Tallinna Ülikool
Informaatika instituut

Turvateadlik tarkvaravalik haridusasutuses.

Bakalaureusetöö

Autor: Mehis Nõulik
Juhendaja: Edmund Laugasson

Autor:..... ..... „ ..... „2016
Juhendaja: ..... „ ..... „2016
Instituudi direktor: ..... „ ..... „2016

Tallinn 2016

Autorideklaratsioon

Deklareerin, et käesolev bakalaureusetöö on minu töö tulemus ja seda ei ole kellegi teise poolt varem kaitsmisele esitatud. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on viidatud.

.....

(autor)

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina _____ (sünnikuupäev: _____)

(autori nimi)

1. annan Tallinna Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose

   _____

   _____

   _____

   (lõputöö pealkiri)

   mille juhendaja on _____,

   (juhendaja nimi)

   säilitamiseks ja üldsusele kättesaadavaks tegemiseks Tallinna Ülikooli Akadeemilise Raamatukogu repositooriumis.

2. olen teadlik, et punktis 1 nimetatud õigused jäävad alles ka autorile.
3. kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest tulenevaid õigusi.

Tallinnas/Haapsalus/Rakveres/Helsingis, _____

(digitaalne) allkiri ja kuupäev

Sisukord

Sõnastik

MBR (Master Boot Record) - *Kõvaketta esimene sektor ehk nullsektor mis kujutab endast 512-baidist buutsektorit ja mida nimetatakse ka jaotussektoriks*. (Vallaste e-teatmik)

Aplet - *väike programm, mis jookseb teise rakenduse sees. Apletid on kasulikud veebis, sest kui nad on kord alla laaditud, siis saab neid kasutajaveebilehitsejas kiiresti täita. Ühes dokumendis võib eksisteerida mitu apleti'it ja nad võivad töötamise ajal üksteisega suhelda. Java on üks peamisi programmeerimiskeeli veebipõhiste aplettide kirjutamiseks.* (Vallaste e-teatmik)

CPU (Central Processing Unit) - *kesktöötlusseade, keskprotsessor ehk arvuti „aju"*. (Vallaste e-teatmik)

Ribalaius - *Ribalaius iseloomustab nii analoog- kui digitaalsignaale ja sidesüsteemis edastatava signaali ribalaius näitab, kui laia sagedusala signaal katab. Ribalaius on võrdeline ajaühikus edastatava informatsiooni hulgaga. Näiteks foto allalaadimiseks ühe sekundi jooksul on vaja suuremat ribalaiust kui ühe tekstilehekülje allalaadimiseks sama aja jooksul. Suured helifailid, arvutiprogrammid ja animavideod nõuavad veel suuremat ribalaiust. Kõige suuremat ribalaiust vajavad virtuaalse tegelikkuse (VR – Virtual Reality) süsteemid ja kolmemõõtmelised audiovisuaalsed programmid.* (Vallaste e-teatmik)

Failipaigutustabel - *Failipaigutustabeliks nimetatakse tabelit, mida operatsioonisüsteem hoiab kõvakettal selleks ettenähtud kaitstud piirkonnas ja kus kirjeldatakse failide füüsilist paigutust kõvakettal.* (Vallaste e-teatmik)

Zero-Day rünnak – rünnak, mille puhul pole uue viiruse signatuur veel avaldatud ning rünnaku puhul kasutatakse ära varem avastamata turvaauku. (Hunter, 2014)

IPS (Internet Protocol Security) - *Andmeturbe standard võrgu- või paketitöötluskihi tasemel.* (Vallaste e-teatmik)

IDS (Intrusion Detection System)

Rendering- *Andmete teisendamine kuvamiseks või printimiseks sobivasse vormingusse.* (Vallaste e-teatmik)

Javascript- *Netscape poolt välja töötatud skriptikeel, mis võimaldab veebiarendajatel luua interatkriivseid veebisaite. Javascript suudab suhelda* ***HTML****-keeles kirjutatud lähtekoodiga ja võimaldab muuta veebilehed dünaamiliseks.* (Vallaste e-teatmik)

HTML (HyperText Markup Language) – *Enimlevinud kodeerimissüsteem (tekstivorming) veebidokumentide loomiseks. HTML koodid ehk märgendid määravad ära selle, kuidas veebileht arvutiekraanil välja näeb.* (Vallaste e-teatmik)

PDF (Portable Document Format) – *Porditav dokumendiformaat või failivorming, Adobe Systems'i loodud platvormist sõltumatu vorming teksti, graafika esituseks.* (Vallaste e-teatmik)

XML (Extensible Markup Language) – *Suvaliste andmete struktureerimiseks mõeldud märgistuskeel, mis loodi eesmärgiga võtta see veebis kasutusele HTML'i asemel.* (Vallaste e-teatmik)

Unreachable code – Surnud koodijupp. Kättesaamatu koodi osa lähtekoodist, mida ei käivitada kunagi kuna sellel ei ole konkreetset käsuvoolu ja selle funktsioone ei käivitata. (Firm)

Sissejuhatus

Käesolema bakalaureusetöö teemaks on “Turvateadlik tarkvaravalik haridusasutuses”. Infotehnoloogia on üks lahutamatu osa igapäevases töös ja eraelus. Tänapäevases väga kiiresti arenevas ühiskonnas puutume kokku üha rohkem erinevat liiki pahavaraga.

Autor on motiveeritud bakalaureusetöö teemal kirjutama, kuna on ise kokkupuutunud erinevat liiki pahavaraga oma elu jooksul ning soovib uurida kui palju pööratakse tähelepanu haridusasutustes IT-turvalisusele tarkvara valiku tegemisel. Sõltuvalt tarkvara valikust ja õpetamise metoodikast sõltub ka edasine IT-alase hariduse efektiivsus ja nende inimeste hakkama saamine tulevikus ning kogu riigi edasine käekäik. Mida haridusasutuses õpetatakse seda ka üldjuhul kasutatakse hilisemas elus.

Käesoleva bakalaureusetöö eesmärgiks on tutvustada pahavara liike, analüüsida haridusasutuste tarkvara valikut ja välja tuua tegurid, mis on määranud tarkvara valiku haridusasutuses. Samuti on autor välja toonud kahe populaarsema tarkvara varasemalt kasutatud turvaauku.

1 Internet ja selle ohud

Internet kujutab endast ebaturvalist teabekanalit mille ülesandeks on infovahetus. **Interneti turvalisus** on arvuti turvalisuse üks haru, mille skoop on internet. See hõlmab kasutaja veebilehitseja kui ka võrgu turvalisust üldisemal tasandil, kuna see kehtib ka teiste rakenduste ja operatsioonisüsteemide kohta tervikuna. Interneti turvalisuse eesmärgiks on kehtestada eeskirju ja meetmeid, et kaitsta end rünnakute eest internetis. Ebaturvaliseks teeb interneti pahatahtlike kasutajate püüded varastada või kuritarvitada tavakasutajate informatsiooni. Erinevad meetodeid on võetud kasutusele, et kaitsta andmevahetust, sealhulgas krüpteerimine ja elementaarsete kui ka komplitseeritud turvalahenduste arendamine.

1.1 **Pahavara** (*Malware*)

Pahavara on programm, mida kasutatakse arvuti operatsioonide segamiseks, salastatud andmete kogumiseks või ligipääsuks personaalsele arvutile. Viirused, ussid, juurkomplektid kuuluvad kõik pahavara alla, kuna nende eesmärk on tekitada kasutajale kahju.

Pahavara sümptomid (Lord, 2012):

- Suurenenud protsessori kasutus.
- Arvuti või veebilehitseja on muutunud märgatavamalt aeglasemaks.
- Probleemid võrku ühendamisel.
- Programmi või kogu süsteemi hangumine ja/või kokkujooksmine.
- Modifitseeritud või kustutatud failid.
- Kummaliste failide, programmide või töölaua ikoonide teke.
- Programmide iseeneslik konfigureerimine, käivitamine või sulgemine (pahavara üritab tihti uuesti konfigureerida või välja lülitada pahavaratõrjet ja tulemüüri programme).

1.1.1 Viirus **(***Virus)*

Arvutiviirus on pahatahtlik arvutiprogramm, mis saab ise paljuneda arvutites või arvutivõrkudes ilma kasutaja oleks teadlik, et arvuti on nakatanud. Kuna iga järgnev koopia suudab ka ise paljuneda, võib nakkus levida väga kiiresti. Viirus põhjustab ootamatuid ja sageli kasutajatele ebameeldivaid tagajärgi. Uuringud näitavad, et arvuti mis on ühendatud internetivõrku võidakse rünnata iga 39 sekundi järel. Selleks, et vältida avastamist kasutajate poolt, kasutavad viiruste loojad erinevaid pettestrateegiaid: (Daoud, Jebril, & Zaqaibeh, 2008)

- **Ülekirjutamise viirus** (Overwriting Virus): Viiruse tüüp, mis kirjutab üle süsteemi faili andmed oma koopiaga hävitades algse programmi. Pärast süsteemi puhastamist viirusest, tuleb kasutajatel algne programm uuesti paigaldada. (webopedia)

- **Nimekaimu viirus**(Companion Infection): Viiruse tüüp, mis võimaldab viirusel kasutada mõne arvutiprogrammiga identset nime, aga erinevat laiendit. Näiteks võib kasutajal olla programm.exe ja viirus loob koopia programm.com. Kui kasutaja käivitab programm.exe käivitab viirus program.com enne kui programm.exe programmi käsud täidetakse. Paljudel juhtudel algne programm käivitub ning kasutajaid ei saagi aru, et arvuti on nakatanud viirusega.

