

Kaitse oma arvutit!

Ettekande koostas: Eha Kask

*Kasutatud materjal:
Arvutikaitse ABC
(Aare Kirna)*

Sisukord

- Arvutikaitse
- Botnet
- Brauserikaaperdajad
- DDoS
- Helistajad
- Hüpikaken
- ID kaart ja Mobiil ID
- Klahvinuhk
- Krüpteerimine
- Küberkuritegevus
- Küpsised
- Lunavara
- Nuhkvara
- Näotustamine
- Pahavara
- Paroolid
Paroolihaldus
- Piraatlus
- Privaatlus
- Reklaamvara
- Rootkit
- Rämpspost
- Seadused
- Sinihammas
Zombi
- Tagauks
- Trikitamine
- Troojalased
- Tulemüür
- Turvaaugud
- USB
- Ussid
- Vahemeherünnak
- Varukoopia
- Veebilehitseja
- Viirused
- Viirustõrje
- VoIP
- Võrgu kaitsmine
- WiFi
- Õngitsemine
- Kaitse oma arvutit!

Sissejuhatus

Maailm muutub ja internet ei ole ammu enam turvaline paik. Millised ohud varitsevad arvutikasutajat internetis? Ja mida nende ohtude vastu ette võtta?

Ettekanne on koostatud raamatu Arvutikaitse ABC, (autor Aare Kirna) põhjal. See on mõeldud kõigile, kes otsivad neile küsimustele kiireid vastuseid.

Antud raamat on valminud sihtasutuse Vaata Maailma projekti Arvutikaitse 2009 raames ning seda toetavad mitu väljapaistvat Eesti ettevõtet ja riigiasutust.

Arvutikaitse

Miks on oluline kaitsta oma arvutit ja kõike, mis selles leidub?

Arvuti ja andmed selle sees on täpselt samasugune vara nagu teie kodu, auto, stereokombain ja CD-d.

Keegi ei pea imelikuks, et kodust lahkudes suletakse aknad ja lukustatakse uks, samuti ei jäeta autot lahtiste akende ja väljalülitatud signalisatsiooniga maja ette seisma. Ometi teevad paljud hooletud arvutikasutajad oma arvuti ja võrguühendusega piltlikult öeldes sedasama.



Arvutikaitse

Ei tasu lohutada end mõttega, et see, mis teile kuulub, pole nagunii kuigi väärtuslik ning ei peaks kedagi huvitama. Ka see, kui keegi teie ukse hingedelt maha tõstab, akna puruks lööb, külmkapist toitu näksib või poriste saabastega voodis trambib, on küllaltki ebameeldiv. Ja tõenäoliselt ei taha te hoopiski, et keegi teie magamistoa aknast sisse piilub ning nähtud intiimseid detaile kogu külale kirjeldab.

Arvutikaitse

Kaitsmata arvuti piltlikult öeldes paraku seda kõike võimaldab. Enamgi veel, teie arvutit ja internetiühendust võidakse teie teadmata kasutada rünnakuteks teiste arvutiomanike vara ja hea nime vastu, rämpsposti ja pahavara laialisaatmiseks või pornopiltide vahelaona.

Arvutikaitse

- Kahjuks ei ole lihtsat ja universaalset vahendit, mis lahendaks kõik arvutikasutaja turvaprobleemid. Küll aga on olemas targad turvarakendused ja äraproovitud käitumisprotseduurid, mis koos terve talupojamõistusega aitavad tõhusalt vältida enamikku internetis valitsevaid ohtusid

Botnet

Botnetiks ehk **robotvõrguks** (robot network) nimetatakse **küberkurjategijate kontrollitavat arvutikogumit**, mis, samal ajal kui arvutite omanikud mängivad, surfavad või muid igapäevaseid toimetusi teevad, pommitab mõnd veebiserverit tühiste päringutega, serveerib porno- või piraattarkvarakollektsiooni, nakatab uusi arvuteid ja saadab laiali spämmi.

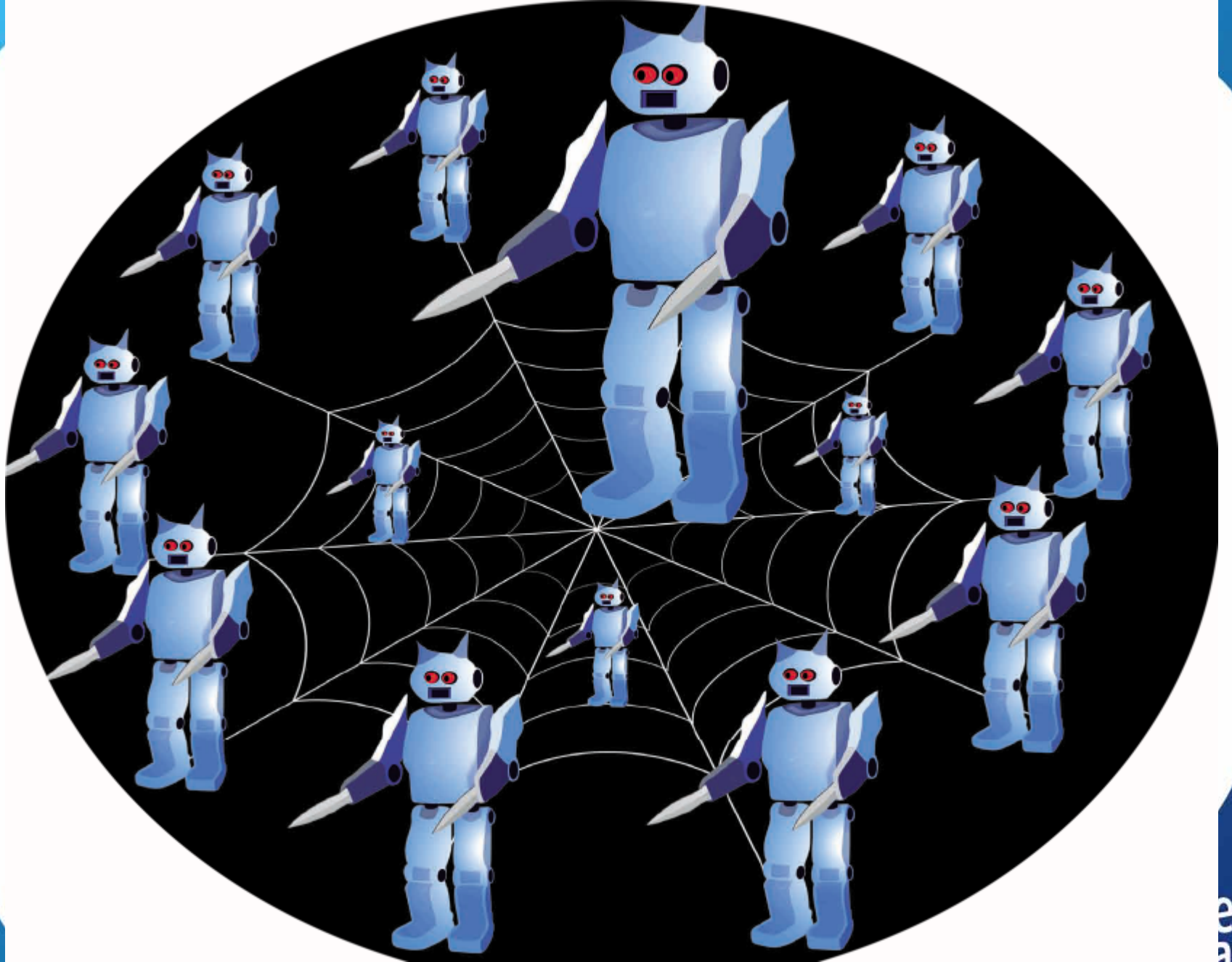
Botnet

Kontrolli alla saamiseks rünnatakse arvutit mõne turvaaugu kaudu (eriti kui arvutis on vananenud ja paikamata tarkvara), sagedamini aga pahavara abil, mis satub teie arvutisse kas kiirsuhtlusprogrammi või elektronposti kaudu või siis kuritahtlikke veebilehti külastades.

