Tallinna Ülikool
Digitehnoloogia Instituut

ENAMLEVINUMAD INTERNETIPETTUSED

Referaat

Autorid: Krister Tarnamaa
Cleven Lehispuu
Indrek Kutsar
Teet Triisa

Tallinn 2017

Sisukord

Sissejuhatus

Tänapäeva maailm on tihedalt seotud internetiga ning sellega käsikäes käivate ohtudega. Internet on avanud iga inimese jaoks ukse tervesse maailma, tehes mugavamaks väga palju igapäevaseid toiminguid, mida varem polnud võimalik digitaalselt teha. Kahjuks kasutavad uut tehnoloogiat ära ka petturid. Seega peab igaüks, kes soovib olla osa internetist, tutvuma riskidega, mis interneti kasutamisega kaasas käivad ja õppima nendest hoiduma.

Käesoleva referaadi eesmärgiks on tuua välja erinevaid internetipettuse vorme ning anda ülevaade, kuidas need toimivad ning kuidas on neid võimalik arvutikasutajal tuvastada ja end nende eest kaitsta.

Töö koosneb kolmest peatükist. Referaadi esimene peatükk annab ülevaate ühest pettuse liigist, milleks on andmete õngitsemine. Teine peatükk keskendub pahavara programmidele ning läbi pahavaraprogrammide arengu on võimalik saada ülevaade, kuidas pahavara on saavutanud üha mastaapsemaid ja kahjustavamaid mõõtmeid. Kolmas peatükk keskendub sellisele internetipettuse vormile nagu loteriipettus, mis on arvutikasutajat psühholoogiliselt manipuleeriv pettuse vorm.

1 Phishing ehk õngitsemine

1.1 Mis on Phishing

Phishing on infoturbe termin, mis tuleneb inglise keelsest sõnast „kalastama“. *Phishing* ehk andmepüük on moodus arvutikasutajatelt välja petta isiklikku või finantsalast teavet petturlusega seotud e-posti sõnumit avades (tavaliselt manusena kaasalisatud faili avades või e-posti kirjaga oleval lingile vajutades), mis suunab kasutaja osavalt võltsitud internetileheküljele. Tavaline võrgus tegutsev andmepüüki kasutav pettur alustab e-kirja sõnumi saatmisega, mis sarnaneb usaldatud allikast (pank, krediitkaardiettevõte või tuntud veebikaubitseja) pärineva ametliku teatega. E-posti sõnumis suunatakse adressaadid petturlusega seotud veebileheküljele, mis näeb välja nagu õige lehekülg ning kus kasutajatel palutakse sisestada isiklikku teavet, nagu panga kontonumbreid või –paroole, isikukoode, telefoninumbreid, elukoha aadressi jne. Seda teavet kasutatakse tavaliselt identiteedi varguseks. (Priit, 2010)

Siiski on *phishing*ust võimalik hoiduda ning see tähendab, et arvutikasutaja peab olema teadlik selliste kirjade olemasolust. Järgnev peatükk annab ülevaate, kuidas on võimalik sellist õngitsemist ära tunda ning tulevasest kahjust seeläbi hoiduda.

1.2 Phishingu äratundmine

Phishingu e-maile on võimalik ära tunda mitmetest märkidest. Esimene asi, mida peaks alati kontrollima, oleks saatja. Kui tegemist on suurfirmaga, siis on see esimene asi, mida kontrollida. Pahatahtlikud saatjad võivad kasutada e-maile nagu: "Alerts@Paypal.co.uk". Kuna Paypal on firma, mis asetseb Ameerikas, on aru saada, et ei ole tegemist ametliku Paypal-iga, mille ametlik e-mail teadete jaoks on “Service@paypal.com”. *Phishingu* saatja e-mailid ei ole ka alati korralikud. Näiteks, kui e-mail on saadetud Ebay-st aadressiga “xzyspxt@hy.tk”, on koheselt arusaadav, et tegu ei ole ametliku lehega. (Mills, 2009)

Kui e-maili adressaadi järgi on raske tuvastada õngitsejat, siis on võimalik e-maili pöördumisest järeldada selle audentsust. *Phishing* e-mailid kasutavad peamiselt üleüldiseid fraase, nagu: “*Dear Customer/Subscriber*”, aga ametlikud firmad kasutavad kliendi eesnime või kasutajanime. (*ibid.*)

Kontrollida tuleb ka internetiaadresse saadetud e-mailis. Kuigi lingi järgi ei ole alati esmapilgul aru saada, kuid kui keskenduda, on võimalik leida vigu ka sealt. Enamus lehti kasutavad SSL protokolli, mis on mõeldud klientide kindlustamiseks, et kasutatakse ametlikke lehti. See tähendab seda, et lingis on näha "*https://"* lingi alguses. Ametlikudel linkidel nagu Paypal-il on brauseri aadressiribal roheliselt välja kirjutatud "*PayPal, Inc [US]*". Osad *phishing* e-mailidega tegelevad inimesed võivad ka üritada peita enda linke läbi lingi lühendamise. (Mills, 2009)

Kuigi õngitsemine on petturite poolt hästi läbimõeldud vorm internetipetturlusest, on võimalik ka tavakasutajana hoiduda selle lõksu langemisest.