- **Ruumi täitja viirus**(Cavity or spacefiller Virus): Viiruse tüüp, mis üritab end paigaldada arvuti vabale kõvaketta osale, mis ei kahjusta programme. Viiruse eeliseks on see, et ta ei pikenda programmi suurust ning seepärast ei vaja teisi varjamise strateegiaid. Seda tüüpi viirust levib vähe, kuna neid on raske kirjutada ja selle kasutamine on piiratud.

- **Kokkupakitud viirus**(Compressing Virus): Spetsiaalne viiruse tehnika, mis pakib kokku algse programmi sisu. Enamasti kasutatakse seda tehnikat siis, kui viiruse looja tahab algsele programmile oma viiruse külge lisada, ilma et allalaetava programmi suurus ei muutuks. Selleks kasutatakse binaarset kokkupakkimise algoritmi.

- **Krüpteeritud viirus** (Encrypted Virus): Sisaldab endas krüpteeritud viirust ja konstantset dekrüpteerimise koodijuppi. Viirusetõrjega kerge avastada kui kasutatakse ühte konstantset dekrüpteerimise koodijuppi. Süsteemi nõrgestamiseks ei kasutata ühte dekrüpteerimise koodijuppi vaid nende kogumit ning viirus valib suvaliselt neist ühe, millega end dekrüpteerida arvutis.

- **Alglaadimisviirus** (Boot Sectors Virus): Viirus, mis nakatab kõvaketaste alglaadimissektoreid (**MBR**). Arvuti mis on nakatanud alglaadimisviirusega käivitab viiruse arvuti sisse lülitamisel.

- **Makroviirus** (Macro virus): Nakatab Microsoft Word või muu sarnase programmi ja põhjustab tegevuste jada, mis teostatakse programmi käivitamisel. Makroviirused levivad sageli e-posti teel.

- **Pahatahtlik mobiilne koodijupp** (Malicious mobile code): Mobiilne koodijupp on kergprotsess programm, mis laetakse alla eemalasuvast süsteemist ning mida on võimalik käivitada lokaalselt minimaalse või ilma kasutaja sekkumiseta. Levitamiseks kasutatakse Java **aplette**, **JavaScripti** skripte, VisualBasic skripte ja ActiveX komponente, mis võivad ilmenda erinevatel veebilehtedel või **HTML** vormingus e-posti teel. Ründaja võib kasutada mobiilset koodijuppi erinevate pahatahtlike toimingute juures, sealhulgas kasutajate tegevuste monitooring, volitamata juurdepääs arvuti failisüsteemi, nakatada arvutit Trooja hobusega või kaaperdada kasutaja veebibrauser.

1.1.2 Autonoomne tarkvara *(Bot)*

Teenusetõkestamise rünne, DoS-rünne on arvutisüsteemi või võrgu vastu suunatud ründe tüüp, mis ujutab võrgu üle tarbetu liiklusega, nii et võrguteenuse kasutamine muutub võimatuks. DoS-rünne kasutab täielikult ära võrgu ribalaiuse või põhjustab süsteemi arvutusressursside ülekoormuse. DoS-ründed võivad olla suunatud mistahes võrguseadme vastu, kaasa arvatud ruuterid ning veebi-, e-posti- ja nimeserverid.
DoS-rünnete tõkestamiseks peavad sidefirmad ja internetiteenuse pakkujad välja selgitama ründe allika ja blokeerima marsruuterites kuritahtliku liikluse.

Kõigi tuntud DoS-rünnete vastu on loodud tarkvaralisi vahendeid, mida süsteemiülemad võivad paigaldada oma võrgu kaitseks taoliste rünnete vastu. Samal ajal leiutavad pahatahtlikud häkkerid ehk kräkkerid pidevalt uusi DoS rünnakuid, mis nõuab üha uute tõrjeprogrammide loomist või olemasolevate täiustamist. Veel on olemas ka DDoS ehk siis DoS rünne mitmest arvutist korraga (*Distributed DoS*). (Vallaste e-teatmik)

Robotivõrk koosneb suurest hulgast hõivatud arvutitest ehk zombidest, mida omaniku teadmata kasutatakse DoS-, DDoS-rünnete korraldamiseks või rämpsposti levitamiseks. Arvutite hõlmamiseks kasutatakse harilikult ussviiruseid, Trooja hobuseid ja tagauksi, mis avab ligipääsu pahatahtlikule kasutajale tavakasutaja arvutisse ning ootavad käsku robotivõrku kontrollivalt isikult. Eksisteerib terve robotivõrguäri, mis seisnev hõivatud arvutite nimekirjade koostamises ning nende müümises kräkkeritele ja rämpspostitajatele. (Vallaste e-teatmik)

1.1.3 Nuhkvara *(Spyware)*

Nuhkvara nimetatakse faile, mis paigaldatakse arvutisse ilma kasutaja teadmata ja mis võimaldavad salaja jälgida arvutikasutamist. On palju erinevaid nuhkvara liike: klahvivajutuste registreerijad ja paroolivargad, teie poolt külastatavate veebilehtede ja kasutatavate programmide salvestajad, e-posti jälgijad ja ümbersuunajad. Kuna nuhkvara on algselt mõeldud tavakasutaja pealt raha teenimiseks, siis tavaliselt arvutisüsteemi nuhkvara ei kahjusta. Tegelikkuses on paljudel tavakasutajatel nuhkvara nakatanud nende arvuti, ilma et kasutaja sellest ise teadlik oleks. (lifehacker, 2010)

1.1.4 Uss *(Worm)*

Uss sarnaneb viirusega, ta suudab end paljundada võrgukeskkonnas teiste programmide abita, erinevalt tavalisest viirusest, mis vajab paljunemiseks ja levimiseks alg programmi faili. Uss viirus on eraldiseisev programm ning ei vaja alg programmi faile ega kasutaja poolset abi propageerimiseks. Levimiseks kasutavad ussid süsteemi haavatavat kohta. Liikumiseks kasutab uss failide või informatsiooni transportimist , lubades sellel liikuda ilma kõrvalise abita. (Cisco) Kui arvuti on nakatanud ussiga, istub uss arvuti aktiivmälus ja saadab iseennast teistesse arvutitesse peamiselt e-posti teel. (Vallaste e-teatmik)

1.1.5 Trooja Hobune *(Trojan Horse)*

Trooja hobune on kasuliku programmi või andmete sisse manustatud kahjulik programmiosa, mis täidab tegelikult mingit varjatud ülesannet, näiteks muudab teatud tingimustel andmeid, rikubub kõvakettal failipaigutustabeli (**FAT**) või teeb arvutis muud kurja. Trooja hobust nimetatakse vahel ka arvutiviiruseks, kui see laialt levib, kuigi erinevalt viirusest see ise ennast ei paljunda. Enamasti kasutatakse terminit "Trooja hobune" siiski ainult nende kuritahtlike programmide kohta, mis ise ei paljune ning isepaljunevaid programme nimetatakse viirusteks. (Vallaste e-teatmik)

1.1.6 Tagauks *(Backdoor)*

Tagauks on programm, mis võimaldab süsteemi luua turvamata ligipääsu. Tagauks võib olla paigaldatud mõne programmi koosseisu mis garanteerib ligipääsu süsteemi. Kõigepealt nakatub süsteem viiruse, trooja hobuse, ussi või nuhkvaraga, misjärel võimaldab nakkusallikas installeerida tagaukse. Tagauksi kirjutavad ka tarkvara loojad mille abil tarkvara parendada ning see on tagaukse tegelik eesmärk.

1.1.7 Juurkomplekt *(Rootkit)*

Juurkomplekt on teatud tüüpi Trooja hobune, mis hoiab iseennast ning oma tegevuseks vajalikku failidest, registrivõtmetest ja võrguühendustest koosnevat komplekti peidetuna, nii et arvutikasutajal on võimatu avastada selle olemasolu ja tegutsemist oma arvutis. Et selline jälgede peitmine oleks võimalik, peab Trooja hobune looma endale juurkasutaja õigused.

1.1.8 Õngevõtmine *(Phishing, Password fishing)*

Õngevõtmine mis tähendab salasõnade õngitsemist. See termin võeti kasutusele 2003.a. suvel ja tähistab teatud liiki internetikelmust. Suli saadab massiliselt laiali e-posti sõnumeid, mis tuleks näiliselt mõnelt väga suurelt ja tuntud firmalt või pangalt ja teatab, et e-kirja saaja

krediitkaardi andmed vajavad uuendamist või kinnitamist ning palub klõpsata e-kirjas sisalduval lingil. See viib inimese veebilehele, mis näeb välja täpselt nii, nagu oleks tolle suure firma oma, kuid tegelikult on võltsitud. Sellel lehel nõutakse krediitkaardi andmeid, isikukoodi või midagi taolist. Et tekitada suuremat usaldust, varustatakse selline veebileht ka digisertifikaadiga (seegi on harilikult võltsitud) ning andmed edastatakse krüpteeritult. Kogutud andmeid kasutades kurjategija ligipääsu pangaarvetele ja võib esineda teie nime all ka muudes operatsioonides. Kui saate sellise e-kirja, siis tuleb kõigepealt lugeda digisertifikaati ning minna firma ametlikule veebisaidile ja kontrollida, kas firma on tõepoolest teile sellise e-kirja saatnud. (Vallaste e-teatmik)