Kui operatsioonisüsteemil on sisse lülitatud mingisugusedki turvaseaded, vajab pahavara arvutisse installeerumiseks kasutaja otsest kaasabi, nii et enne „**Yes**” või „**OK**” nupu vajutamist on alati kasulik lähemalt uurida, millega nõus ollakse.

Botnet

Botnetti võib kuuluda miljoneid arvuteid, niinimetatud zombisid, viimasel ajal aga näivad kurjategijad eelistavat väiksemaid ja ohutumaid, paarikümnest tuhandest arvutist koosnevaid botnette, millest piisab täiesti sihitud rünnaku jaoks. Üldiselt arvatakse, et iga neljas 600 miljonist internetti ühendatud arvutist võib kuuluda mõnda botnetti.



Brauserikaaperdajad

Liik pahavara, mis vahetab veebilehitseja stardi- või otsingulehekülje, nii et teie vaikeleheküljeks seatud www.neti.ee või www.google.com asemel avatakse brauseri käivitamisel mõni kahtlane otsingumootor või pornolehekülg.

Eesmärgiks on kas teenida tolle pornolehekülje külastuste pealt rohkem reklaamitulu või siis suunata kasutajaid pahavara levitavatele lehekülgedele.

Brauserikaaperdajad

- Brauserikaaperdajad (*browser hijackers*) võivad olla väga tüütud, pahatihti ei piisa kaaperdatud lehekülgedest lahtisaamiseks veebisirvija seadete muutmisest
- – pärast taaskäivitamist on soovimatud stardileheküljed jälle tagasi. Mõnikord on seesugusest pahavarast lahtisaamiseks lisaks pahavara kustutamisele vaja muuta ka Windowsi registrit.

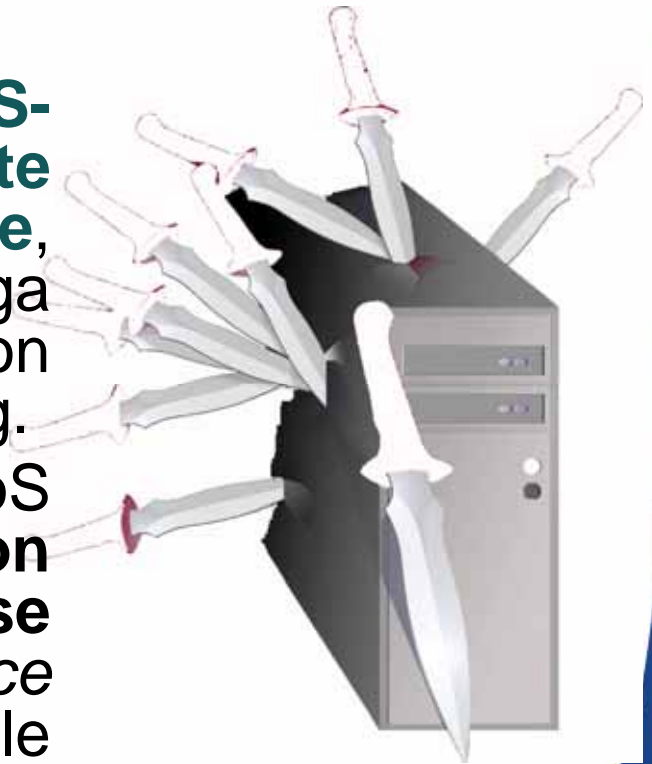
Brauserikaaperdajad

- **Kasutatakse ka kaaperdamistehnikaid, mis ei luba surfajal pornoleheküljelt lahkuda.** Seda tehakse kas järjest lahtiklõpsuvate hüpinkakendega või siis taaskäivitatakse lehekülge aknas, mida ei saa sulgeda (käivitatakse eraldi rakendus, milles juhtimismenüüd pole kättesaadavad).
- Sellegi eesmärgiks on teenida küllastajate pikema leheküljel viibimise pealt rohkem reklaamitulu.



DoS ja DDoS

- *Denial of Service* ehk **DoS-rünnakuga koormatakse ettevõtte internetiliiklust korraldav seade**, kas server või ruuter, üle suure hulga päringutega, milleks tavaliselt on võrguliikluse standardne *ping*-päring.
- **Koduarvuti omanikku DoS tavaliselt ei ähvarda. Parim rohi on alarmeerida oma internetiteenuse pakkujat** (ISP, *Internet Service Porvider*, on firma, kellele serveriomanik internetiühenduse eest maksab).



Helistajad



Helistajad

- **Pahavara, mis muudab arvuti sissehelistamisteenuse seadeid.** Tavaliselt nii, et eelnevalt seadistatud internetiühenduse pakkuja asemel helistatakse mõnele kõrge minutitariifiga numbrile, mille pealt küberkurjam saab oma protsendi.
- Helistajad olid levinud kümmekond aastat tagasi, kuid püsiühenduste valdavaks muutumisel on jäänud haruldaseks. **Uus helistamispahavara laine ähvardab neid, kes ühenduvad internetti mobiiltelefoniga.**

Helistajad

- Otseselt tavakasutajaid kahjustavate helistajate kõrval on häkkerid kasutanud ka programme, mis helistavad läbi teatud numbrivahemiku, näiteks kõik +372 algavad numbrid, et leida mitteavalikel numbritel vastavaid modemeid, fakse või muid võrguteenuseid.
- **Eraldi kategooria on helistamistarkvara, mida kasutatakse selleks, et raadiomängudes paremini telefoniliinile pääseda. Viirustõrje saab helistamispahavarast enamasti probleemideta jagu.**

Hüpikaken

Eraldi brauseriaken (*popup window*), mis hüppab lahti siis, kui külastate teatud veebilehekülgi, ja üritab reklaami näidata.

Hüpikakende eesmärgiks on pikendada konkreetsel leheküljel viibimise aega (mõnikord kasutatakse selleks brauseri põhiakna all avanevat akent, mida kasutaja märkab alles siis, kui pealmise akna kinni paneb) ning **teenida rohkem reklaamitulu**. Aastast 2004 on hüpikakende blokeerijad kõigisse enamlevinud brauseritesse

Mitte kõik hüpikaknad pole ebameeldivad ega pahatahtlikud – paljud koduleheküljed pakuvad teile hüpikakende abil lisainformatsiooni, abitekste ja muud kasulikku teavet. Intelligentsemad brauserid neid ka tavaliselt ei blokeeri.



ID-kaart ja Mobiil-ID

Kiipkaart, millele lisaks pealetrükitud, visuaalselt identifitseerivatele andmetele (pilt, nimi, sünniaeg, isikukood jms) on salvestatud ka teie elektrooniline identiteet: autentimis- ja allkirjastamissertifikaat koos salajaste võtmetega.

Elektroonilist identiteeti võib sisaldada ka spetsiaalne mobiiltelefoni SIM-kaart – Mobiil-ID.