1.3 Kuidas hoiduda Phishingust

Phishingust on võimalik hoiduda mitmetel viisidel. Alljärgnevalt tuuakse ära ühed peamised võimalused, kuidas vältida pettuse ohvriks langemist.

Pettust on võimalik vältida järgmiste võtetega (Mills, 2009):

- Oma e-maili ei tohi anda avalikel lehekülgedel välja.
- Tuleks kasutada e-maili aadressi, millel ei ole suur võimalus sattuda "*Spam"* nimekirjadesse. Näiteks: "Krister.Tarnamaa@gmail.com" asemel, kasutada hoopis "Krister.Tarnamaa_axy@gmail.com".
- Kui e-mail tundub kahtlane, siis kontakteeruge firma klienditoega isiklikult.
- Kui e-kirjas palutakse informatsiooni kinnitamist, siis tuleks kirjutada käsitsi aadressiribale firma internetiaadress, selle asemel, et e-kirjas lingi peale klikkida.
- Ei tohi välja jagada isiklikke andmeid, mis on küsitud e-maili kaudu. Ametlikud firmad kasutavad e-maili tavalise kommunikeerimise jaoks ja ei palu kunagi inimesel vahetada või kinnitada oma andmeid läbi e-maili lingile vajutades.
- Tuleb jälgida, et kasutatakse ohutuid lehti, kui saadetakse tundlikku rahanduslikku infot.
- Vahetada paroole tihedalt ja mitte kasutada sama parooli mitmel lehel.

Kokkuvõtvalt, *Phishing* on identiteedivargus. Nakatumine toimub sedasi, et pahaaimamatu kasutaja vajutab talle saadetud e-kirjas internetiaadressile ja seeläbi hakatakse otsekui õngitsedes arvutikasutaja isiklikke andmeid, mis varastatakse kasutajale visuaalselt peidetud programmide läbi, saatma kurjategijatele. Saadud infot ärakasutades on võimalik tekitada pettuse ohvrile ulatuslikku materiaalset kahju. Siiski on olemas levinud õpetused ja ettevaatusabinõud, et hoiduda sellisest pettasaamisest.

2 Pahavara

2.1 Mis on pahavara

Pahavara on üsna lai mõiste, mis kirjeldab erinevaid pahatahtlikke programme. Nende hulka kuuluvad trooja hobud, ussid, juurkomplektid, nuhkvarad, *ransomware*-viirused, erinevad küberohud ning ka potentsiaalselt soovimatud programmid (PUP-id). Pahavara laaditakse arvutisse tavaliselt kasutaja teadmata ja nõusolekuta, kasutades selleks turvaauke ja muid kuritegelikke meetmeid. Ainus, mis suudab võidelda pahavara rünnaku vastu, on uuendatud pahavaratõrje programm. Turvaeksperdid soovitavad tungivalt inimestel laadida usaldusväärne tõrjeprogramm, vältimaks pahavara rünnakuid. (Doevan, 2016; Milosevic, 2013)

Pahavaraprogrammid on tavaliselt arendatud välja selleks, et teha mingeid toiminguid arvutis, mis aitaksid programmi loojal raha teenida. Pahavara võib näiteks varastada isikuandmeid, nagu erinevate interneti lehekülgede sisselogimisandmed ja pangaandmed, või proovib programm lukustada olulised failid ning pressida failide omanikult välja raha failide lahti krüpteerimise eest. Mõned pahavaraprogrammid (nagu näiteks reklaamtarkvara või muu selline) on välja töötatud üksnes selleks, et näidata inimeste arvutites sponsoreeritud reklaame ning teenida klikkide pealt raha. Peaaegu kõikidel pahavaradel on võime blokeerida teatud turvatarkvarasid. Lisaks sellele suudavad need programmid end ise uuendada, laadida alla veelgi rohkem pahavaraprogramme ning tekitada nakatunud arvuti turvasüsteemi turvaauke. (Doevan, 2016)

Pahavara tegevus oleneb peamiselt pahatahtliku osalise eesmärkidest. Alljärgnevalt on loetletud sõltuvalt eesmärkidest pahavaralise programmi tegevused.

Hävitavad eesmärgid (Carnegie Mellon University, 1999):

- arvuti või seadme välja lülitamine;
- failide hävitamine või muutmine;
- andmete hävitus;
- antiviiruse blokeerimine;
- kõvaketaste sisu hävitamine;
- pahavara jaotamine üle võrgu.