1.1.9 Lunavara *(Ransomware)*

Lunavara on pahavara vorm, mis sisuliselt hoiab arvutisüsteemi vangistuses samaaegselt nõudes kasutajalt lunaraha. Pahavara piirab kasutaja ligipääsu arvutile krüpteerides failid või lukustades kogu süsteemi. Kasutajat sunnitakse maksma lunaraha, et tagastada ligipääs krüpteeritud failidele või lukustatud süsteemile. (Veracode, 2012) Lunavara levib tavaliselt nagu tavaline viirus. Üks levinuimaid sotsiaalse manipulatsiooni viise, kuidas pahavara looja oma ohvreid leiab, on petukirja abil. Petukirjas sunnitakse kasutajat avama kirjalisa, mis nakatab arvuti pahavaraga või suunab kasutaja nakkust levitavale veebilehele. (Lõugas, 2016)

1.2 Pahavara levimine

1.2.1 Pahavara aastal 2015 Eestis

2015. aastal keerukamad ja tunduvalt suuremat mõju avaldanud juhtumid olid väljapressimise eesmärgil sooritatud pahavarарünded ehk lunavara juhtumid. 2015.aastal teavitati 150 ründest. Eriti palju esines lunavara juhtumeid 2015. aasta viimase kahe kuu jooksul: neli korda enam kui eelnenud kümne kuu jooksul.Tüüpiliste rünnakute puhul krüpteeriti tavakasutajte kõvaketastel olevad andmed, esines ka juhtumeid kui krüpteeriti serverite kõvaketaste andmeid. 2015. aasta järeldus on, et lunavaraga nakatumist on raske täielikult ära hoida isegi kui kasutusel on kõige paremad infoturbe süsteemid. Lunavara kahju aitab vähendada

andmete varundamine. Samuti tuleks kindlaks määratleda kasutajagruppide õigused ning ligipääsud, et lunavaral ei oleks võimalik levida vabalt.

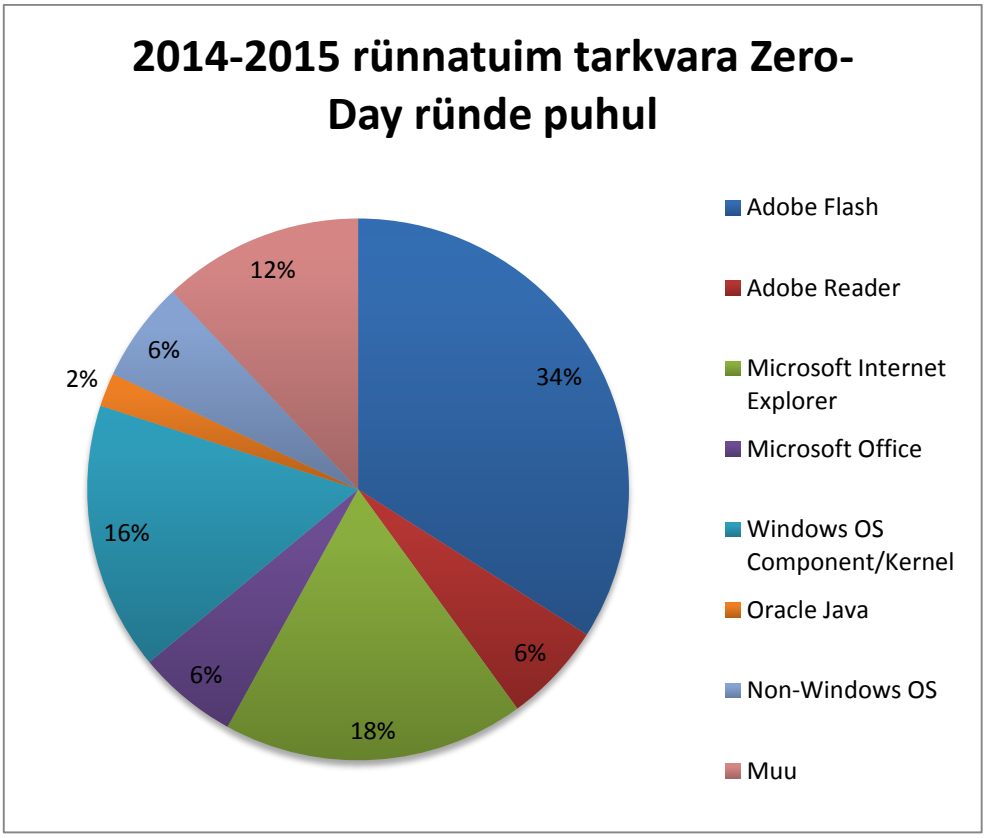
Lisaks lunavara rünnakutele toimus möödunud aastal ka mitmeid teenusetõkestusründeid (DDos) väljapressimise eesmärgil. Juhtumid on sarnased, asutus või ettevõtte langeb teenusetõkestusründe ohvriks. Seejärel saadetakse ohvri kontaktaadressile e-kiri ning nõutakse lunaraha, vastasel korral järgneb tunduvalt suuremas mahus ja pikema kestusega teenusetõkestusrünne. Möödunud aastal registreeriti keskimselt üks teenusetõkestuserünne nädalas. (Riigi Infosüsteemide Amet, 2016)

1.2.2 Zero-Day rünnakud

Tarkvara nõrgad kohad on pidev probleem arendajatele ja kasutajatele. Adobe Flash(edaspidi Flash) on üks sagedamini rünnatud toode. Kolmandiku moodustusid Flash Zero-Day ründed, (Joonis 1 - McAafee uuringute põhjal rünnatuim tarkvara) mis avastati 2014 ja 2015 IT-turvalisusega tegevate firmade poolt. Tänu Flash populaarsusele, tegeleb Adobe aktiivstelt turvaaukude kõrvaldamisega. Ennustatakse, et rünnakud Flashi suunas vaibuvad sellel aastal. Kuna Flash lähtekoodi keerukus ja kvaliteet pole muutunud aastate vältel, ei tasu välistada rünnakute täieliku lõppemist.

Turvaauke MS Internet Exploreris(edaspidi Explorer) on täna vähem kui paar aastat tagasi. See langus on tingitud Exploreri uute turvauuendustega ning nüüd muidugi uue veebilehitseja Microsoft Edge kasutuselevõtmisega. On vaid aja küsimus, kui Microsoft Edge hakatakse samamoodi ründama nagu Explorerit, kuna alati leidub komplitseeritud Zero-Day rünnakuid.

Java, PDF ja Microsoft Office (edaspidi MS Office) rünnakuid on oluliselt vähenenud viimastel aastatel. Java puhul on kohatud vaid üht rünnakut viimase kahe aasta jooksul. MS Office kriitilised Zero-Day rünnakud ei ole samuti väga laialdaselt levinud kuid taolised rünnakud on väga ohtlikud ettevõtetele kes tegelevad andmetöötlusega. Hetkel kasutusel olevad pahavara avastajad ja tõrjumismeetodid ei ole siiani piisavalt tõhusad, mis baseeruvad MS Office baasil. Näitena krüpteeritud MS Office dokumenti on võimalik kasutada, et vältida avastamist pahavaratõrje tarkvara poolt. (Li & Sun, 2016)



Joonis 1 - McAafee uuringute põhjal rünnatuim tarkvara

2 Tarkvaravalik haridusasutuses.

Uuringu eesmärgiks oli uurida haridusasutustes töötavate IT-spetsialistide(edaspidi **spetsialist)** käest, millist tarkvara kasutatakse ning uurida suurimad mõjutegureid tarkvaravaliku tegemisel. Uuringu aluseks valisin Eesti riigigümnaasiumid kuna just sealt tulevad Eesti riigi tuleviku tegijad. Uuringu põhi eesmärk on välja tuua, kui paljud spetsialistid mõtlevad ka haridusasutust hallates turvalisuse peale. Küsitluse täitis 21 riigigümnaasiumi IT-spetsialisti. Uuringu tüübiks oli mugavusvalim.

2.1 Haridusasutustes enimkasutatav tarkvara

Enim kasutatavam tarkvara haridusasutuses on tekstitöötlus tarkvara. Tasulise tekstitöötlus tarkvara kõige populaarsem on Microsoft Office programmid. 89% haridusasutustest kasutavad oma igapäeva töös Microsoft Office tooteid, kuna tegu on kõige levinuma kontoritarkvaraga. Microsoft Office'it kasutatakse väga paljudes ettevõtetes, siis õpilased saavad omale baasteadmised ja oskused, mida on võimalik rakendada ka tulevases töös. (Titlow, 2012) Viis aastat tagasi võis praktiliselt makro pahavara pidada välja surnuks – eelkõige tänu Microsoft Office turvalahenduste uuendustele. (fossBytes, 2015) Eelmisel aastal on makro pahavara taaselustunud, enamjaolt **VBA** makro näol – seekord ei ole tegu isepaljuneva viirusega, vaid allalaetava Microsoft Office dokumendis peituva Trooja Hobuse pahavaraga. (Grooten, 2014) Suurema teadmiste ja oskuste pagasiga kasutajal on arvuti pahavaraga nakatamise oht väiksem, kuna pahavaraga nakatumine eeldab kasutajapoolset tegevust.