ID-kaart ja Mobiil-ID

- **ID-kaardiga sisselogimise** turvalisus on samal tasemel nagu maailma militaar- ja luurestruktuurides, **lisaks saab ID-kaardiga anda digiallkirja**, mida ei saa võltsida ega selle andmist eitada. Kui ID-kaardi kasutamiseks on vaja kiipkaardilugejat ja spetsiaaltarkvara, siis Mobiil-ID jaoks piisab mobiiltelefonist

ID-kaart ja Mobiil-ID

Piltlikult öeldes hoitakse ID-kaardi elektroonilisel kiibil väga pikka ja raskesti murtavat parooli, mis pealegi koosneb kahest osast ehk võtmest.

Selle võtmepaari avalikku võtit hoitakse koos kaardiomaniku elektrooniliste isikuandmetega ID-kaardi kiibi avalikus osas, kust seda saavad lugeda kaardipõhiste läbipääsusüsteemide kaardilugejad, veebiteenused ja muud ID-kaardil põhinevate rakenduste kasutajad.

ID-kaart ja Mobiil-ID

Võtmepaari salajase võtme ainueksemplar on salvestatud kiibi kaitstud osasse, millele pääseb ligi ainult PIN-koodide abil.

Avalik võti ja salajane võti on omavahel matemaatiliselt seotud, kuid avaliku võtme põhjal ei ole võimalik tuletada salajast võtit.

ID-kaart ja Mobiil-ID

ID-kaardiga autentimisel saadab veebiserver ID-kaardi omanikule tolle avaliku võtmega krüpteeritud sessioonivõtme, (väike aknake Teie andmetega) mille see siis oma salajase autentimisvõtmega lahti krüpteerib ning mille abil saab asuda serveriga üle turvakanali krüpteeritud andmepakette vahetama.

Kui midagi ei klapi – kasutaja sertifikaat on kehtetu, PIN1 on vale või üritatakse kasutada võltsitud sertifikaati – **siis sessioonivõtmeid vahetada ei õnnestu ja ligipääs veebiteenusele on tõkestatud.**

ID-kaart ja Mobiil-ID

- **ID-kaardi kuritarvitamiseks ei piisa selle PIN-koodide väljanuhkimisest, vaja on ka füüsilist ID-kaarti ennast.** Samuti ei saa kuritarvitada võõrastesse kätte sattunud ID-kaarti, kui ei tea selle PIN-koode või kui avaliku võtme infrastruktuur ei kinnita kaardiomaniku sertifikaatide kehtivust.
- **ID-kaardi kiibil on ka valesisestuste loendur,** mis tähendab seda, et kaardi PIN blokeerub pärast kolme valesisestust. Blokeerunud PIN-i saab lahti blokeerida PUK-koodi abil.

ID-kaardi ja Mobiil-ID turvaliseks kasutamiseks:

- 1. **Sulgege kindlasti veebilehitseja**, kui olete ID-kaardi/Mobiil-ID kasutamise lõpetanud!
- 2. **Kui internetilehitsejas kuvatud kontrollkood erineb mobiiltelefoni ekraanile kuvatud kontrollkoodist**, siis katkestage toiming, sulgege lehitseja ja alustage toimingut uuesti.
- 3. **Ärge unustage ID-kaarti kaardilugejasse!**
- 4. **Ärge hoidke PIN-koode koos ID-kaardi või mobiiltelefoniga!**
- 5. **Ärge öelge ega näidake oma PIN-koode mitte kellelegi!** Kui kahtlustate, et keegi on teie PIN-koodid teada saanud, muutke nad ID-utiliidis/ mobiiltelefoni vastavas menüüs kohe ära!
- 6. **Kui olete ID-kaardi kaotanud, helistage kohe telefonil 1777 ja peatage sertifikaadid** – nii ei saa kaarti elektrooniliselt kuritarvitada. Kui kaotasite mobiiltelefoni SIM-kaardi ja/või PIN-koodid, helistage numbril 123.
- 7. **Kui ID-kaart on teilt varastatud, pöörduge Kodakondsus- ja Migratsiooniametisse** ja laske kaart kehtetuks tunnistada – siis ei saa seda ka füüsiliselt väärkasutada, näiteks teie nimele lepinguid sõlmida.

Klahvinuhk

- **Klahvinuhk** (*keylogger*) on nuhkvara, mis salvestab kõik klahvivajutused algul failina arvuti kõvakettale ja hiljem saadab need üle interneti ettenähtud e-posti aadressile või FTP-serverisse.
- **Klahvinuhk võib olla ka riistvaraline** – selle võib paigutada klaviatuurijuhtme pistiku ja pesa vahele või monteerida klaviatuuri sisse. Niisugused klahvinuhid salvestavad klahvivajutused oma sisemällu.

Klahvinuhk

Tarkvaralised klahvinuhid võivad lisaks salvestada ka ekraanipilte ja hiireklõpse.

Klahvinuhk installeeritakse teie arvutisse teie teadmata. Seda võivad teha lapsevanemad, teie asutuse süsteemiülem, jälitusametkonnad ja muud kontrollorganid.

Nii saab jälgida, milliseid veebisaite te külastate, millest lobisete jututubades, kellega vahetate e-posti, mis on teie sõnumite sisu jne. Seejuures registreeritakse ka iga tegevuse täpne aeg.

Enamasti tegelevad klahvinuhkide paigaldamisega aga kurjategijad, kes soovivad välja nuhkida teie paroolid, krediitkaardinumbreid jms informatsiooni, et teha tühjaks teie pangaarve, võtta teie nimel laenu, ajada teie kaela oma pahategusid jne

Klahvinuhk arvutis töötavate programmide nimekirjas tavaliselt ei kajastu. Üles leiab ja eemaldab selle kas viirustõrje või spetsiaalne klahvinuhkide otsimise tarkvara.



Krüpteerimine

Krüpteerimine tähendab loetaval kujul oleva informatsiooni muutmist loetamatuks.

Pealtnäha kaootiline tulemus allub siiski teatud reeglitele ehk algoritmile, mis võimaldab vastava šifri ehk võtme abil muuta krüpteeritud informatsiooni taas loetavaks ehk dekrüpteerida.

Krüpteerimist kasutatakse arvutite ja arvutivõrkude, mobiiltelefonide, sinihamba ja muude seadmete turvalisuse tagamiseks.

Küberkuritegevus

Paarkümmend aastat tagasi võeti servereid maha ning jooksutati arvutisüsteeme kokku peamiselt huligaansetel ajenditel, viiruste kirjutamine oli tore nali ning valitsusasutuste ja suurfirmade arvutivõrkudesse sissemurdmise põhimotiiviks oli näidata, et nende süsteemiadministraatorid on saamatud nannipunnid ja lollpead.



Küberkuritegevus

Vanad head ajad on pöördumatult möödas, vana kooli arvutihuligaanid on kas vangist väljas või muidu täiskasvanuks saanud, uus põlvkond aga maandab end häkkimise asemel arvutimängudega.

Küberkuritegevuses on elurõõmus mürgeldamine asendunud tõsise ja plaanipärase rahateenimisega.

Summad pole väiksed: ainuüksi Ameerika Ühendriikides ulatus 2006. aastal küberkuritegevuse käive 2,8 miljardi dollarini.

Kui veel arvestada, et internetti kasutab käesoleva aasta alguse seisuga ümmarguselt miljard inimest, siis ei maksa imeks panna, et kurjategijate jaoks on internet koht, kus võib väga väikese vaeva ja pea olematu riskiga teenida väga palju raha.