Ressursside või identiteedi kasutuse-põhised eesmärgid (Carnegie Mellon University, 1999):

- masina kasutamine osa *botnet*ist;
- arvuti ressursside kasutamine krüptoraha kaevandamiseks;
- kasutades nakatunud arvutit, et teha seadusvastaseid tegusid või teiste arvutite ründamiseks;
- teiste ühendatud seadmete nakatamiseks.

Rahavarguse või väljapressimise eesmärgid (*ibid.*):

- pangakonto andmete varastamine;
- *ransomware* ehk väljapressimise põhine pahavaralise programmi installimine.

Andmete varguse eesmärgid (*ibid.*):

- tööstusspionaaž;
- kasutajate paroolid või pangakonto info;
- kasutaja isiklike andmete vargus;
- ärisaladuste vargus.

Spionaaž, jälgimine või jälitamise eesmärgid (*ibid.*):

- kirjutamise jälgimine;
- kasutaja ekraani jälgimine;
- kasutaja veebikaamera jälgimine;
- kasutaja arvutisüsteemi kaugjuhtimine.

Pahavara on kahjurvara, mis on üldnimetajaks sellistele programmidele, mille eesmärgiks on nii arvutitele kui ka nendes olevatele infosüsteemidele kahju teha ning mis hiljem kahjustab ka kaudselt pettuse ohvrit. Pahavara programmid võivad arvuteid rivist välja lüüa ning ka kasutaja andmeid varastada ning enamjaolt on sellised programmid loodud nii, et tegutsevad arvutites nende kasutaja teadmata.

2.2 Pahavara areng ja ajalugu

Pahavara ajalugu võib jagada mitmesse kategooriasse, mis kajastab ajavahemikku selle kategooria sündmuste algusest ning seeläbi on võimalik jagada pahavara ajalugu viide kategooriasse. Selles alapeatükis kirjeldatakse pahavara arengut nendes viies etapis.

Esimene kategooria on varajane pahavara faas. See on aeg, mil esimesed pahavaralised programmid loodi. Teine etapp on varajane Windowsi faas. See kirjeldab esmakordselt Windowsi pahavara programme, nagu esimest e-kirja ussi ja makrousse. Kolmas kategooria on võrguusside areng. Need ohud muutusid just sel ajal populaarseks, kui internet levis üha laialdasemalt. Neljas osa on *rootkit*id ehk käomunad ja *ransomware*id ehk väljapressimise pahavarad. Need olid kõige ohtlikumad pahavarad enne 2010. aastat. Seejärel, viiendana, tuli pahavara, mis tehti virtuaalseks spionaažiks ja sabotaažiks ning selliseid pahavarasid on loonud mõnede riikide salateenistused. Viimase pahavara evolutsiooni faasiga oleme ka praegu silmitsi seismas. (Milosevic, 2013)

1986. aastal ilmus esmakordselt pahavara arvutisse. See oli viirus nimega Brain. A. Brain. A töötati välja Pakistanis, kahe venna poolt - Basit ja Amjad. Nad tahtsid tõestada, et arvuti ei ole turvaline platvorm, nii et nad lõid viiruse, mis kopeerib ümbrikkettaid ehk flopidiske. See nakatas iga flopiseadme käivitava sektori ja iga sisestatud käivitamissektori. Selle pahavara käivitamiseks tuli nakatunud flopiketas sisestada arvutisse, mis nakatas selle flopiseadme lugeja, nii et seade nakatas omakorda järgmine kord sisestatud uue flopiketta. See viirus aga ei kahjustanud tegelikult seadet, vaid autorid allkirjastasid koodi koos oma telefoninumbrite ja aadressiga, eesmärgiga osutada tähelepanu probleemidele, ning mitte teha kahju inimestele või kahjustusi riistvarale. (Milosevic, 2013, lk 58) Kuid hiljem muidugi pahavara muutus järjest rohkem hävitavaks.

Pärast Brain, A. oli ka teisi viiruseid. Üks huvitavamaid oli Omega viirus. Seda nimetati Omega viiruseks oomega märgi tõttu, mida ta arvuti kasutajaliidesel ehk konsoolis kirjutas teatud tingimustel. See nakatas alglaadimissektori, kuid ei tekitanud palju kahju, väljaarvatud kui oli 13. kuupäev ja reede. Sellel päeval arvuti ei suutnud käivituda. Michelangelo viirus näiteks pidi Michelangelo sünnipäeval aastal 1992

