej doby bol zničený. Jeho vzkriesenie zabezpečila inštalácia „*Ransomware*[6]“ hrozieb a „*phishing*[7]“ kampaní spojených s „*Dropboxom*[8]“. Zeus je hlavne využívaný ako lacná a ľahko použiteľná súprava nástrojov pre hackerov a používa sa až dodnes. [3]
Conficker	Conficker je vážny počítačový červ, ktorý napáda hlavne osobné počítače využívajúce operačný systém Windows. Prvýkrát bol identifikovaný v roku 2008, kedy bol známy pre jeho agresívne útoky voči antivírusovým aplikáciám a neskoršie infikovanie celého systému. Conficker predstavoval tretinu „TOP 10“ internetových hrozieb a stále je tomu tak. Museli byť vytvorené špecializované anti-malvérové nástroje na boj s Confickerom, ktoré ho nakoniec odstránili z infikovaných počítačov. Mnoho systémov infikovaných v minulosti bolo považovaných za stratené kvôli tomu, že ich kontrolu prevzali vzdialení útočníci.
CryptoLocker	CryptoLocker nie je zďaleka tak starý, ako ostatné známe malvérové hrozby, ktoré sú súčasťou tohto zoznamu. Avšak, je rozumné zmieniť, že CryptoLocker si získal svoju pozornosť vo veľmi krátkej dobe. CryptoLocker uzamkne infikovaný systém a neumožní jeho užívanie, len obmedzene v rámci základných funkcií. [4]

[6] Ransomware je druh malvéru, ktorý zabraňuje prístupu k počítaču, ktorý je infikovaný.

[7] Phishing (z anglických slov password fishing – doslova rybolov hesiel) je činnosť, pri ktorej sa podvodník snaží vylákať od používateľov rôzne heslá, napr. k bankovému účtu.

[8] Dropbox je webové úložisko, ktoré umožňuje užívateľom ukladať a zdieľať súbory a zložky s ostatnými užívateľmi internetu.

2.1.1. Počítačový vírus

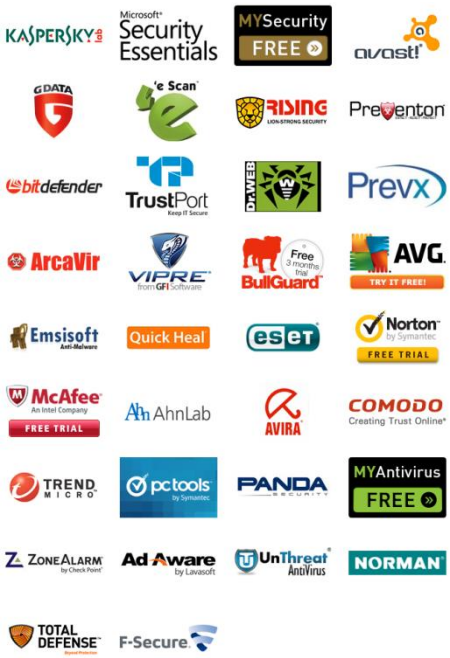
Počítačový vírus je program alebo jeho časť, ktorý sa šíri bez vedomia používateľa tak, že sa pripojí k akémukoľvek typu súboru alebo inému programu a ktorého cieľom je vlastné šírenie sa z počítača na počítač.

Dopadom a aktivitami počítačových vírusov a červov môže byť dotknutá ktorákoľvek osoba počas výmeny informácií prostredníctvom elektronickej pošty, prostredníctvom prenosu médií, sťahovaním programov, súborov, dokumentov alebo iného typu formátov z internetu.

Väčšina počítačových vírusov je ukrytá v súboroch alebo programoch s koncovkami typu: **.exe, .bin, .com, .vbs, .js** a podobnými.

V začiatkoch svojej existencie sa vírusy šírili najmä prostredníctvom diskiet. Internet umožnil používanie nových oveľa rýchlejších mechanizmov šírenia. Najmä vďaka masívnemu používaniu elektronickej pošty a rastúcemu počtu počítačov pripojených na internet.