Küpsised

Sessiooniidentifikaator, suupärasemalt küpsis (*cookie*) kujutab endast väikest tekstikujulist andmeplokki, mille veebiserver saadab teie veebilehitsejale ja mis salvestatakse teie arvuti kõvakettale. Küpsist hiljem serverile tagasi saates annab teie veebilehitseja serverile märku, et on sellega juba suhelnud ning edasi võib jätkata sealt, kust eelmine kord pooleli jäi.



Küpsised

Küpsised ise ei loe teie arvutist informatsiooni ega saada seda laia maailma. Küll aga võidakse küpsiste abil kogutud informatsiooni, näiteks teie surfamiseelistuste või ostlemishuvide kohta, müüa kolmandatele osapooltele. Pärast aga hakkate saama rämpsposti ahvatlevate pakkumistega.

Lunavara

Lunavara (*ransomware*), tuntud ka kui krüptoviirus või krüptouss, **on selline pahavara, mis krüptib kasutaja arvutis kas teatud olulised andmed või terve kõvaketta, misjärel kurikaelad nõuavad andmete lahtikrüptimisvõtme eest lunaraha.**

Viimase maksmine, muide, ei garanteeri veel seda, et ohver ka krüptovõtme kätte saab.

Arvutisse satub lunavara, nagu mis tahes muu pahavara, kas spämmi, pahatahtliku kodulehekülje või hooletult arvutisse torgatud andmekandja kaudu.

Lunavara vastu aitab toimiv viirustõrje, eriti väärtuslikuks vasturohuks on aga värske varukoopia.



Nuhkvara

Pahavara, mis paigaldatakse arvutisse ilma selle kasutaja teadmata ning on mõeldud tema tegevuste ja isikuandmete jälgimiseks ning arvuti kontrollimiseks.

Nuhkvara võib jälgida kasutaja veebisurfamisharjumusi, aga ka salvestada paroole, klahvivajutusi ja ekraanipilte.

Mõnikord paigaldab nuhkvara arvutisse lisaprogramme, suunab ümber veebiliiklust.

2005. aastal tehtud uuringu järgi leidis 62 %-s personaalarvuteis nuhkvara, kusjuures 92% arvutite omanikest ei teadnud selle olemasolust midagi.

Tavaliselt tuleb nuhkvara kaasa mõne huvitava programmi või programmilaienduspaketiga.

Eestis näiteks on nuhkvara tiritud alla koos mõne P2P-failijagamisprogrammi, divx-formaadis filmide vaatamiseks vajaliku koodeki või Messengeri lisaemotikoniga. Tuntumad nuhkijad on CoolWebSearch, Zango, Zlob ja Internet Optimizer.



Pahavara

Pahavaraks, ka kurivaraks nimetatakse sellist tarkvara, mida kasutatakse ilma omaniku teadmata tema arvutisse tungimiseks ja/või selle kahjustamiseks.

Pahavara on mitut liiki: viirused, troojalased, ussid, nuhkijad, helistajad, reklaamijad ja paljud muud.

Pahavara ei teki ise, seda kirjutavad inimesed, keda ajendab kas uudishimu, soov huligaanitseda või teid teie rahast ilma jätta.

Pahavara võib arvutisse sattuda CD-plaadil või muul andmekandjal, olla kaasa pandud e-kirjale, peidetud mõnda programmi või dokumenti, olla veebibrauseriga alla laetud või tulla ise, aukliku või puuduva tule müüri kaudu.

Nakatunud arvutil võib kahjustuda kõvaketas, emaplaat või mõni muu seade, pahavara võib arvutist kustutada olulisi andmeid või kasulikke programme.



Pahavara

Uusim pahavara üritab siiski toimetada teie arvutis võimalikult vaikselt ja tagasihoidlikult, et te midagi kahtlustama ei hakkaks ning oma igapäevaseid toimetusi julgelt edasi toimetaksite – kasutaksite internetipanka, vahetaksite konfidentsiaalseid sõnumeid, sisestaksite oma kasutajatunnuseid ja paroole.

On olnud juhuseid, mil pahavara kontrolliv küberkurjategija on koguni hoolitsenud arvuti opsüsteemi turvaparanduste pealepaneku eest ja jälginud, et viirustõrje toimiks korralikult ja eemaldaks konkureeriva pahavara.

Omakasupüüdmatuslega pole sellel siiski pistmist – teie arvutiresurss, pangaandmed ja muu isiklik info on liiga väärtuslik saak, et seda kellegagi jagada.



Paroolid

Juba Vana-Rooma sõjaväes kasutati paroole selleks, et omasid ära tunda ning võõraid tähtsatest kohtadest eemal hoida. Sestap teatakse tänapäevalgi, et paroole tuleb piisavalt tihti vahetada ning mida vähem inimesi salasõna teab, seda parem.

Mis muidugi ei tähenda, et seda soovitust ka päriselus järgitakse: kuni kolmandik internetikasutajaid jagab lähedastega oma paroole, enamik aga vahetab lemmiksalasõnu väga harva.

Kurikaelad teavad väga hästi, et lausa 40% kõigist paroolidest on laialt levinud tähekombinatsioonid nagu „admin”, „1234”, „parool” või „kala”.

Vägagi tõenäoliselt pannakse parooliks oma perekonnaliikmete või lemmiklooma nimi, üldlevinud on ka sünnipäevade või auto numbri kasutamine.



Paroolid

Üllataval kombel saab parooli kätte ka siis, kui parooli lihtsalt omaniku käest küsida. Küllap kõik meist on saanud e-kirju, milles turvaprobleemidele viidates palutakse sisestada etteantud veebivormi nii oma isikuandmed kui ka internetipanga paroolid. Kuid naiivsusel pole piire – internetiturvafirmade statistiliste andmete järgi langeb sellise nn paroolipüügi ohvriks ikka veel tervelt 1–2% kasutajaid.

Paroole saab varastada ka pahavara abil. Kätte saab need mitmel moel – salasõnad võidakse kopeerida veebibrauseri salvestatud paroolide loendist, salvestada võrguliikluse jälgimise käigus või siis jäädvustada vahetult üksikute klahvivajutuste kaupa.

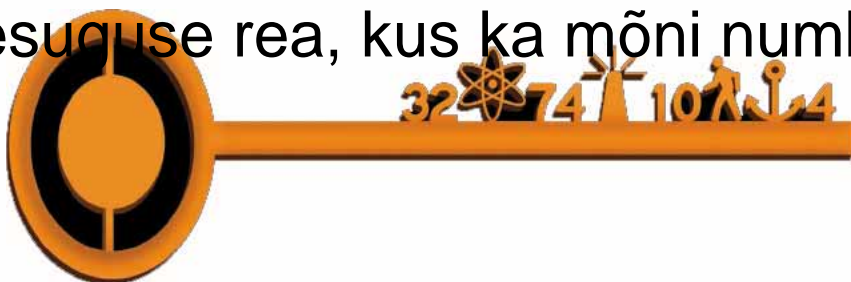
Nõuandeid paroolidega ümberkäimiseks:

1. Äрге jagage oma paroole mitte kellegagi! Need, keda te täna usaldate, ei pruugi homme enam olla teie sõbrad.
2. Hoiduge paroolidest, mis on kas üldlevinud või teid ümbritsevaga liiga lihtsalt seostatavad!
3. Kui keegi, keda te parasjagu näost näkku ei näe, küsib teie käest teie paroole, kahtlustage alati halvimat! Ja isegi otsekontakti puhul ärge oma parooli öelge, vaid toksige see ise sisse.
4. Kui parooliks kasutatava sõna võib leida sõnaraamatust, teeb see parooli murdmise mitu suurusjärku lihtsamaks.
5. Leidke mõni hea nipp oma paroolide meeldejätmiseks või kirjapanekuks!
6. Kui paroole on palju, kasutage paroolihaldustarkvara.
7. Seal, kus võimalik, kasutage ID-kaarti. Äрге seda pärast kasutamist lugejasse unustage!
8. Arvutil olgu töökorras viirustõrje ning sisselülitatud tulemüür. See käib nii kodu kui tööarvuti kohta, avalikus kasutuses olevasse arvutisse ärge parem üldse oma paroole sisestage.