57 % haridusasutustest kasutavad lisaks Microsoft Office programmidele paralleelselt LibreOffice programme. Tegu on avatud lähtekoodiga ja vabavaralise kontoritarkvaraga. Kasutajad on teinud avaldusi, et LibreOffice paigaldamisel käivitub nende nuhk- ja/või pahatõrjevara. Üldjuhul on tegu vale-positiivsega (PortableApps). On ka juhtumeid, kui LibreOffice lähtekoodi on peidetud pahavara mis eeldaks programmi allalaadimist originaalallika asemel mõnest võõrast allikast. (Hayes, 2012)

31 % haridusasutustest kasutavad Adobe Readerit. Pahavara levitamine PDF dokumentide kaudu on populaarne meetod kui pahavara looja tahab süsteemi kahjustada. Viimaste uuendustega on Adobe parandanud Readeri nõrku kohti. Adobe on lisaks kasutusele võtnud robustse liivakasti (sandbox) tarkvara, mis aktiveerub kui kurjategija üritab PDF dokumendi kaudu süsteemi rünnata. Tänu liivakasti tarkvarale on kurjategijal väga limiteeritud ajaaken süsteemi kahjustamiseks. (Lakhani, 2016)

Üldiselt kasutatakse tarkvara, mis on viimaste aastate jooksul sattunud vähem teadaolevate rünnakute küüsi(Joonis 1 - McAafee uuringute põhjal rünnatuim tarkvara, ning rünnaku ohvriks sattumise oht on väiksem. Ohtu minimaliseerib lisaks tarkvara uuenduste rakendamine. Siiski ei tohiks lasta valvet alla ning kontroll tarkvara üle peaks olema pidev.

2.2 Suurimad mõjutegurid programmi valikul

Mõjutegureid programmide valikul on mitmeid. Alapeatükis on väljatoodud haridusasutuste spetsialistide mõjutegurid mis on mõjutanud neid programmi valiku tegemisel.

Reklaami mõju - Reklaamitööstusel on tänapäeval suur mõju ning paljud spetsialistid just selle arvelt oma valikuid teevadki.

Asutuse IT-spetsialisti oma valik - Spetsialisti oma eelistused sealhulgas teadlikkus, võimekus, uuringud. Üldjuhul kasutatakse seda mida spetsialist on soovitanud, ilma et keegi veenduks valitud programmi sobivuses. Kasutusele võetakse programm, millega on varasemalt kokkupuudutud.

Finantsiline võimekus haridusasutuses on madal - Väga palju spetsialistidest tõi välja programmide valiku puhul, et see on vabavaraline. Vabavaraga kaasnevad mitmed vabadusastmed, mida omandvara puhul ei kaasne ehk vabadus kasutada, levitada, muuta, uurida. (Free Software's Four Freedoms) Hind on vabavara puhul teisejärguline kuigi just see on saanud sageli selle valiku üheks kriteeriumiks, seda ka Eestis. Seega vabavara valikuga ei tehta mingeid allahindlusi tarkvara kvaliteedis ega hariduslikus sisus - vastupidi: avanevad hoopis uued võimalused, mida omandvara puhul polnud ja seda just hariduslikus mõttes, mistõttu vabavara sobib just eriti hästi haridusasutustele kuid muidugi ka kõikidele teistele. (GNU Operating System, 2014)

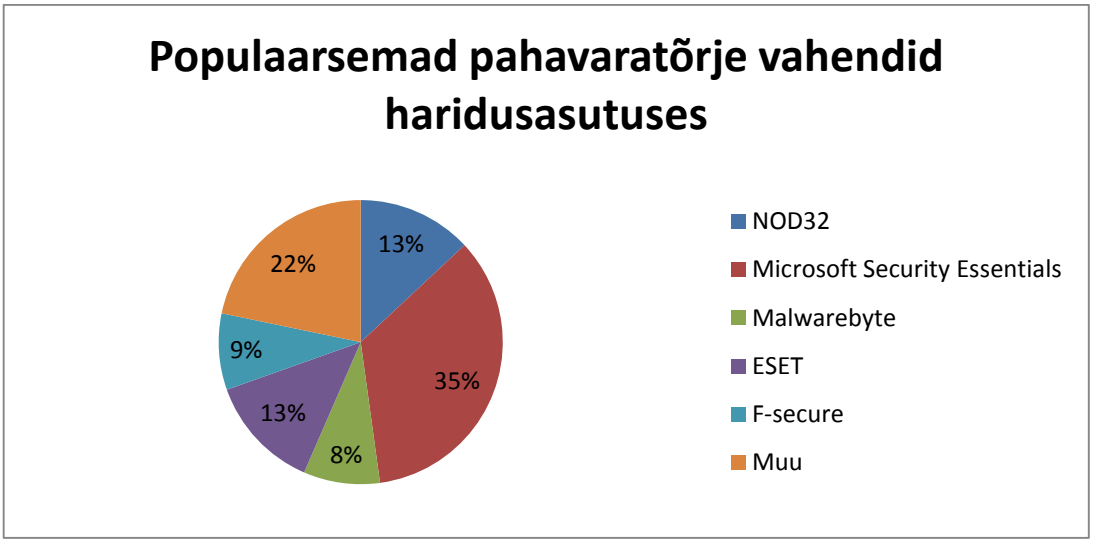
Sotsiaalne mõju - Avaldab suurel määral mõju tarkvaravaliku puhul, sõltumata turvalisusest. Liialt palju usaldatakse sotsiaalseid soovitusi ilma uurimata.

Vahelduvad programmid – Soovitakse õpilastele õpetada erinevaid variante näidates kui suur on vahe tasulisel või tasuta programmil, lisaks ka õpilaste silmaringi laiendamiseks. Õpilastele soovitakse selgeks teha loogika mis erinevate programmide kasutamisel kasuks tuleb. Programmide funktsionaalsus on erinev kuid loogika on sama, näiteks tekstitöötlus programmide puhul. Vabavaralisi programme saavad õpilased kasutada oma arvutis legaalselt, ilma et keegi peaks finantsvahendite puudulikkuse pärast omale alla laadima piraatprogramme. Vabavaralistel programmidel leidub ka piisavalt õpetusi programmiga toimetulekuks. Kõige peamine, praktiline kasutus era- ja ärisektoris.

2.3 Pahavaratõrje vahendid haridusasutuses

Enim kasutatavam pahavaratõrje tarkvara on Microsoft Security Essentials (Microsoft Defender). 35% haridusasutustest kasutavad seda igapäevaselt, et kaitsta end pahavara eest. Kasutatakse enamjaolt tänu sellele, et see tuleb Microsoft Windowsiga tasuta kaasa, ning haridusasutuse spetsialistid ei näe põhjust kasutada lisavahendeid kaitseks.

Teiseks ja kolmandaks kõige populaarsemateks kaitsevahenditeks kujunesid NOD32 ja ESET. Mõlemat pahavaratõrje programmi kasutatakse haridusasutuses võrdselt – 13%. Tarkvara kasutamise põhjuseks toodi välja mugavuse aspekt – litsentsi pikendada on lihtne ning spetsialistide arvates täidab see piisavalt hästi oma ülesannet.



Joonis 2 - Pahavaratõrje vahendid

2.4 IT-turvalisus

Mitte ükski haridusasutuse IT-spetsialist ei toonud välja turvalisuse aspekti. Üha vähem pööratakse turvalisusele tähelepanu, mis omakorda suurendab uute probleemide päevakorda tekkimist, mida kinnitab ka uuring - mitte ükski spetsialist ei maininud valiku tegemisel turvalisust. Kui ei mõelda turvalisuse peale praegu, ei mõelda selle peale ka tulevikus. IT-turvalisuse tagamine ja kohustus on lahutamatud osad IT kasutamisel. IT-turvalisusele pööratakse võrreldes teiste valdkondadega (kulutustega, mugavusega, ..) palju vähem tähelepanu. Eriti vähe pööratakse tähelepanu uue tarkvara või süsteemide kasutusele võtmisel või ei pöörata sellele üldse tähelepanu. (RIA, 2009) Turvameetmete kasutusele mittevõtmine võib kaasa tuua raskeid tagajärgi, näiteks infosüsteemi rakenduste töö katkemine takistab oluliselt igapäevaselt tehtavat tööd. (Hansson & OÜ, 2013) IT-turvalisuse tagamine peab olema haridusasutuste tegevuste lahutamatu osa. Kõige halvemal juhul lükatakse turvameetmete kasutuselevõttu koguaeg edasi ning tänu sellele on haridusasutusel oht ja risk palju suurem sattuda rünnaku ohvriks. Kõikide haridusasutuste õpilased ja vilistlased on Eesti riigi tulevik millest sõltub edasine jätkusuutlikus ja areng. Tänaseks on põhimõtteliselt kõik elu protsessid seostunud infotehnoloogiaga. Üheks suurimaks probleemiks on kasutajate IT-turvalisuse tagamine ning teadvustamine. Õpilastel puuduvad teadmised kuidas kaitsta end internetiohtude eest ning kuidas käituda juhul kui arvuti on kokkupuutunud mõne potentsiaalselt kahjutekitava programmiga. Ei mõelda iseenda turvalisuse peale ning väga tihti

jagatakse oma andmeid mõne kolmanda osapoole tarkvaraga. Samuti ei märgata ohtu interneti avarustes ning väga tihti sisestatakse oma personaalne info mõnda veebikeskkonda, mille tagajärjel kasutatakse saadud infot illegaalsete eesmärkide täitmiseks. Õpilastele tuleks seletada kui tähtis on turvalisus ja kuidas seda tagada, et süsteemi ei pääseks kahjurid, mis võiksid kompromiseerida või kahjustada tervikut süsteemi.