ümber kirjutama esimese 100 kõvaketta sektorit. Seda tehes hävitati failide jaotamise tabel ja arvuti ei saanud käivituda. Selle sama kategooria all olev V-märk oli viirus, mis nakatas ka algkäivitussektori ja kirjutas iga kuu V-märgi ekraanile. Walker on järgmine viirus, mis oli üsna visuaalne ja ilmus 1992. aastal. See oli animeeritud kujutis vanemast mehest, kes kõndis ühest ekraani küljest teise. (Milosevic, 2013, lk 59)

Järgmine suur samm pahavara evolutsioonis oli mutatsioonimootori (MtE) juurutamine. Mutatsioonimootor loodi Bulgaaria häkkeri poolt, kes kutsus ennast Dark Avengeriks. See oli tööriist, mis võis viirustele lisada mutatsioonifunktsioone, nii et neid oleks viirusetõrjete abil raskem tuvastada. Põhimõtteliselt oli see esimene polümorfismimoodul, mis võis viirusega kokku puutuda ja muuta seda nähtamatuks. Viiruse loomise labor oligi esimene kasutajaliides viiruste loomiseks. Kasutaja võis valida viiruse omadusi ja luua seda. See tegi viiruse loomise lihtsaks. Sellel olid mõningad puudused, kuid peaaegu igaüks, kes seda GUI-tööriista kasutas, võis luua viiruse. (*ibid.*)

Kui Windows välja tuli, oli see paljudele kasutajatele huvitav, sest see andis võimsa kasutajaliidese. Selle kasutuslihtsus meelitas paljusid kasutajaid. Teise kategooria viiruseks oli WinVir, mis oli esimene Microsoft Windowsi viirus. See ei kahjustanud programmi ulatuslikult, vaid selle peamine omadus oli see, et see paljunes ja et see oli esimene viirus, millel oli võime nakatada Windows PE (*Portable Executable*) faile. Boza oli selle Windowsi faasi üks esimene viirus, mis oli spetsiaalselt kirjutatud Windows 95-le. See nakatas Portable EXE-faile – et ehk faile, mis kasutasid Windows 95 ja Windows NT-d. Happy99 oli aga esimene Windowsi etapi e-posti viirus. See levitas e-kirja manusena käivitusfaili ja see pahavara tuvastati 1998. aastal. Sel ajal olid rämpsposti filtrid vaevu olemas ja võimaldasid saata käivitusfaile. Kui kasutaja klõpsas ja käivitas manuse, kuvati talle ilutulestikuga ekraan, kuid viirus samuti paljundas kirja manuse ja saatis kirja kõigile kasutaja kontaktidele. (Milosevic, 2013, lk 59) Melissa oli viirus, mis kombineeris makroviiruse ja e-kirjaviiruse võtteid. See oli nakatunud MS Wordi failiga kaasas. Kui fail avanes, kopeeriti see kasutaja kettale juhuslikult valitud dokumendile ja saatis selle kõigile kontaktidele. See oli teabe lekke tõttu üsna probleemne pahavara. (Skoudis & Zeltser, 2004, lk 18)

1980ndate lõpus loodi kogemata esimene PC-uss, mida võis pidada pahavara arengu kolmandaks etapiks. 1988. aastal kirjutas MITi üliõpilane Robert Tappan Morris programmi, mis oli suureks muutvaks sündmuseks pahavara ajaloos. Osana oma projektist soovis Morris loendada internetiga ühendatud arvuteid. Nii kirjutas ta väikese programmi, mis paljuneks ühest ühendatud arvutist teise ja loendaks arvuteid. Aga Morris tegi vea, uss külastas ka neid arvuteid, mida ta juba varem oli külastanud. Tegelikult levitas see uss nakatunud arvutist kõigile teistele ühendatud arvutitele kogu aeg viirust ja see tekitas palju võrguliiklust ja sellel ajal peaaegu tekitas internetiliikluses hävingu. (Milosevic, 2013, lk 62) Interneti algusajal ei arvanud keegi eriti midagi interneti turvalisusest ning see võimaldaski Morrisel oma ussi-katsetusi teha.

Neljas etapp pahavara ajaloos on *RootKit* ehk pahavara tööriistad, mis muudavad olemasolevat operatsioonisüsteemi tarkvara nii, et ründaja suudab masinale saada juurdepääsu ja end peita (Milosevic, 2013, lk 64). Esimene *RootKit* tehti kunagi SONY Entertainment poolt ja sellel oli üsna halb mõju SONY mainele hiljem. SONY BMG RootKit sündis 2005. aastal, kui SONY käis välja idee oma väljaannete autoriõiguse kaitsmiseks. Neil oli idee avastada ja keelata nende publikatsioonide kasutamist selle *RootKit*i kaudu teistele meediatele. (Skoudis & Zeltser, 2004, lk 305)