Paroolihaldus

Hea parool peaks olema pikk ja keeruline ning sisaldama nii numbreid kui ka tavatähestikus puuduvaid märke. Aga siin tekib kohe jälle uus häda: niisugust parooli on kole paha meelde jätta.

Natuke kavalam on kirjutada oma salasõnad üles näiteks telefoninumbri kujul – kurikael ei hakka päris kindlasti teie telefoniraamatut läbi helistama, et teha kindlaks, milline kirjapandud number tegelikult ei tööta. Luulehuvilised võiksid valida oma lemmikpoeesia seast seesuguse rea, kus ka mõni number kirjas on.



Piraatlus

Warez on mitmuse tuletis sõnast *software*, arvutikasutajate slängis tähendab see **piraattarkvara kogumikku**.

Praegusel ajal vahetatakse piraattarkvara peamiselt P2P-võrkude (BitTorrent, Kazaa ja muud seesugused) vahendusel, väiksemal määral FTP- või veebiserverite kaudu.

Enamikes maailma riikides, sealhulgas ka Eesti vabariigis, on tarkvara loata kopeerimine ja levitamine seadusega karistatav. Kuid peale seadusega pahuksisse sattumisele võib piraattarkvara allalaadimine ja kasutamine olla tavakasutajale ka muidu ohtlik.

Pahatihti on see nagu tasuta juust hiirelõksus – koos piraattarkvaraga tuleb kaasa mõni viirus või trooja, hiljem probleemide tekkides aga on tavaliselt piinlik tunnistada, et jah, minu arvutis on piraattarkvara.



Privaatsus

Privaatsuse all mõeldakse isiku võimet kontrollida enda kohta saadaolevat informatsiooni..

Kergekäeliselt väljaantud (või väljapetunud) isikuandmed võivad kaasa tuua identiteedivarguse – teie nime all ostetakse kaupu, tarbitakse teenuseid, pannakse toime kuri- või väärtegevusi.

Pealtkuulatud või võltsitud sõnumid võivad olla heaks väljapressimise algmaterjaliks,

Eraldi teema on sotsiaalsed võrgustikud (Rate, Orkut, blogid ja foorumid), kus pahatihti jagatakse täiesti mõtlematult oma eraelu intiim detaile. Anonüümsus võib sellistes keskkondades olla petlik – eriti Eesti-suguses väikses ühiskonnas on väga lihtne teie nimi ja teie avaldatud seigad omavahel kokku viia.

Igal veebisaidil, mis kogub isikuandmeid, peab olema kirjas ka seletus, milleks ja missuguseid andmeid kogutakse, kuidas kogutud andmeid kasutatakse.



Reklaamvara

Reklaamvara (*adware*) tuleb teie arvutisse tavaliselt mõne teise rakenduse tasuta kaasaandena ning on parimal juhul ainult veidi tüütu, näidates reklaame ja plõksides lahti hüpikaknaid.

Vastikum reklaamvara installeerub teie arvutisse ilma selleks eelnevalt nõusolekut küsimata ning võib näiteks asendada brauseri avalehe mõne oma reklaamkliendi omaga. Sageli võib reklaamvara tekitada tõsist tüli juhul, kui soovite seda oma arvutist eemaldada, nii et puhas installatsioon võib olla kiireim ja lihtsaim võimalus reklaamvarast lahti saada.

Viirustõrje saab reklaamvarast tavaliselt hõlpsasti lahti, probleem tekib siis, kui reklaamvara installeeritakse koos mõne seesuguse programmiga, mida te ise kangesti kasutada soovite. Niisugune reklaamvara on nõus ka tavavahenditega arvutist lahkuma, kuid ainult koos soovitud programmiga.



Rootkit

Rootkit ehk käomuna on selline tarkvara, mis toimetab arvutis juurkasutaja (ehk administraatori) õigustes, tavaliselt operatsioonisüsteemi tuuma tasandil, hiilides niiviisi mööda operatsioonisüsteemi turvamehhanismidest.

Tuntuim käomuna oli Sony multimeediafailide kopeerimiskaitsemehhanism, mis peitis end sügavale operatsioonisüsteemi ning mida oli tõsiselt tülikas eemaldada. Samasuguseid peitemehhanisme kasutab aga ka mitmesugune pahavara, kindlustades selle, et tema olemasolu jääb nii kasutajal kui ka viirustõrjel märkamata.

Paljud viirustõrjefirmad pakuvad spetsiaaltarkvara käomunade leidmiseks – näiteks F-Secure BlackLight, AVG Anti-Rootkit ja Radix Anti-Rootkit. Käomuna lõplikuks eemaldamiseks tuleb üldjuhul eemaldada kõvakettalt kogu info ning operatsioonisüsteem koos kõigi programmidega uuesti installeerida.



Rämpspost

Viimastel andmetel moodustab spämm juba 94% kogu meililiiklusest, ühe kuu jooksul saadetakse üle maailma hinnanguliselt 296 miljardit rämpssõnumit, kusjuures spämmi hulk kaldub iga poole aasta järel kahekordistuma.

Spämmijad teavad suurepäraselt, et 99 inimest 100-st peavad spämmi tüütuks ja vastikuks ning kustutavad selle samal hetkel, kui see nende postkasti potsatab. Neid huvitabki ainult see üks protsent, ülejäänud üheksakümne üheksa meilisaaaja meelepaha eest kaitsevad nad end sellega, et saadavad spämmi kas mõnes uduste kasutustingimustega võrgus asuva ajutise serveri või botneti kaudu. See üks protsent spämmisaaajaid, kes kirja läbi loevad, on aga piisavalt hinnaline saak, mille nimel tasub ponnistada.

Spämmi saatmise kulud on pea olematud, eeldatav kasu võib olla aga väga suur. Lisaks tavalisele süütule, kuid tüütule reklaamile saab spämmi abil laiali saata pahavara, õngitseda isiku- ja krediitkaardiandmeid, ligipääsuparoole ja muudki huvitavat.

Rämpspostitada saab Nigeeria päritolu investeerimispakkumisi, aga ka reaalselt kaubeldavate aktsiate ostusoovitusi. Mis viimastesse puutub, siis nii praktika kui ka teaduslikud uurimused näitavad, et aktsiaspämmiga saab teenida keskel läbi 5,7% kasumit.





Seadused

Võõraste arvutivõrku sissemurdjaid võib karistada arvuti, arvutisüsteemi või arvutivõrgu ebaseadusliku kasutamise eest **koodi, salasõna või muu kaitsevahendi kõrvaldamise teel** (§ 217, kuni kolmeaastane vangistus), samuti arvutivõrgu või arvutisüsteemi ühenduse rikkumise või tõkestamise eest (§ 207, rahaträhv).

Kräkkereid, kui nad on toime pannud arvutis olevate andmete või programmi ebaseadusliku vahetamise, kustutamise, rikkumise või sulustamise või sisestanud arvutisse ebaseaduslikult andmeid ja programme, **võib ees oodata kuni aastane vangistus, sama teo eest eesmärgiga takistada arvuti- või telekommunikatsioonisüsteemi tööd aga kuni kolmeaastane vangistus** (§ 206, arvutikahjurlus).