Počítačové vírusy ako také nepredstavujú až takú hrozbu a nepodieľajú sa na krádeži informácií vo vysokej miere. Najlepšou ochranou pred infikovaním počítačovým vírusom je mať nainštalovaný jeden z voľne dostupných antivírusových programov, ktoré rozpoznajú takmer každý typ počítačového vírusu a ich častá aktualizácia vírusovej databázy umožňuje takmer 100%-tnú ochranu. [1]



Obrázok 3: Logá najznámejších antivírusových programov

2.1.2. Trójsky kôň

Pojem „trójsky kôň“ má svoj pôvod v gréckej mytológii v Homérovej Iliade, ktorá popisuje históriu Grékov, ktorí chceli obsadiť Tróju. Gréci vedeli, že mesto je veľmi dobre opevnené, aby odolalo útokom, preto sa rozhodli zostrojiť veľkého dreveného koňa a ponechať ho Trójanom ako dar na znak mieru. Trójania ocenili toto gesto a zobrali si koňa do mesta. V noci vyšli grécki vojaci zo skrýše, ktorá bola vo vnútri koňa a otvorili brány Tróje, aby pustili dnu grécku armádu, ktorá sa zmocnila mesta.

Tento pojem sa preniesol do informatiky. V skutočnosti je na internete za trójskeho koňa považovaný program alebo jeho časť, ktorý nazývame spustiteľný kód, a ktorý sa prezentuje ako bezvýznamný program, ale jeho cieľom je nakaziť počítač a otvoriť porty pre používateľov. Na rozdiel od vírusov sa trójsky kôň nekopíruje, ani nešíri, ale môže pôsobiť deštrukčne.

Väčšina trójskych koní je ukrytá v súboroch alebo programoch s koncovkami typu: **.exe, .bin, .com, .zip**, a pod.

Vo všeobecnosti sú trójske kone používané na vytvorenie a uchovávanie nepretržitého nepovoleného prístupu k počítaču pripojenému na internet.

Trójske kone zaraďujeme do 6 kategórií podľa aktivít, ktoré vykonávajú:

- Vzdialený prístup,
- Posielanie údajov,
- Deštrukčné kone,
- Typu „*Denial of Service*[9]“
- Typu „*proxy*[10]“
- Typu „*FTP*[11]“ [3]

[9] Denial of Service – slovensky "odmietnutie služby", je druh útoku na systém (server, alebo webovou službu), ktorý spočíva v tom, že útok zahltí server a to spôsobí preťaženie serveru a následne i pád systému. Občas sa nazýva aj Distributed Denial of Service – známa skratka DDoS.

[10] Proxy alebo proxy server je server počítačovej siete, ktorý umožňuje klientom nepriame pripojenie k inému serveru. Funguje ako sprostredkovateľ medzi klientom a cieľovým serverom, prekladá požiadavky klienta a oproti cieľovému serveru vystupuje ako klient.

V praxi existuje viacero trójskych koní. Medzi najznámejšie patria SubSeven, Backorifice a Netbus. No v roku 2013 sa objavil trójsky kôň, ktorý je zaradený do kategórie najnebezpečnejších malvérov súčasnosti. Tento trójsky kôň bol spomenutý na začiatku podkapitoly, no jeho funkčnosť nebola uvedená do detailov.

CryptoLocker

Tento typ trójskeho koňa sa začal šíriť v **septembri 2013**, kedy sa prvýkrát objavil. Do počítača sa môže dostať pomocou e-mailov aj od známych a priateľov. Počítač známeho človeka nemusí byť napadnutý. CryptoLocker sa dostane do emailu počas svojej cesty z jedného počítača do druhého. Preto sa nedá vypátrať žiadnym antivírusovým programom. CryptoLocker ako sa „*next-gen malware*[12]“ dostane do počítača a následne začne postupne prehliadať jednotlivé zložky s dokumentmi, pričom vyhľadáva súbory a fotografie, ktoré

Obrázok 4: Úvodné okno malvéru "CryptoLocker"