2010. aastal toimus üks suur samm pahavara arengus, mis tõi ilmale viienda etapi pahavara programmide ajaloos. Pahavara ei nähtud enam kui kõigest ohtu äridele, isiklikele rahalistele vahenditele või isiklikele failidele, vaid ka paljude riikide sõjaväe- ja politseiteenistused ning salajased asutused kaasati pahavara loomisesse. Pahavara saab nüüdsel ajal näha sarnaselt mistahes muu relvana. Samuti võib pahavara tekitada pommiga peaaegu sama kahju, kuigi ei ohusta inimelusid. Selle parimaks näiteks on Stuxnet pahavara, mis avastati 2010. aasta suvel. Stuxnet loodi Iraani tuumaprogrammi hävitamiseks või vähemalt aeglasemaks muutmiseks ning mis levis arvutisse ja paljunes siis USB-seadeldistele. Stuxnet füüsiliselt rikkus uraani rikastamiseks turbiine, muutes selle pöörlemissagedusi. (Milosevic, 2013, lk 66-67)

Nagu näha, on pahavaraliste programmide täpsustamiseks mitu võimalust. Seda võib liigitada selle käitumisviiside järgi. Samuti selle järgi, kuidas see ühest süsteemist teise edastatakse. (Messier, 2016, lk 269) Kokkuvõtvalt on olemas mõned tuntud

kategooriad tänapäeval, mida tavaliselt pahavara kirjeldamiseks kasutatakse ja nendest annab ülevaate järgmine peatükk.

2.3 Erinevad pahavara tüübid tänapäeval

2.3.1 Viirus

Arvutiviirus ehk viirus on programm, mis on võimeline end iseseisvalt kopeerima ning arvutit nakatama. Viirused suudavad suurendada oma levimisefektiivsust, nakatades võrgus paiknevaid või teise arvuti poolt sagedasti kasutatavaid failisüsteeme. (Vikipeedia, 2017)

Eelmainitult mõistetakse termini „viirus“ all ekslikult ka muud tüüpi, ka isepaljunemisvõimeta pahavaraprogrammide puhul, näiteks reklaam, nuhkvara, ussid või trooja hobused. Ussviirused kasutavad ära süsteemis leiduvaid turvaauke, et end võrgu kaudu, võrku lülitatud arvutist uutesse arvutitesse levitada. Ehtne viirus levib ühest arvutist teise nakatunud peremees-programmi ümbertõstmisel. Selline levimine toimub näiteks failide saatmisel üle võrgu ja interneti või nende transportimisel erinevate andmekandjatega, nt CD, DVD ja USB-mälupulk. (*ibid.*)

Kui ühtede pahavaraprogrammide tegevusel tekivad kasutajale märgatavad sümptomid, siis teised tegutsevad süsteemis kahtlust äratamata.

2.3.2 Trojan

Trojan-iks nimetatakse ükskõik missugust pahatahtelist rakendust, mida kasutatakse arvutile ligipääsusaamiseks kasutajale valetades selle tõelisest eesmärgist. Trojaneid levitatakse üldiselt läbi e-maili manuste või internetist alla laadides faile, mis tunduvad ohutud. Enamus trojaneid töötavad uksena, mis lubab pahatahtlikul inimesel saada ligipääsu nakatanu arvutile ning sealhulgas ka nende finantsandmetele, paroolidele kui ka identiteedile. (Carnegie Mellon University, 1999)

2.3.3 Bot ja Botnet

Üldiselt, *bot* on tarkvara, mis täidab automatiseeritud ülesandeid. Palju *bot*-te võib olla aga hoopis abistava eesmärgiga, näiteks *bot*-id kihavad läbi interneti, indekseerides

veebilehti otsingumootorite jaoks või jutu-*bot* firma veebilehel vastab kliendi tekkinud küsimustele (Harvey, 2017)

Botnet-iks nimetatakse arvutite kogumit, mis on nakatanud viirusega, mis laseb pahatahtlikul isikul juhtida eelnimetatud kogumit pahatahtlikuks tegudeks. Nendeks tegudeks on DoS rünnakud (*Denial of Service attacks*), rämpsposti saatmiseks, digirahanduste kaevandamiseks ja andmevarguseks. Iga nakatunud arvutit nimetatakse *bot*-iks, mida on võimalik kontrollida läbi spetsiifilise rakenduse, mis annab nakatajal võimaluse jälgida ja juhtida arvuti võrguliiklust ja ligipääsu arvuti andmetele. *Botnet*id on levivad viirused, mis võivad üle võrgu võtta juhtimise üle ka teistelt arvutitelt. (Ramneek, 2003)