Arvutiviiruse levitamise eest (§ 208) võib raskemal juhul saada **kuni kolmeaastase vangistuse, võõraste sõnumite või kirjade lugemise eest** (§ 156, sõnumisaladuse rikkumine) **rahaträhvi, ametiisik kuni aastase vangistuse**.

Paroolipüüdjad, õngitsejad ja vahemeherünnaku autorid võidakse arvutikelmuse (§ 213) eest **trellide taha saata kuni viieks aastaks**.

Seadused

Piraatkoopia valmistamise eest levitamise eesmärgil (§ 222) tehakse rahatrahv ja konfiskeeritakse kuriteo toimepanemise vahend, **piraatkoopiaga** kauplemise eest aga ähvardab kuni **3.aastane** vangistus ja piraatkoopia konfiskeerimine. Sama karistuse saab ka arvutiprogrammi ebaseadusliku füüsilise kasutamise või valdamise eest ärilisel eesmärgil (§222¹). **Kuni 3. aastaks võib vangiminna ka selle eest, kui jagate oma piraatkoopiat avalikus võrgus** – kas siis FTP-serveri või P2P failijagamisprogrammi kaudu (§ 223). Arvutiprogrammi kräkkimise või koopiakaitse mahavõtmise eest (§ 225) on samuti ette nähtud kuni 3. aastane vanglakaristus.

Süsteemiadministraatorid ja muud vastutavad isikud peavad meeles pidama, et arvuti, arvutisüsteemi või arvutivõrgu **kaitsekoodide ebaseadusliku üleandmise eest**, kui see on toime pandud omakasu eesmärgil ja kui sellega on tekitatud oluline kahju või põhjustatud muu raske tagajärg (§ 284),

karistatakse rahatrahvi või kuni 3. aastase vangistusega.

Sinihammas

Sinihammas (bluetooth), võimaldab erinevatel seadmetel omavahel ilma juhtme või infrapunakiireta suhelda.

Põhimõtteliselt peaks see võimaldama ühendada telefoni, arvutit, klaviatuuri või kõrvaklappe ilma juhtmeteta ning isegi ilma omaniku aktiivse vahelesegamiseta.

Bluesnarfing on rünnak, mis võimaldab üle *bluetooth*-ühenduse tungida võõrasse telefoni ja arvutisse, sorida seal kalendrit, kontakte ja sõnumeid ning väidetavalt varastada fotosid ja teisi faile.

Kui teil just ei ole väga ajast ja arust telefon, näiteks Nokia 6310 või Ericsson T68, ei maksa teil karta, et keegi pääseks ilma teie nõusolekuta teie andmetes sorima.



Sinihammas

Bluetooth'i turvalisusele tuleks siiski tähelepanu pöörata. Kontrollige oma mobiiltelefoni sinihamba seadeid ning pange oma telefoni nähtavuseks "Varjatud". Oma telefoniga seotud seadmeid saate edasi kasutada.

Kui te *bluetooth*'i parasjagu ei kasuta, lülitage see parem välja. Sästate nii oma taskusõbra akusid kui ka iseenda närve.

Zombi

Zombi on arvuti, mis on pealtnäha täiesti korras, kuid mida kontrollib võrgus asuv küberkurjategija ning mis koos teiste omasugustega kuulub ülevõetud arvutite võrku – botnetti.

Tavalisim viis arvuti zombistamiseks on nakatada see pahavaraga. Näiteks tirib arvutikasutaja võrgust alla mõne näiliselt süütu programmi, mille peale ka tema viirustõrje ei oska midagi kahtlustada. Ent pärast käivitamist tõmbab seesama süütu programm võrgust alla oma pahategevad komponendid, avab arvutis tagaukse ning kannab kusagil võrguavarustes passivale küberkaabakale ette, et arvuti on üle võetud ning ootab tema käske.

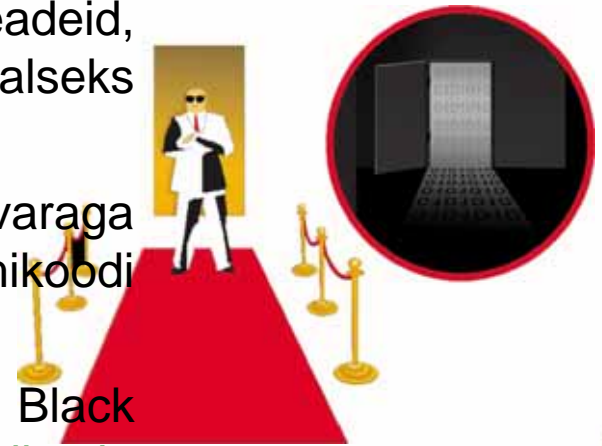


Tagauks

Kõikidesse nüüdisaegsetesse operatsioonisüsteemidesse on sisse ehitatud kontrollmehhanismid ja kasutusõiguste süsteem, mis näiteks takistab ühel arvutikasutajal lugemast teise kasutaja kirju ning ei luba tavalisel kasutajal muuta süsteemiseadeid, installeerida programme ega kustutada arvuti normaalseks tööks vajalikke faile.

Sagedamini aga paigaldatakse tagauks pahavaraga nakatumise järel – selleks muudetakse kas programmikoodi või muid opsüsteemi seadeid.

Tuntuim **tagaukseprogramm** on Black Orifice, Black Orifice võimaldab muuta kõiki arvutis olevaid faile ja süsteemiseadete registrit, jälgida reaajas ekraanipilti, kontrollida hiirt ja klaviatuuri ning kogu võrguliiklust. **Enamik viirustõrjujaid tunneb selle programmi ära ja liigitab pahavaraks.**



Trikitamine

Arvutisüsteemid on täis võimsaid ja tarku kaitsevahendeid – viirustõrjeid, tule müüre, krüpteeritud sidekanaleid, väärkasutuse hoiatussüsteeme ja palju muud. Inimene on niisuguste turvasüsteemide kõige nõrgem lüli ning kurjategijad teavad seda väga hästi.

Arvutikurjamate töö sarnaneb sageli mustkunstnike omaga – nende eesmärgiks on panna tavaline arvutikasutaja nägema seda, mida ta triki õnnestumiseks peab nägema, mitte seda, mis tegelikult toimub. Usalduse kuritarvitamise lihtsaks näiteks on elektronkirjad, mille pealtnäha on saatnud kas väga hea sõber, ülemus, pank või mõni tuttav. Aga kas ikka on?

Nii ei maksa olla sugugi meelitatud, kui saate kirja mõne Aafrika presidendi otseselt järeltulijalt, ega imestada, kust ta teid küll tunneb. Veel vähem tasub uskuma jääda seesuguses kirjas väljapakutud plaane hiigelpäranduse jagamiseks – vähe sellest, et te ei näe kunagise diktaatori kokkuriisunud miljonitest sentigi, tõenäoliselt kaotate ka märkimisväärse osa isiklikust varast. Üldse ei maksa uskuda suvaliselt saatjalt tulnud sõnumeid, mis näivad liiga head, et olla tõsi – olgu selleks siis võit loteriis, milles te pole osalenud, geniaalne investeerimisplaan 200%-lise kasumiga, absurdsest odavast luksuskaubast või siis eluiga ja riistvara pikendavad imevahendid.