2.5 IT-turvalisuse suurendamine

Kõige haavatavam osa arvutisüsteemis on inimene. Haridusasutused peavad keskenduma sama palju töötajate ja õpilaste koolitusele turvalisuse osas, kui muudele tegevustele. See tähendab, et mitte koondada vahendeid ainult viimase nuhk- ja/või pahavaratõrje peale, vaid samuti hariduse ja töötajate koolitusele - inimfaktorile. (Computing now, 2013)

Tarkvara funktsionaalsus, kasutusmugavus on aspektid, mis peaaegu alati konkureerivad IT-turvalisusega. Seetõttu tuleb tarkvara väljavalimisel teha analüüs, seda võrrelda sarnastega, uurida potensiaalseid turvaauke ning teha kasutajasgrupile selgeks, kuidas vältida potensiaalseid ohtusid. Hiljem tekkinud puudujäägid tarkvara valikul võivad põhjustada ulatuslikke probleeme süsteemi töös. Tehes kärpeid tarkvara kasutusmugavuse või loobudes mõnest funktsionaalsusest võib ära hoida turvaintsidentidest tekkinud kulusid. (RIA, 2009)

Tuleb määratleda IT-turvalisuse eesmärgid, et oleks võimalik välja töötada abinõud, mis on pikaajaline protsess. IT-turvalisusega seotud ülesandeid tuleb pidevalt korrata ning regulaarselt tuleks üle vaadata uued turvastandardid. Vältida tuleks liiga põhjalikke turbenõudeid – need võivad tunduda pigem kasutajate kiusamisena. Turbenõuded tuleks koostada sellised, et neid oleks võimalik täita kõigil. (RIA, 2009)

Üks võimalus IT-turvalisust suurendada on kasutada tarkvara, mis on vähem haavatavam pahavarale - see olekski üks lihtsamaid, säästlikumaid, jätkusuutlikumaid viise turvateadlikuks tarkvaravalikuks haridusasutuses. Seda võimalust on tihti alahinnatud - eriti haridusasutustes. Isegi põhikooli riikliku õppekava informaatika valikaine soovitab eelistada vabavara kuid kahjuks kiputakse seda soovitust sageli ignoreerima. Näiteks MS Windowsi platvormile loodud pahavara ei toimi Linuxis. Levib mitmeid arvamusi, et kui Linuxit hakatakse rohkem kasutama - küll siis pahavara ka rohkem tegem hakaatakse. Samas ei ole see siiski nii kuna tegemist on juba algselt turvalisema ülesehitusega, mis muudab pahavara

leviku keeruliseks. Linux on täna levinud ja seda eriti missioonikriitilistes kohtades (nt pangad) ent ometi ei ole suudetud sinna nii massiliselt pahavara luua nagu seda on MS Windowsi platvormile. (Noyes, 2010) Lisaks on mitmeid mehhanisme, mis aitavad ka Linuxit veel omakorda turvalisemaks muuta, neid tuntakse märksõna security hardening all. Analoogseid lahendusi on erinevatele operatsioonisüsteemidele ent ka kasutatav operatsioonisüsteem ise peab ülesehituse poolest olema piisava turvalisusega. Paljud turvaeksperdid võrdlevad MS Windowsi turvaliseks muutmist kui sõela lappimist, millega vett üritatakse kanda. (Raymond) Paljud missioonikriitilised serverid kasutavad Linuxit jt vabu UNIX'eid. (Compare business products, 2010) Ometi ei suudeta neid sisuliselt maha murda - vastasel korral ei saaks me rääkida internetipangandusest. On selge, et turvalisus ei ole seisund vaid protsess, mille eest peab pidevalt hea seisma. See tähendab regulaarselt tarkvara uuendama, süsteemi kontrollima jt turvaprotseduure läbi viima. Kuid siiski on pahavara Linuxis pigem erand kui reegel - seda ei saa aga öelda MS Windowsi kohta kus olukord kipub vastupidi olema. Internetis liigub õpetusi kuidas Linuxis pahavara käivitada kui on soov testida kuna niisama on keeruline pahavara käivitada - peab ise selleks pingutama. On selge, et keegi seda vabatahtlikult ei tee oma süsteemi nakatamiseks kui ei ole just tegemist katsetamisega (Ubuntu documentation, 2011).

Liigub ka arvamusi, et kui Linuxis on paigaldatud MS Windowsi ühilduvuskiht Wine siis selle kaudu on võimalik kahju teha. See on tõsi ja seetõttu ka missioonikriitilistesse süsteemidesse (nt serverid) Wine'i jt nõrgemate operatsioonisüsteemide ühilduvuskihte ei paigaldata. Kui see siiski on vajalik siis kasutatakse selle eraldamist süsteemist - konteinerid (Linux Containers), virtualiseerimine. (CategoryVirtualization)

Siiski on võimalik ka Linuxile viirusetõrjeid paigaldada (peamiselt MS Windowsi kasutajate käest tulnud failide puhastamiseks, et edasi ei levitaks teistele MS Windowsi kasutajatele). (Linux Security Review, 2015)

Üks ekstreemsemaid näiteid MS Windowsi pahavara kahjulikkuse ulatusest on dokumentaafilm "Veebisõdalased" (Dahl, 2008) seal suudeti 133 MHz Pentium protsessoriga arvuti abil jooksutada MS Windowsi viirust Blaster ning tekitada ~6 miljardi USA dollari suuruses majanduskahju USA'le, mille käigus umbes pool USA territooriumit mõneks päevaks elektrita oli ja isegi üks tuumaelektrijaam seiskus. Selle taga oli kõigest 15-aastane noormees kes testis enda loodud pahavara. Võib vaid ette kujutada, millist kahju suudetakse

teha kui selle ülesande võtavad ette kogenud terroristid kellel on ka piisavalt rahalist jm ressurssi. See oli omakorda õppetunniks, et missioonikriitilisi süsteeme ei ole mõistlik nii haavatava tarkvara kui MS Windows peale paigaldada. Filmis küll seda selliselt ei näidata kuna püüti olla viisakad Microsofti vastu ja pigem räägiti juba sellest, et kas üldse missioonikriitilisi süsteeme internetiga ühendada, millel ka teatav mõte olemas kuid siiski mitte väga praktiline kuna süsteeme on vaja kaughallata ja internet on üks paremaid viise selleks tänapäeval. Räägitud on ka turvalisema interneti "Internet2" loomisest ja see on täna juba olemas kuid mitte veel massiliselt levinud, kus näiteks kasutamine võimalik vaid isikut tuvastades jms tõhusamaid turvameetmeid kasutades. (Internet 2)

3 Nakatumine pahavaraga

Antud peatükkis näidatakse, kuidas paar aastat tagasi rünnati PDF ja Microsoft Office failiga kasutajate arvuteid ning saadi sellele ligipääs. Tuleb märkida asjaolu, et sellised rünnakud oleksid olemata kui kasutatavat tarkvara valitaks turvateadlikumalt, millest oli juttu eelmises peatükis. Autor valis kaks programmi, mida kasutatakse enamates haridusasutustes. Antud turvaauke autor ise ei testinud kellegi peal ning kogu info ja pildimaterjal on võetud internetist. Autor tahab lihtsalt edasi anda mõtte, kui lihtne on murda kellegi arvutisse kui avatakse faili, mis näiliselt tuleb tuttavalt ja usualdusväärsest allikast.

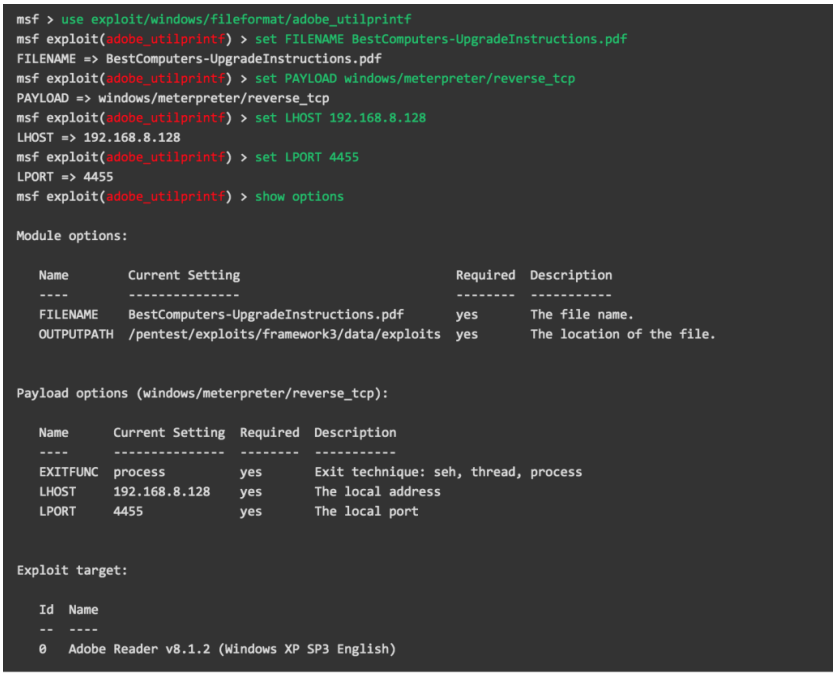
3.1 PDF pahavara loomine Metasploit programmiga

Metasploit – Testimisplatvorm mida kasutatakse turvatestide tegemiseks ning turvaaukude valideerimiseks. Platvorm sisaldab Metasploit raamistikku ja kommerts versioone: Metasploit Pro, Express Community ja Nexpose Ultimate.

Pahavara loomiseks kasutatakse vanemat turvaauku, mida tuntakse Adobe Reader 'util.printf()' **JavaScripti** funktsioonina. See oli probleemiks Windows operatsioonisüsteemidel mis kasutasid Reader versiooni 9.4.6 kuni 10. Adobe Reader kasutab **stack** ehk pinu puhvrit mis ebaõnnestus kasutaja poolt sisestatud andmete kontrollimisel. PDF faili avamisel saab ründaja kasutada seda turvaauku ning käivitada oma kirjutatud koodi saades rünnatava kasutaja privileegid süsteemis. Ründaja saab samuti kokku jooksutada programmi, mille tulemuseks on **DoS** rünne.