2.3.4 Reklaamvara

Paljudele inimestele ei meeldi reklaamid ning nendega ollakse ka põhimõtteliselt ära harjunud ja seeläbi on inimesel välja arenenud midagi, mida kutsutakse bänneripimeduseks, mis sisuliselt peatab inimest neid interneti lehekülgedel olevaid reklaame märkamast. Reklaamijad teavad seda ning nad üritavad oma reklaame teha aina enam meeldejäävamaks ning väljapaistavamaks, seda sellepärast, et saada kasutajatelt tähelepanu. Kahjuks osad reklaamijad ei lahenda seda probleemi enda reklaamide paremaks muutmisega, vaid kasutavad selleks reklaamvara. (Cucu, 2017)

Reklaamvara on sellist tüüpi pahavara, mis tõmbab alla või kuvab seadme kasutajale reklaame. Tavaliselt see ei varasta süsteemist andmeid, vaid on rohkem ärritav, kuna see sunnib kasutaja reklaame vaatama, mida nad parema meelega oma süsteemis näha ei tahaks. Osad eriti ärritavad vormid genereerivad veebilehitseja hüpikaknaid või reklaamaknaid, mida ei saa kinni panna. Kasutajad tavaliselt nakatavad enda arvuteid enese teadmata sellist sorti pahavaraga kui nad laevad alla ning paigaldavad teisi rakendusi, mis vaikimisi paigaldavad ka reklaamvara. (Harvey, 2017)

2.3.5 Lunavara

Lunavara on pahavara, mis lukustab kasutaja klaviatuuri või arvuti, eesmärgiga takistada juurdepääs failidele ning andmetele, seniks kuni kasutaja maksab lunaraha, mis on tavaliselt nõutud krüptorahas. Selline digitaalne väljapressimise skeem pole

midagi uut, seda on kasutatud alates 2005. aastast. Sellest ajast on ründajad kõvasti arendanud oma skeemi ning välja arendanud krüptovara, mis krüpteerib kasutaja failid kasutades privaatset võtit, mida ainult ründaja valdab, selle asemel, et lihtsalt arvuti kasutust piirata. Tänapäeval lunavara ei ohusta ainult laua- ja sülearvuteid, vaid ka nutiseadmeid. (Zetter, 2017)

On ka teist vormi lunavara, mis otseselt arvutit ei ohusta, vaid ainult ähvardab, kas arvutit rünnata või kasutaja kohta piinlikku informatsiooni avalikustada, kui kasutaja lunaraha maksmisest keeldub. (Harvey, 2017)

2.3.6 Nuhkvara

Nuhkvara on tarkvara, mis on paigaldatud arvuti seadmesse ilma lõppkasutaja teadmiseta. Kas selline tarkvara on pahavara, on vaieldav, kuna seda paigaldatakse ka ohututel eesmärkidel, kuid see võib ohustada lõppkasutaja privaatsust ning seda ka ära kasutada. (Rouse, 2016)

Nuhkvara, mis on paigaldatud mitte pahatahtlikel eesmärkidel, võidakse ka vahel kutsuda jälgimisvaraks. Näiteks töökohtades võib selline tarkvara olla paigaldatud korporatsiooni arvutitesse, eesmärgiga jälgida töötaja tegevusi. Samuti ka näiteks kodus, vanemad võivad kasutada jälgimisvara oma lapse internetitegevuste jälgimiseks. Veel ka reklaamijad, kes uurivad kasutaja internetilehitseja küpsiseid, jälgides millistel lehtedel kasutaja käib ning saadud informatsiooniga suunata kasutajale reklaame. Kuid rakendused, kus kasutajale teavitatakse, et tema andmeid kogutakse, ei vaadelda kui nuhkvara. (Rouse, 2016)

Kuritahtlikult saab nuhkvaraga näiteks salvestada klahvivajutusi, sellist sorti nuhkvara nimetatakse klahvinuhiks. Sellist sorti nuhkvara kasutatakse paroolide kogumiseks ja kommunikatsioonide pealt kuulamiseks. Veel ka varastada krediitkaardi informatsiooni või muid pangaandmeid. (Lemonnier, 2015)

3 Loteriipettus

3.1 Mis on loteriipettus

Loteriipettuse elektroonilise kuju tüüpiliseks petuskeemiks on inimese e-postkasti, telefoni sõnumitesse või sotsiaalmeedia sõnumitesse saabunud kiri, milles teavitatakse teda konkursi või loterii võidust, millest ohver teadlikult osa ei ole võtnud. Tegemist on tihtipeale *advance*- tasu tüüpi pettustega, mis tähendab seda, et pettusena lubatud raha kätte saamiseks on ohvril vaja teha omapoolseid kulutusi. Nende kulutuste vabandusteks tuuakse tihtipeale näiteks asjaajamis-, posti-, kindlustuskulude katmine või riigilõivu tasumine. Antud kulude tasumisele ei järgne reeglina kunagi lubatud võitusummat, vaid vabandused ja uued kulutused. (Australian Competition & Consumer Commission, kuupäev puudub)