Troojalased

Trooja hobune, lühendatult troojalane on selline pahavara, mis sokutab end teie arvutisse näiliselt süütu rakendusena, kuid käivitamisel pakib lahti oma pahategeva poole (või tirib selle internetist alla). Tavaliselt haagib troojalane end mõne süsteemse protsessi külge, jälgib arvutikasutaja tegevust ning võtab aeg-ajalt ühendust oma peremehega. Viimane omakorda kas kasutab arvutist leitud andmeid arvutiomaniku rahakoti tühjendamiseks või siis arvutit ennast kas spämmi saatmiseks, teiste arvutite nakatamiseks või koordineeritud rünnakuks mõne veebiteenuse vastu.



Troojalased

Tavaliselt teeb troojalane kõik, et tema olemasolu jääks arvuti omanikule märkamatuks, kuid mõned troojalased võivad näiteks välja lülitada arvutisse paigaldatud viirustõrje ja tule müüri.

Enamasti on troojalaste autorite eesmärgiks mitte arvutisüsteemi kahjustamine, vaid, vastupidi, mil arvutit kontrolliv kurikael on koguni installinud opsüsteemi turvapaiku ja hävitanud konkureerivat pahavara!

Parimaks kaitseks seesuguse pahavara vastu on mõistlik ja turvateadlik käitumine: **ärge avage tundmatutelt saatjatelt tulnud kirjade manuseid ega klõpsige nende saadetud linke, hoiduge porno- ja kräkitud programmivõtmete saitidest ning ärge kasutage piraattarkvara.**

Tulemüür

Tulemüür on tarkvararakendus, mille põhiülesandeks on reguleerida liiklust erineva turvatasemega arvutivõrkude vahel, eraldades näiteks väiksema kodu- või kontorivõrgu ülejäänud internetist.

Kui ehitiste puhul peab tulemüür takistama tule levikut ühest hoone osast teise, siis arvutivõrkudes on **tulemüüri ülesandeks takistada pahatahtlike rünnete levikut** väheturvalisest **välisvõrgust** kaitstumasse sisevõrku või konkreetsesse arvutisse.



Turvaaugud

Senikaua, kuni arvutiprogramme loovad inimesed, esineb neis ikka mõni viga. Mida keerulisem süsteem ja mida rohkem inimesi selle valmimisel osales, seda suurem on ka vigade tõenäosus.

Turvaauk on arvutiprogrammi või -süsteemi niisugune omadus, mida selle loomise ajal kas ei mõeldud korralikult läbi, ei osatud ette näha, tehti hooletult või otsustati ignoreerida ning mille kaudu saab sedasama süsteemi kuritarvitada.



USB

Sedamööda, kuidas tulemüürid ning muud sissetungi tõkestavad seadmed muutuvad järjest kavalamateks ja tõhusamateks ning võrku sissetungimine, eriti märkamatu sissetungimine, muutub järjest keerulisemaks, on **ripakile jäetud USB-pesa küberkurjategijatele tõeline kullaauk.**

Spetsiaaltarkvaraga mälupulk tuleb ainult mõneks sekundiks sisestada arvuti kättesaadaval küljel olevasse USB-pesasse, vastavad rakendused tõmmatakse automaatselt käima ning kogu arvutis leiduv vähegi huvipakkuv informatsioon saadetakse kas eelnevalt defineeritud meiliaadressile, ftp-saidile või, kui on rohkem aega, salvestatakse sellelesamale mälupulgale. Jäävad ära tülikas ja ohtlik sissemurdmine ning näha pole ka pahateo jälgi.



Ussid

Internetiüsse (*worms*) **eristatakse viirustest peamiselt nende paljunemisviisi järgi** – kui arvutiviirus haagib end tavaliselt mõne teise programmi külge ning vajab paigaldamiseks või levimiseks kasutaja kaasabi, siis **uss on võimeline internetis levima ja paljunema iseseisvalt, kasutades tavaliselt operatsioonisüsteemi või rakenduste turvaauke.**



Ussiga nakatunud arvuti võidakse muuta zombiks ning kasutada koos teiste samasugustega näiteks mõne veebiserveri ründamiseks, et serveri omanikult raha välja pressida.

Vahemeherünnak

Nn vahemeherünnak (*man in the middle attack*) kasutab olukorda, mil arvutikasutaja arvab, et suhtleb turvalise serveri või teenusega. Ründaja, kes seda suhtlust pealt kuulab, võib selle ajal saadud andmeid kasutades vastavalt oma eesmärkidele mängida kasutajale ise serverit ning meelitada temalt välja turvakriitilisi andmeid.



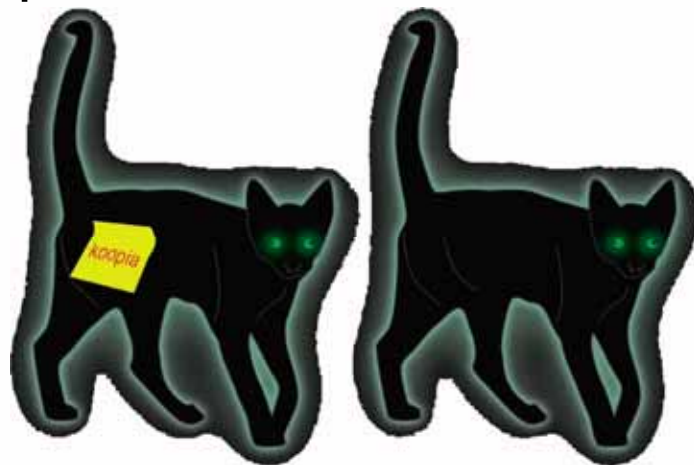
Väga levinud ja suhteliselt ohutu on näiteks krüpteerimata WiFi-ühenduse pealtkuulamine.

Kui pahaaimamatu WiFi- kasutaja logib end sisse oma POP3-protokolliga kasutavasse postkasti, liigub tema e-maili kasutajanimi ja parool üle võrgu lahtise tekstina.

Seda pealt kuulanud pahatahtlik tegelane võib saada kasutajatunnuse ja parooliga hiljem ise samasse postkasti siseneda, lugeda läbi kogu serveris talletatud kirjavahetuse ning kasutaja sõpradele ja töökaaslastele kas või sõimukirju saata.

Varukoopia

Isegi kui teie arvutil on parim võimalik viirustõrje, tulemüür ja muud turvalahendused, võib ikkagi juhtuda, et arvutis olevad andmed lähevad kaotsi või saavad kahjustatud – kas siis ütleb kõvaketas üles või tassib varas arvuti lihtsalt minema. Sel puhul on kasulik omada andmete või failide koopiat kas siis CD-ketastel, võrgukettal või mõnel muul viisil. Varukoopia väärtus on seda suurem, mida värskem on koopia.



Veebilehitseja

Veebilehitseja ehk brauser on selline tarkvararakendus, mille abil saab lokaalses arvutis vaadata/kuulata internetis (või ka kohtvõrgus) paiknevatel veebilehtedel olevat teksti, pilte, videot, heli- ja teisi faile ning muud informatsiooni.

Samas kaasnevad kasutusmugavuse ja mitmekülgisusega ka **turvariskid** – kuna veebilehitsejal peab oma ülesannete täitmiseks olema juurdepääs väga paljudele arvuti opsüsteemi ja riistvara osadele, on just veebilehitsejast kujunemas **peamine** tarkvararakendus, mille kaudu kurjategijad nn **tavakasutaja arvutit rünnata üritavad**.





Viirused

Need on pahavara kuulsaimad esindajad. Esimene viirus, The Creeper, liikus interneti eelkäijas ARPANET-is juba 1970. aastatel.