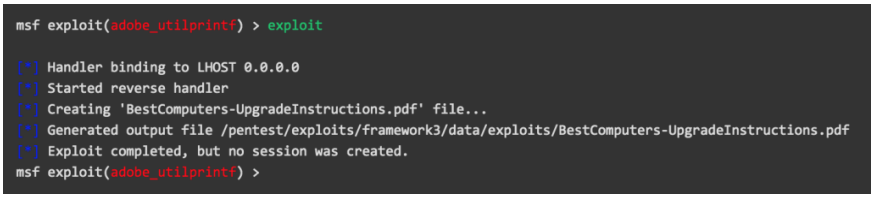
Kuigi see on vanem turvaauk töötavad enamus uuemad turvaaugud sarnasel loogikal. Ründajad kasutavad ära **Zero-Day** rünnakut et saavutada sama tulemus, mida näeme siin. (Lakhani, 2016)

Kõigepealt pannakse paika pahavara sätted. Joonis 3 – Metasploit konsool, pahavara seaded



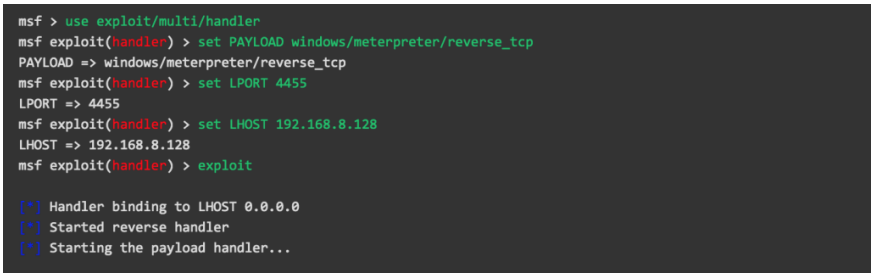
Joonis 3 – Metasploit konsool, pahavara seaded

Kui pahavara sätted on paika pannud, luuakse PDF fail. Joonis 4 – Metasploit konsool, pahavara loomine



Joonis 4 – Metasploit konsool, pahavara loomine

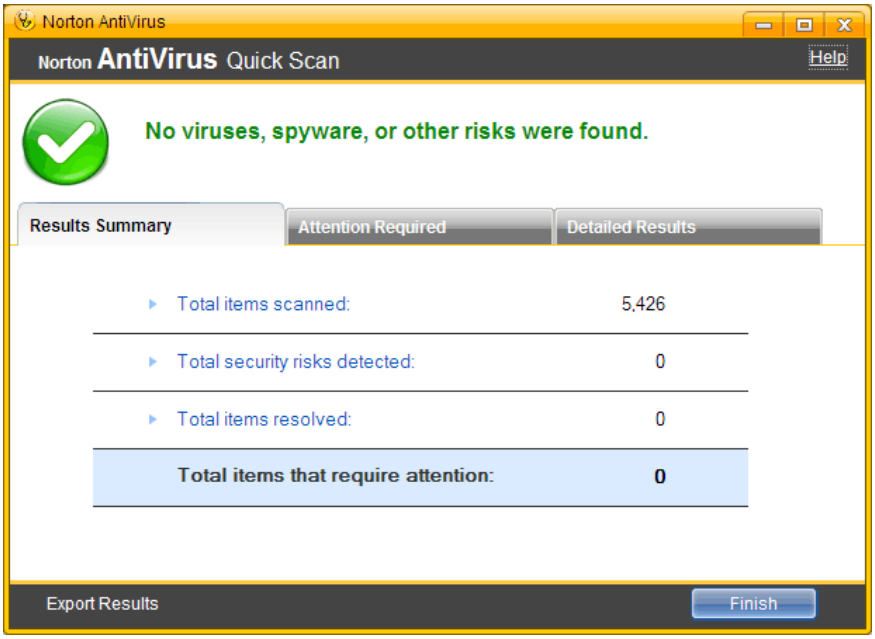
Nagu näha on loodud väljund PDF fail „BestComputers-UpgradeInstructions.pdf“. Enne PDF faili välja saatmist on vaja seada **listener** ehk kuulaja mis ühendub rünnatava arvutiga ning saab sellelt tagasisidet kui kasutaja PDF faili avab. Joonis 5 – Metasploit konsool, kuulaja paigaldamine



Joonis 5 – Metasploit konsool, kuulaja paigaldamine

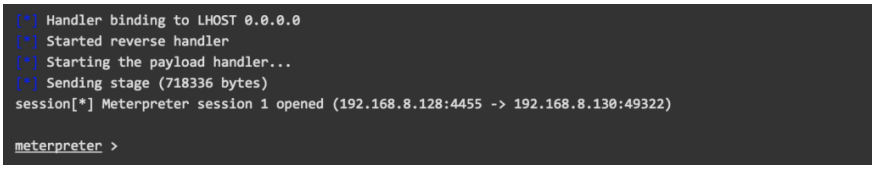
Nuhkvaratõrje tarkvaraga PDF faili kontrollides tundub, et PDF fail on puhas, ning ei sisalda kasutajale ohtu. Joonis 6 – Norton AntiVirus pahavaratõrje tarkvara Faili avades kuvatakse

kasutajale vaid hall taust PDF failis, kuna sisu reaalselt PDF failile pole vajagi. Et käivitada pahavara, on vaja ainult avada PDF fail. Kasutaja ei pruugigi aru saada, et tema arvuti on nakatanud pahavaraga, mis tagab ründajale ligipääsu tema arvutisüsteemile kui ka andmetele.



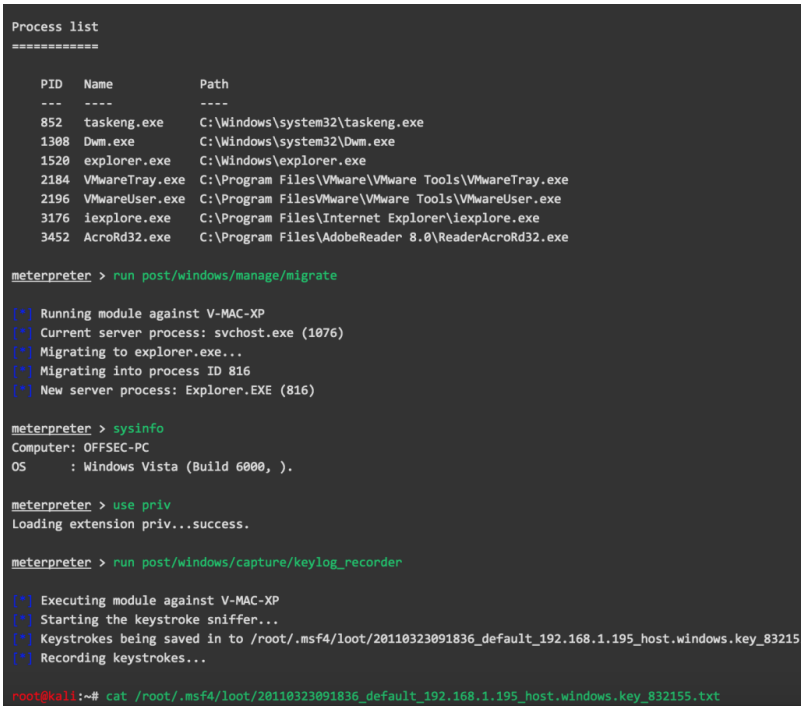
Joonis 6 – Norton AntiVirus pahavaratõrje tarkvara

Niipea kui kasutaja faili avab, näeb ründaja tagasisidet sessiooni avamise kohta Joonis 7 – Metasploit konsool, ohvri poolt avatud sessioon.



Joonis 7 – Metasploit konsool, ohvri poolt avatud sessioon

Edasi on võimalik ründajal tegutseda oma nägemise järgi kasutaja süsteemis. Ründaja peidab oma pahavara protsessi süsteemis, et sessioon ei katkeks ka pärast PDF faili sulgemist, näeb kasutajal kasutuselolevat operatsioonisüsteemi ning käivitab klahvijälgimise protsessi Joonis 8 – Metasploit konsool, ohvri arvuti andmed.