Ohvri omapoolsete kulutuste asemel või nendega koos võivad petturid küsida ka personaalseid andmeid kinnitamiseks, et tegu on ikka õige võitjaga ja pangakonto andmeid, et oleks võimalik saata raha. Neid andmeid kasutades proovivad petturid sooritada identiteedivargust, et pääseda ligi ohvri pangakontole. (*ibid.*)

3.2 Loteriipettuse äratundmine

Loteriipettuse puhul peaks internetikasutaja või e-kirja lugeja, kes on saanud sellekohase teate, hoiduma pettuse ohvriks langemiseks, kasutades ära mitmeid võimalusi. Esiteks, kui pole ostetud piletit või pole kuidagi muudmoodi sisenenud kuskile võistlusele, siis pole reeglina ka võimalik võita. (Spamlaws.com, n.d.)

Petturid võivad küsida ohvrilt ettemaksu erinevate võiduga kaasnevate kulude katmiseks. Tegelikult võtavad ehtsad loteriid kõik võiduga kaasnevad kulutused lihtsalt võidusummast maha. Need ettemaksud ongi peamine viis, kuidas petturid raha teenivad. (Wikipedia, 2016)

Petturid saadavad tihtipeale kirju, kasutades tasuta e-postiteenuseid nagu Outlook, Yahoo!, Hotmail, Live, MSN, Gmail jne. (*ibid.*)

3.3 Kuidas hoiduda loteriipettusest

Et mitte langeda loteriipettuse ohvriks, on oluline pidada kinni teatud ohutust tagavatest reeglitest (Bureau of Consular Affairs, U.S. Department of State, n.d.):

- Kui saadud teates nõutakse raha ette, siis on tegemist peaaegu alati pettusega.
- Tuleb olla ettevaatlik telefoninumbritega, mis e-kirjatsi saabuvad. Need võivad olla välismaa tasulised telefoninumbrid, mille hinnast tihtipeale ette ei hoiatata.
- Kõik kasutajatingimused ja reeglid tasub hoolega läbi lugeda enne nendega nõustumist. Tehingud, mis tunduvad liiga head, võivad sisaldada lisatasusid, mis võivad esialgu kasutajale kahe silma vahele jääda.
- Pakkumise õigsust tuleks kontrollida kasutades veebiotsingut. Ei tohiks kasutada e-kirjas sisalduvaid kontaktandmeid, sest need võivad olla ohtlikud. Otsingus tuleks kasutada samu nimesid ja sisus esinevaid fraase, mis on kontrollitavas kirjas. Kui tegemist on levinud pettusega, siis on see internetis kindlasti arutusel.
- Kui on kahtlust, et saabunud kiri on pettus, siis tuleks see kiri lihtsalt ära kustutada ja mitte sellega enam rohkem tegemist teha. Mitte mingil juhul ei tohiks saata raha, personaalseid andmeid ega dokumente.
- Petturitega tuleb ka hoiduda füüsiliselt kokkusaamisest, sest see võib olla ohtlik.

Et loteriipettusest hoiduda, tuleks tähele panna mitmeid ohutust tagavaid abinõusid. Kunagi ei ole loteriipettusel seost ausate firmadega, mille identiteedi varastamisega püütakse tegutseda. Sellise petmisskeemi puhul küsitakse alati rahalist summat, et hüvitada võidusaatmise kulud, kuid selline võte ei ole kunagi omane ausatele loteriid korraldavatele organisatsioonidele. Et sellisest internetipettusest hoiduda, on võimalik saadetud lotovõidu andnud organisatsiooni kontrollida läbi interneti otsingumootorite.

Kokkuvõte

Internetiohutus sõltub suuresti meist endist. Interneti mõnude nautimisega kaasneb ka kohustus olla asjatundlik ja ettevaatlik kasutaja, et kõigi isiklikud andmed oleksid kaitstud. Isiklike andmetega peab olema äärmiselt hoolas, sest on võimalus, et iga hetk jälgitakse kasutaja trükkimist või saadetakse kogemata pahatahtlikele isikutele olulisi isiklikke andmeid. Identiteedivargus ja ärakasutamine on väga sagedased juhtumid. Ettevaatlikkus ja asjatundlikkus on ainsad viisid hoiduda nendest ohtudest.