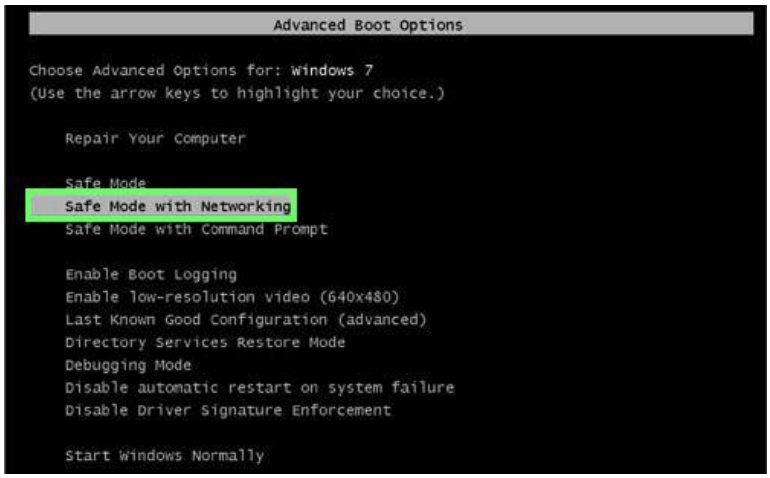
môže zašifrovať. Na obrazovke sa zobrazí okno s textom, „Ak do 100 hodín nezaplatíte 2 „*Bitcoiny*[13]“, vaše súbory sa zašifrujú.“ Do uplynutia tohto času je nutné vykonať anonymnú platbu v elektronickej mene Bitcoin. V opačnom prípade dôjde k vymazaniu dešifrovacieho kľúča a k súborom sa už nikto nedostane. Na zakúpenie Bitcoinu sú potrebné peniaze, no BitCoin je anonymný, takže platba sa nedá vystopovať. **Dôležité je, že kurz Bitcoinu sa mení a v súčasnosti sa jeho hodnota pohybuje na hranici 250 €.**

[11] FTP – z angličtiny „File Transfer Protocol je takzvaný protokol prenosu súborov určený na prenos súborov medzi počítačmi, či už na internete alebo lokálnej sieti.

[12] Malvér novej generácie

[13] Internetová mena

Odstránenie z počítača nie je ľahké ani po dvoch rokoch od jeho objavenia. Jedna z možností je pri štarte operačného systému Windows stlačiť klávesu F8, ktorá otvorí špeciálne menu na štart systému. V tomto menu je treba vybrať možnosť „Safe mode with Networking“, čo v preklade znamená „Núdzový režim s prácou v sieti“ a stlačiť ENTER. Potom je potrebné prihlásiť sa cez infikovaného používateľa a následne stiahnuť špeciálny antivírusový program, ktorý je určený priamo pre CryptoLocker a s jeho pomocou odstrániť všetky záznamy CryptoLockera. Tento postup nemusí vždy fungovať, preto sa odporúča skúsiť obnoviť systém. [5]



Obrázok 5: Spustenie Windowsu 7 cez núdzový režim

2.1.3. Keylogger

Názov tohto druhu malvéru pochádza z anglických slov „key“ a „logger“, čo v preklade znamená „snímač kláves“.

Keylogger je program, ktorý zaznamenáva stlačené klávesy a zapisuje ich do súboru, ktorý je následne odoslaný „pirátovi“.

Obrázok 6: Rozhranie pre keylogger

Ide o nelegálny nástroj, prostredníctvom ktorého sa odcudzujú údaje o prihlasovacom užívateľskom mene a hesle. Moderné typy takýchto programov ukladajú dokonca aj obraz celej obrazovky, ktorý umožňuje lepšie identifikovať, ku ktorej aplikácii uložené meno a heslo patria. Takto získané údaje sú následne zneužívané na páchanie iných druhov počítačovej kriminality.

3. Prvé vírusy 20. storočia

V predchádzajúcej kapitole bolo uvedených mnoho informácií o malvéri a jeho podobách. Všetky informácie sa týkali aktuálnych problémov s počítačovou kriminalitou. Táto kapitola je určená práve histórii a prvým vírusom, ktoré sa objavili spolu s technickým rozvojom v minulom storočí.