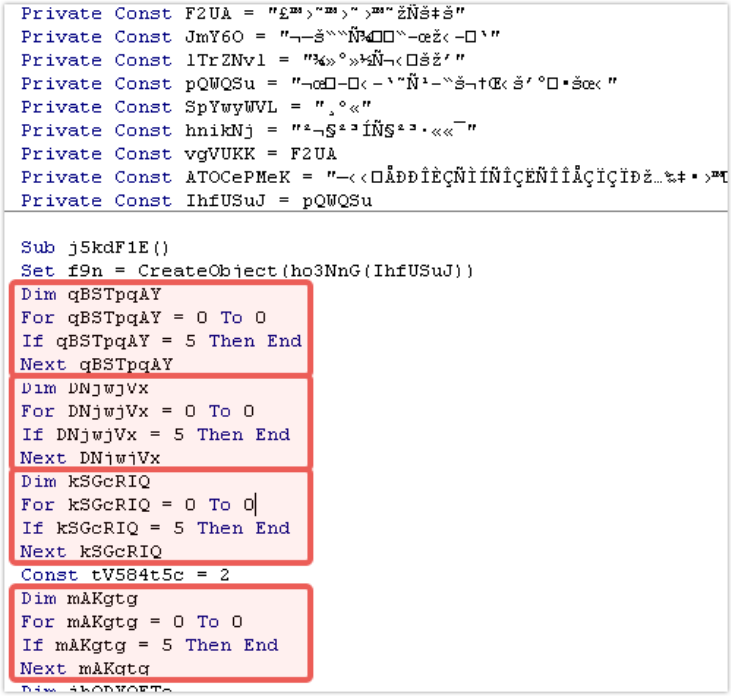
Joonis 8 – Metasploit konsool, ohvri arvuti andmed

3.2 Microsoft Office VBA makrod

Microsoft Office dokumendid – Word, Excel, PowerPoint ja muud dokumendid võivad sisaldada endas varajatud koodi mis on kirjutatud **VBA** programmeerimiskeeles. Microsoft Office's on võimalik salvestada oma makrosid kasutades selleks sisseehitatud Macro Recorder'it. See võimaldab automatiseerida korduvaid ülesandeid. Makrod mis on loodud enda jaoks, ei kujuta endast turvariski. Ründajad aga loovad makrosid, et teha võimalikult palju kahju kasutaja arvutis. Makrod võivad kasutada **VBA Shell**'i käsurida, et jooksutada suvalisi käske või programme ning kustutada käsurea abil faile. (How-to Geek, 2013)

Üllatusena on **VBA** pakettides hakatud kasutama omaette seisvat **XML** faili formaati, mis võeti kasutusele Microsoft Office poolt aastal 2003. Pahavara autorid loodavad, et harvaesinevat ja kasutatavaid **XML** tüüpi faile ei ole lisatud kõikidesse turvauuendustesse lootes et Microsoft Office ei suuda seda korralikult dekonstrueerida.

Kasutades hiljuti leitud näidet, ekstraktiti VBA koodijupp XML'i andmestruktuurist. Joonis 9 – Ekstraktitud VBA koodijupp



```
Private Const F2UA = "£™›"™›" ›™"žŇš‡š"
Private Const JmY6O = "¬—š˜˜Ñ¤□□˜–œž‹–□‘"
Private Const lTrZNvl = "¾»°»½Ñ¬‹□šž′"
Private Const pQWQSu = "¬œ□–□‹–‘˜Ñ¹–˜š¬†Œ‹š′°□▪šœ‹"
Private Const SpYwyWVL = "¸°«"
Private Const hnikNj = "ª¬§ª³Íѧª³·««¯"
Private Const vgVUKK = F2UA
Private Const ATOCePMeK = "—‹‹□ÅÐÐÎÈÇÑÌÍÑÎÇËÑÎÎÅÇÏÇÏÐž…‰‡▪›™
Private Const IhfUSuJ = pQWQSu

Sub j5kdF1E()
Set f9n = CreateObject(ho3NnG(IhfUSuJ))
Dim qBSTpqAY
For qBSTpqAY = 0 To 0
If qBSTpqAY = 5 Then End
Next qBSTpqAY
Dim DNjwjVx
For DNjwjVx = 0 To 0
If DNjwjVx = 5 Then End
Next DNjwjVx
Dim kSGcRIQ
For kSGcRIQ = 0 To 0
If kSGcRIQ = 5 Then End
Next kSGcRIQ
Const tV584t5c = 2
Dim mAKgtg
For mAKgtg = 0 To 0
If mAKgtg = 5 Then End
Next mAKgtg
```

Joonis 9 – Ekstraktitud VBA koodijupp

Algul keerulisena tunduv koodijupp on tegelikult lihtne, mis on sihipäraselt keeruliseks aetud, et tekitada segadust koodi lugemisel. Pärast koodi dekodeerimist ja müra(**Unreachable Code**) eemaldamist näeb kood välja selline.

```
Set fsoObj = CreateObject("Scripting.FileSystemObject")
Set tempDirPath = fsoObj.GetSpecialFolder(2)

exeUri = "http://178.[redacted]:8080/azvxjdfr31k/abs5ajsu.exe"
exePath = tempDirPath & "\fdgfdgdfga.exe"

Set httpObj = CreateObject("MSXML2.XMLHTTP")
httpObj.Open "GET", exeUri, False
httpObj.send

Set fsoObj = CreateObject("Scripting.FileSystemObject")
If fsoObj.FileExists(exePath) Then
    fsoObj.DeleteFile (exePath)
End If

Set streamObj = CreateObject("ADODB.Stream")
With streamObj
    .Type = 1
    .Open
    .Write httpObj.responseBody
    .SaveToFile exePath
    .Close
End With

Set streamObj = Nothing

Set shellObj = CreateObject("Shell.Application")
shellObj.Open tempDirPath & "\fdgfdgdfga.exe"
```

Joonis 10 – Dekodeeritud kujul kood

Koodi eesmärk on luua HTTP ühendus, allalaadida käivitatav fail abs5ajsu.exe, see salvestada TEMP kausta uue nimega fdgffdgdfga.exe ning see lõpuks käivitada. Siin näites kasutatud pahavara oli üks varaint Dridex'st ehk teisisõnu Trooja Hobune. (Chantry, 2015)

3.3 Rünnakute tõkestamine

Kui mõni taoline rünnaku katse tehakse haridusasutuse pihta ning rünnak on edukas, siis oleks võimalik jälgida ja vaadata rünnatud kasutaja õigustele määratud faile, dokumente jms. Samuti oleks võimalik välja uurida kasutaja paroole ning tekitada kaost haridusasutuse infosüsteemis.

Me võime kaitsta oma võrku taolist tüüpi pahavara ja rünnakute eest kasutades tugevamat e-kirja ja veebi sisu filtreerimist ja rakendades **IPS** (Intrusion Prevention System) ja **IDS** (Intrusion Detection System) süsteeme. Kui **IPS** süsteem ebaõnnestub ründe puhul, aitab **IDS** pahavara tuvastada ja kõrvaldada. Samuti on võimalik kasutada rakenduste tasemel kontrolle, et nurjata rünnak:

- **JavaScripti** blokeerimine
- **PDF** visualiseerimise(**rendering**) blokeerimine
- **PDF** lugejate faili- ja võrgutasandil blokeerimine

Uuemad Adobe Reader versioonid sisaldavad endas pahavara liivakasti, mis käivitatakse siis, kui pahavara leitakse Readeri poolt. Siiski on olemas pahavara mis suudab vältida vastumeetmeid, seega soovituslik oleks kasutada mitmetasandilist kaitset.

Muud üldised meetmed, millel on relatiivselt tugev võimalus avastada ja kõrvaldada seda tüüpi rünnakuid:

- **Zero-Day** rünnakute vastu implementeeritud pahavara avastamise vahendid
- Võrgust väljamineva võrguliikluse monitoorimine
- Turbetööriistade seadistamine, mis spetsiaalselt otsivad programmijuppe mis suudavad muuta kasutajaõiguseid ja käivitada operatsioonisüsteemi teenuseid. (Lakhani, 2016)

- Rünnakuid on võimalik takistada ka selliselt, et kasutatakse tarkvara, mis on vähem haavatavam pahavara suhtes ehk siis valitakse tarkvara turvateadlikumalt. Selleks on vabavara ning seda olukorda on täpsemalt kirjeldatud eespool peatükis “IT turvalisuse suurendamine”.

4 Kokkuvõte

Käesoleva bakalaureusetöö põhieesmärgiks oli uurida haridusasutuste IT-spetsialistide käest millist tarkvara kasutatakse ning mis määras tarkvara valiku.

Kõigepealt kirjutab autor erinevates pahavara liikidest ning seletab lahti nende tähenduse. Seejärel analüüsib haridusasutuste spetsialistide vastuseid küsimustikule. Lühidalt on kirjeldatud kolme enim kasutatad tarkvara ning välja toodud nende nõrgad kohad. Uuringust selgus, et mitte ükski spetsialist ei maininud tarkvara valimisel turvalisust.

Autor võrdles ka haridusasutustes kasutatavaid pahavaratõrje tarkvara, milline neist oli kõige kasutatavam ning kuidas varieerusid ülejäänud.

IT-turvalisusele pööratakse palju vähem tähelepanu kui näiteks mugavusele või funktsionaalsusele. IT-turvalisuse tagamine ja kohustus on tegelikkuses lahutamatud osad IT süsteemide kasutamisel ja uue tarkvara valikul.