Pärast esimese pahavara levikut on möödas rohkem kui 25 aastat. Pahavara on küll läbi aja muutunud, kuid mõned põhimõtted on jäänud samaks. Esimene pahavaraviirus Brain A. levis diskettide läbi ning Stuxnet - üks keerukamaid pahavaraprogramme – levis üle USB-seadeldiste. Pahavara loomise eesmärgid ja motiivid muutusid kõigest väljapaistvast humoorikast naljast kättemaksu ja kasumit taotlevaks spionaažiks ja sabotaažiks. Kasum on endiselt suur motivaator pahavara loomiseks ja see jääb sedasi ka ilmselt tulevikus. Sõjaliste eesmärkide loomine, nagu spionaaž ja sabotaaž, on pahavara loojatel tänapäeval õnnestunud. Ilmselt võime tulevikus oodata rohkem sõjalisi pahavara ja küberrünnakuid, sest see on ründajatele üsna turvaline ja võib põhjustada sama kahju kui sõjalised rünnakud. Tuleb näha, kuidas viirusetõrjeloojad tegelevad selliste ründajatega, kellel on ühest küljest peaaegu piiramatud ressursid pahavara loomiseks ja mis on ka kasumlikud loojatele.

Kokkuvõtvalt, pahavara võib rünnata kõikjal ja kõikides operatsioonisüsteemides. Külastatud veebilehtede turvalisuse pidev jälgimine ja hoidumine interneti kahtlastest nurkadest ei jäta petturitele võimalust privaatsetele andmetele ligipääseda, seda nii tavakasutajatel, ettevõtetes kui riigikaitsesüsteemide puhul. Lisaturvameetmena peaks iga korralik internetikasutaja olema varustatud tõhusa antiviiruse tarkvaraga ja kasutama vaid ajakohaseid viirusetõrje programme.

Kasutatud kirjandus

Australian Competition & Consumer Commission. (kuupäev puudub). *Unexpected prize & lottery scams*. Kasutamise kuupäev: 20. March 2017. a., allikas ScamWatch: https://www.scamwatch.gov.au/types-of-scams/unexpected-winnings/unexpected-prize-lottery-scams

Bureau of Consular Affairs, U.S. Department of State. (n.d.). *International Financial Scams*. Retrieved March 20, 2017, from U.S. Passports & International Travel: https://travel.state.gov/content/passports/en/emergencies/scams.html

Carnegie Mellon University. (1999, March 8). *Trojan Horses*. Retrieved March 20, 2017, from CERT: http://www.cert.org/historical/advisories/CA-1999-02.cfm

Cucu, P. (9. mai 2017. a.). *Adware: Definition and Removal Guide*. Allikas: Heimdalsecurity: https://heimdalsecurity.com/blog/adware-definition-removal/

Doevan, J. (24. 10 2016. a.). *Pahavara*. Allikas: Viirused: http://viirused.ee/pahavara/

Harvey, C. (4. april 2017. a.). *Different Types of Malware and How to Defend Against Them* . Allikas: Esecurityplaneti veebisait: https://www.esecurityplanet.com/malware/malware-types.html

Lemonnier, J. (6. juuni 2015. a.). *What is Spyware?* Allikas: avg: https://www.avg.com/en/signal/what-is-spyware

Messier, R. (2016). *Operating System Forensics.* Waltham: Syngress.

Mills, E. (2009, November 17). *How to recognize phishing e-mails*. Retrieved March 20, 2017, from cnet: https://www.cnet.com/how-to/how-to-recognize-phishing-e-mails/

Milosevic, N. (8 2013. a.). History of Malware. *Digital forensics magazine, 1*(16), 58-66.

Priit. (14. February 2010. a.). *Mis on Õngitsemine ehk Phishing*. Kasutamise kuupäev: 20. March 2017. a., allikas Arvutiturve: https://arvutiturve.wordpress.com/2010/02/14/mis-on-ongitsemine/

Ramneek, P. (2003, August 8). *Bots & Botnet: An Overview*. Retrieved March 20, 2017, from SANS Institute: http://www.sans.org/reading-room/whitepapers/malicious/bots-botnet-overview-1299

Rouse, M. (september 2016. a.). *Spyware*. Allikas: Techtarget: http://searchsecurity.techtarget.com/definition/spyware

Skoudis, E., & Zeltser, L. (2004). *Malware: Fighting Malicious Code.* Upper Sadle River: Prentice Hall Professional.

Spamlaws.com. (n.d.). *The Rundown on Lottery Scams*. Retrieved March 20, 2017, from Spam Laws: http://www.spamlaws.com/lottery-scams.html

Vikipeedia. (10. March 2017. a.). *Arvutiviirus*. Kasutamise kuupäev: 20. March 2017. a., allikas Vikipeedia: https://et.wikipedia.org/wiki/Arvutiviirus

Wikipedia. (17. November 2016. a.). *Lottery scam*. Kasutamise kuupäev: 20. March 2017. a., allikas Wikipedia: https://en.wikipedia.org/wiki/Lottery_scam

Zetter, K. (14. mai 2017. a.). *What is randomware? A guide to the global cyberattack's scary method.* Allikas: Wired: https://www.wired.com/2017/05/hacker-lexicon-guide-ransomware-scary-hack-thats-rise/