V roku 1962 vytvorila skupina inžinierov v laboratóriách spoločnosti Bell Telephone počítačovú hru s názvom Darwin. Hra bola zostavené okolo „sudcu“ umiestneného v pamäti počítača, ktorý definoval pravidlá a hrací poriadok medzi konkurenčnými programami vytvorenými hráčmi. Tieto programy mohli sledovať a ničiť programy konkurentov, ale aj znásobovať svoju existenciu. Hra spočívala v likvidácii programov konkurentov a kontrole bojového poľa. Táto pôvodne neofenzívna hra napísaná vedcami a inžiniermi, sa stala námetom pre počítačové vírusy, pretože ľudia pochopili, že teória automatického kopírovania a reprodukcie by mohla byť úspešne aplikovaná aj pre úplne iné ciele.

Na začiatku 70-tych rokov bol odhalený v počítačovej sieti ARPANET, predchodca internetu, počítačový vírus „CREEPER“. Bol naprogramovaný pre systém Tenex, prevádzkovaný a využívaný verejnosťou, a tento vírus bol schopný sám pristupovať do vzdialeného systému prostredníctvom modemu a nakopírovať sa tam. Na napadnutých systémoch sa objavovala hláška: „I´M THE CREEPER: CATCH ME IF YOU CAN“. O niekoľko týždňov neskôr bol neznámymi autormi vytvorený program „REAPER“, ktorý ničil tento vírus. Samotný Reaper je vírusom, šíri sa po počítačoch pripojených na sieť a zničí CREEPERA, keď ho vypátra. Doteraz nie je jasné, kto bol autorom Reapera.

Obrázok 7: Systém napadnutý vírusom "Creeper"

V roku 1974 sa objavil vírus nazývaný „RABBIT“. Cieľom tohto vírusu bolo množenie sa a prenikanie do iných počítačov. Zahlcoval systém svojimi vlastnými kópiami, čím značne spomaľoval výkon počítača. Ak Rabbit dosiahol určitú úroveň zahltenia napadnutého počítača, tak sám zastavil svoje množenie.

ZÁVER

Problém počítačovej kriminality je v súčasnosti veľmi diskutovaným a spomínaným pojmom, ktorý si zaslúži istú dávku pozornosti, či zo strany laickej verejnosti alebo trestných orgánov. V mojej práci som sa snažil poukázať na najdôležitejšie prejavy kriminality páchanej počítačmi, bez ktorých sa tento typ kriminality nezaobíde.

Prvú kapitolu som venoval vysvetleniu pojmu počítačová kriminalita laickej verejnosti pre lepšie pochopenie tohto problému, ktorý je rozšírený medzi verejnosťou už niekoľko rokov.

V ďalších kapitolách som sa snažil čitateľov oboznámiť s problematikou malvéru a historickým vývojom vírusov.

Ako som už uviedol na začiatku, táto práca by mala slúžiť hlavne laickej verejnosti, no na pochopenie niektorých pojmov je potrebná určitá znalosť informatiky.

BIBLIOGRAFIA

1. **Kostrecová, E.** *Počítačová kriminalita.* Bratislava : Slovenská technická univerzita, 2010. ISBN: 9788022734103.

2. **Kozlow, Anatoly.** metalifestream.com. *Black Hats and White Hats: Interview with an Ethical Hacker.* [Online] http://metalifestream.com/wordpress/?p=5717.

3. **Wikipedia.** Wikipedia.org. *Protokol prenosu súborov.* [Online] https://sk.wikipedia.org/wiki/Protokol_prenosu_s%C3%BAborov.

4. **GoldSparrow.** enigmasoftware.com. *Top 6 Scariest and Most Dangerous Malware on the Loose.* [Online] http://www.enigmasoftware.com/top-6-scariest-most-dangerous-malware/.

5. **Pcrisk.cz.** Pcrisk.cz. *Návod pro odstranění CryptoLocker "Vaše osobní složky jsou zašifrovány!".* [Online] https://www.pcrisk.cz/odstraovaci-piruky/7359-cryptolocker.

6. **Statista.** www.statista.com. *Cyber crime: average company loss in selected countries 2015.* [Online] http://www.statista.com/statistics/293274/average-cyber-crime-costs-to-companies-in-selected-countries/.

7. **Wikipedia.** wikipedia.org. *Usenet.* [Online] https://sk.wikipedia.org/wiki/Usenet.

8. —. wikipedia.org. *Hoax.* [Online] https://sk.wikipedia.org/wiki/Hoax.