Kuid kui valida tarkvara, mis on vähem haavatavam siis tagatakse sellega ka kõrgem turvalisus - see ongi turvateadlik tarkvaravalik ja kehtib mitte ainult haridusasutustele vaid kõigile. Selliseks tarkvaraliigiks on vabavara, mida on sageli alahinnatud - seda eriti haridusasutustes kuigi isegi põhikooli riiklik õppekava läbi informaatika valikaine lausa soovitab seda õpetada ja kasutada. On selge, et turvalisus ei ole seisund vaid protsess, mille eest peab pidevalt hea seisma ent siiski on vabavara juba eos oluliselt turvalisema ülesehitusega, mis väldib pahavara massilise leviku nagu seda on juhtunud MS Windowsi platvormil.
Ent siiski valides tarkvaraks vabavara välditakse muuhulgas terve rida turvalisusega seotud probleeme, mis paraku kummitavad vaid omandvara. Spekuleeritakse teemal: kui vabavara levima hakkab siis sinna ka pahavara rohkem tehakse - see ei ole paraku paika pidanud kuna vabavara juba ka kasutatakse päris palju ja selle turvalisema ülesehituse tõttu ei ole see selliselt realiseeritav olnud. Vabavara kasutamist soovitab ka Eesti valitsus läbi põhikooli riikliku õppekava, koosvõime raamistiku (Majandus- ja Kommunikatsiooniministeerium, 2014) riigihangete kui ka Riigi Infosüsteemide Ameti kodulehe. (Riigi Infosüsteemi Amet)

5 Kasutatud kirjandus

Compare business products. (23. märts 2010. a.). Kasutamise kuupäev: 27. aprill 2016. a., allikas http://www.comparebusinessproducts.com/fyi/50-places-linux-running-you-might-not-expect

Ubuntu documentation. (09. aprill 2011. a.). Kasutamise kuupäev: 18. aprill 2016. a., allikas Linuxvirus: https://help.ubuntu.com/community/Linuxvirus

Veracode. (oktoober 2012. a.). Kasutamise kuupäev: 11. 2016 04. a., allikas https://www.veracode.com/blog/2012/10/common-malware-types-cybersecurity-101

(11. september 2013. a.). Kasutamise kuupäev: 19. 03 2016. a., allikas How-to Geek: http://www.howtogeek.com/171993/macros-explained-why-microsoft-office-files-can-be-dangerous/

Computing now. (november 2013. a.). Kasutamise kuupäev: 12. aprill 2016. a., allikas https://www.computer.org/portal/web/excelsior-college/content?g=7797379&type=article&urlTitle=is-human-error-biggest-cybersecurity-vulnerability-

GNU Operating System. (09. november 2014. a.). Kasutamise kuupäev: 30. aprill 2016. a., allikas http://www.gnu.org/education/

Majandus- ja Kommunikatsiooniministeerium. (18. mai 2014. a.). Kasutamise kuupäev: 24. aprill 2016. a., allikas https://www.mkm.ee/et/riigi-infosusteemi-koosvoime-raamistik

fossBytes. (15. detsember 2015. a.). Kasutamise kuupäev: 26. aprill 2016. a., allikas http://fossbytes.com/return-of-the-macro-malware-and-evolution-of-fileless-malware/

F-secure. (2015). Kasutamise kuupäev: 15. 04 2016. a., allikas https://www.f-secure.com/documents/996508/1030743/Threat_Report_2015.pdf

Kaspersky. (detsember 2015. a.). Kasutamise kuupäev: 12. aprill 2016. a., allikas https://securelist.com/files/2015/12/Kaspersky-Security-Bulletin-2015_FINAL_EN.pdf

Linux Security Review. (26. mai 2015. a.). Kasutamise kuupäev: 28. aprill 2016. a., allikas Av-comparatives: http://www.av-comparatives.org/wp-content/uploads/2015/05/avc_linux_2015_en.pdf

Riigi Infosüsteemide Amet. (2016). Kasutamise kuupäev: 25. aprill 2016. a., allikas https://www.ria.ee/public/Kuberturvalisus/RIA_kuberturbe_aruanne_2015.pdf

Arvutiturve. (kuupäev puudub). Kasutamise kuupäev: 17. aprill 2016. a., allikas https://arvutiturve.wordpress.com

CategoryVirtualization. (kuupäev puudub). Kasutamise kuupäev: 27. aprill 2016. a., allikas Ubuntu documentation: https://help.ubuntu.com/community/CategoryVirtualization

Chantry, G. (06. märts 2015. a.). *naked security*. Kasutamise kuupäev: 22. aprill 2016. a., allikas https://nakedsecurity.sophos.com/2015/03/06/from-the-labs-new-developments-in-microsoft-office-malware/

Cisco. (kuupäev puudub). Kasutamise kuupäev: 10. aprill 2016. a., allikas http://www.cisco.com/c/en/us/about/security-center/virus-differences.html

Dahl, J. (Režissöör). (2008). *Web Warriors* [Film].

Daoud, E. A., Jebril, I., & Zaqaibeh, B. (september 2008. a.). Kasutamise kuupäev: 4. aprill 2016. a., allikas http://www.emis.de/journals/IJOPCM/files/IJOPCM(vol.1.2.3.S.08).pdf

Firm. (kuupäev puudub). Kasutamise kuupäev: 24. aprill 2016. a., allikas http://pp.ipd.kit.edu/firm/Unreachable_Code

Free Software's Four Freedoms. (kuupäev puudub). Kasutamise kuupäev: 30. aprill 2016. a., allikas fsfe: https://fsfe.org/freesoftware/basics/4freedoms.en.html

Grooten, M. (juuli 2014. a.). *Virus Bulletin*. Kasutamise kuupäev: 6. aprill 2016. a., allikas https://www.virusbulletin.com/virusbulletin/2014/07/vba-not-dead

Hansson, L., & OÜ, P. (2013). *Innovatsioonikeskus.* Kasutamise kuupäev: 11. aprill 2016. a., allikas Hariduse Infotehnoloogia Sihtasutus

Hayes, S. (2012). Behind the Screen with Windows XP and LibreOffice.

Hunter, E. (16. oktoober 2014. a.). *Rahvusvaheline kaitseuuringute agentuur*. Kasutamise kuupäev: 4. aprill 2016. a., allikas http://www.icds.ee/et/blogi/artikkel/vene-hakkerite-ruhmitus-tungis-oluliste-sihtmarkide-arvutivorkudesse/

Internet 2. (kuupäev puudub). Kasutamise kuupäev: 26. aprill 2016. a., allikas http://www.internet2.edu/

Lakhani, A. (28. veebruar 2016. a.). *Doctor Chaos.* Kasutamise kuupäev: 14. aprill 2016. a., allikas http://www.doctorchaos.com//distributing-malware-inside-adobe-pdf-documents/

Li, H., & Sun, B. (2016). *McCafee.* Kasutamise kuupäev: 14. aprill 2016. a., allikas http://www.mcafee.com/us/resources/reports/rp-threats-predictions-2016.pdf

lifehacker. (september 2010. a.). Kasutamise kuupäev: 10. aprill 2016. a.

Linux Containers. (kuupäev puudub). Kasutamise kuupäev: 29. aprill 2016. a., allikas https://linuxcontainers.org/

Lord, N. (oktoober 2012. a.). *Veracode*. Kasutamise kuupäev: 05. aprill 2016. a., allikas https://www.veracode.com/blog/2012/10/common-malware-types-cybersecurity-101

Lõugas, H. (märts 2016. a.). *Geenius*. Kasutamise kuupäev: 11. aprill 2016. a., allikas http://geenius.ee/uudis/eesti-turvaspetsid-opetavad-10-vihjet-millest-ara-tunda-pahavara-levitav-e-kiri

Magelhaes, R. (17. september 2014. a.). *WindowSecurity.* Kasutamise kuupäev: 8. aprill 2016. a., allikas http://www.windowsecurity.com/articles-tutorials/misc_network_security/third-party-software-security-threat-part1.html

Noyes, K. (03. august 2010. a.). *PCWorld*. Kasutamise kuupäev: 22. aprill 2016. a., allikas http://www.pcworld.com/article/202452/why_linux_is_more_secure_than_windows.html

PortableApps. (kuupäev puudub). Kasutamise kuupäev: 10. aprill 2016. a., allikas http://portableapps.com/node/28507

Raymond, E. S. (kuupäev puudub). Kasutamise kuupäev: 19. aprill 2016. a., allikas http://www.catb.org/~esr/faqs/hacker-howto.html

RIA. (juuli 2009. a.). *RIA*. Kasutamise kuupäev: 12. aprill 2016. a., allikas https://www.ria.ee/public/ISKE/Infoturbe_soovituste_juhend_v1.pdf

Riigi Infosüsteemi Amet. (kuupäev puudub). Kasutamise kuupäev: 28. aprill 2016. a., allikas https://www.ria.ee/ee/otsi.html?query=vabavara

Social-Engineer. (kuupäev puudub). Kasutamise kuupäev: 13. aprill 2016. a., allikas http://www.social-engineer.org/framework/psychological-principles/eye-cues/

Sun, B., & Li, H. (2016). *McCafee.* Kasutamise kuupäev: 18. aprill 2016. a., allikas http://www.mcafee.com/us/resources/reports/rp-threats-predictions-2016.pdf

Titlow, J. (15. mai 2012. a.). *Readwrite*. Kasutamise kuupäev: 14. aprill 2016. a., allikas http://readwrite.com/2011/05/15/despite-alternatives-microsoft-office-reigns/

Vallaste e-teatmik. (kuupäev puudub). Kasutamise kuupäev: 20. aprill 2016. a., allikas http://www.vallaste.ee/index.htm?Type=UserId&otsing=6692

webopedia. (kuupäev puudub). Kasutamise kuupäev: 4. aprill 2016. a., allikas http://www.webopedia.com/TERM/O/overwriting_virus.html

Summary

Title: Security-Conscious Software Choice in Educational Institution.

This Bachelor thesis focused in security-conscious software choices in education institutions that have been made by IT-specialists.

First, the author writes about different types of malware and explains their meaning. Secondly the author analyzes IT-specialists responses from the questionnaire. Briefly describes the three most widely used software and points out to their weak spots. The survey revealed that none of the IT-specialists did not mention security when selecting software. Thirdly demonstrates two types of the malware that have caused problems with the most used software in educational institution.

For exmaple software comfortibiliy or functions are much more valuable to IT-specialists than the actual security of the software. IT-security assurance and commitment is in fact a inseparable part of any IT-system and while choosing new software to use.

However, if you choose the software that is less vulnerable it ensures a higher security – that's the security concious software choice, and applies not only to educational institutions but for everyone. It is clear that security is not a state but a process throughout.