Esimene laia maailma lahtilastud viirus Elk Corner kirjutati 1982. aastal. Arvutiviiruste kuldaeg oli kümmekond aastat tagasi, mil Michelangelo põhjustas ülemaailmse paanika ning CIH kärsatas tuhandete kaupa emaplaate läbi.

Vanema põlvkonna viirused levisid flopiketastel, praegusel ajal rändavad nad kas elektronkirjade manustes või internetist allalaaditavate failide küljes.

Rahvasuu nimetab viiruseks mis tahes pahavara, ent konkreetselt on viirus seesugune arvutiprogramm, mis on võimeline end ilma kasutaja soovi ja teadmata iseseisvalt ühest arvutist teise kopeerima ja arvutit nakatama.

Kuna flopid on nüüdseks ametlikult välja surnud, tassitakse uusi viiruseid koju peamiselt mälupulkadel, aga ka näiteks mp3-mängijate või digifotoaparaatide mälukaartidel ning isegi mobiiltelefonide mälus. Olemas on ka mõned spetsiaalsed mobiiltelefoni viirused, näiteks Cabir-A, mis hüppavad ühelt telefonilt teisele üle sinihamba. Tõsi, nakatumiseks tuleb telefoniomanikul vastavas menüüs oma nõusolekut kinnitada.

Viirustõrje

Programmide kogum, mis üritab ära tunda ning kahjutustada või kustutada ohtlikumaid kurivara liike: viiruseid, usse, troojalasi jms.

Moodsamad viirustõrjujad võitlevad peale selle veel reklaamvara, rootkittide, klahvinuhkide ja identiteedi-varguskatsete vastu. Komplekssemad viirustõrjelahendused võivad sisaldada ka tule müüri, spämmifiltrit ja varundusmootorit.



Viirustõrje

Tasulistest viirustõrjekomplektidest on Eestis levinumad F-Secure, Kaspersky, Nod32, McAfee, Nortoni ja Trend Micro tooted, mujal maailmas ka veel BitDefender, DrWeb, Norman, Panda, Prevx ja Sophos.

Tasuta versioone pakuvad AVG, Avast! ja ClamWin.

Viirustõrjeprogrammid on kõige efektiivsemad siis, kui nad on kogu aeg töös, isegi kui see mõjub pärssivalt arvuti jõudlusele, ja kui nende viirusdefiniitsioonid on kogu aeg värsked.

VoIP

Internetipõhised telefonid (*Voice over Internet Protocol*) on üha populaarsemad, peamiselt seetõttu, et nendega üle interneti tehtavad kõned maksavad väga vähe või üldse mitte midagi (kui internetiühenduse kulu välja arvata).

VoIP-telefonide pealtkuulamine ja koguni kõnede võltsimine on täiesti võimalik, õnneks kasutab näiteks meie kodumaine Skype ühenduse krüpteerimist.

Skype'i sõnumivahetus on heaks alternatiiviks turvamata Messengerile, samas võib ka Skype'i kaudu pahavaralinke saata.



VoIP

Vishing (*phishing over VoIP*) on õngitsemis skeem, milleks kasutatakse internetitelefoni.

Ohvrile saadetakse spämmikiri, milles palutakse turvaintsidendi tõttu helistada panga infotelefonile. Kirjas oleval telefoninumbril vastab aga internetitelefoni automaatvastaja, mis küsib mitmesugustel ettekäanel helistaja telefonipanga turvakoode.

Petuskeem kasutab ära asjaolu, et inimesed pole veel harjunud pangatelefone kahtlustama, samuti seda, et enamik niisuguse spämmikirja saajatest ei kontrolli niikuinii, kas kirjas toodud telefoninumber ka tegelikult pangale kuulub.

Võrgu kaitsmine

Koduvõrgu kaitsmiseks internetist tulevate rünnakute eest on vaja **tulemüüri**. See võib olla nii operatsioonisüsteemi enda sisseehitatud tulemüür, kuid veel parem on tulemüüri funktsionaalsusega ruuter. Selle konfigureerimine sõltub konkreetse ruuteri margist, traadita võrgu puhul on paljud seaded universaalsed.

WiFi

Traadita võrgu kasutajate arv läheneb jõudsalt sajale miljonile, ja mitte ilmaaegu. WiFi-t on väga mugav ehitada – traadita võrk ei nõua kapitaalvahutuslikke töid kaablivedamise näol, seda on lihtne paigaldada ja vajadusel laiendada.

Samas on traadita võrgu pealtkuulamine lihtne ja riskivaba võrguliikluse pealtkuulamine ei jäta endast mingeid jälgi, WiFi- võrgu kaitseabinõud on aga pahatihti ebapiisavad.



Krüpteerimata WiFi-andmevoog liigub eetris lahtise tekstina, huviline näeb kõiki veebilehti, millel kasutaja parasjagu surfab, meilipostkasti ja internetiportaali parooli ning MSN-i vestlusi.

Küberkaabaka viljakaim tööpõld on avalik WiFi-võrk, mille võib leida näiteks hotellides, lennujaamades või ka kohalike omavalitsuste pakutuna.

Enesekaitseks tuleks siis vähemalt katsuda hoiduda veebilehtedest, mis küsivad kasutajanime ja parooli.

Õngitsemine

•Õngitsemine ehk phishing on inimpsüühikaga manipuleerimise üks viise, **lollitamistehnika**, millega üritatakse arvutikasutaja viia niikaugemale, et ta annab kurjategijale ise oma juurdepääsuandmed, paroolid, krediitkaardi rekvisiidid ja muu turvakriitilise informatsiooni.

•Näiteks saadetakse teile pangarekvisiitidega e-kiri, mis nõuab, et turvakaalutlustel tuleb vahetada oma internetipanga paroolid ning annab selleks ka lingi, mis viib internetipangaga äravahetamiseni sarnasele koduleheküljele.

•Et asi veelgi ehtsam tunduks, võivad kurjamid võltsida ka nimeserveri kirjeid, nii et isegi brauseriribal olev aadress on panga oma. Viimasel juhul saate aga tavaliselt oma brauserilt hoiatuse, et teie külastatava serveri sertifikaat ei vasta külastatava serveri aadressile.

•Mõistagi ei tohiks pärast sellist hoiatust niisugusele saidile mitte mingeid andmeid sisestada, kõige vähem oma kasutajanime ja parooli.



Kokkuvõtteks.

Kuidas end kaitsta? Nõuanded:

1. Kasutage antiviirust. See kaitseb teid enamiku tuntud pahavara eest.
2. Kasutage tule müüri ja spämmifiltrit. Hea, kui interneti- ja meililiikluse kontroll ning viirustõrje toimub juba enne teie arvutit.
3. Suhtuge kahtlustavalt meilimanustesse, parem, kui potentsiaalselt ohtlike manuste avamine on vaikimisi keelatud. Ärge kunagi avage tundmatult saatjalt tulnud faili, sõprade saadetud failid aga kontrollige kindlasti viirustõrjega üle.
4. Logige administraatori õigustes arvutisse sisse ainult rakenduste paigaldamiseks ja arvuti seadete muutmiseks – igapäevatöö tegemiseks logige sisse piiratud õigustega kasutajana. Sedaviisi suudab arvutisse sisseroninud pahalane hoopis väiksemat kahju tekitada.
5. Tõmmake ja paigaldage regulaarselt tarkvarauuendusi, nii ei pääse teie arvutisse pahavara, mis kasutab tuntud turvaauke.
6. Tehke regulaarselt varukoopiaid. Isegi kui arvutiga läheb pahasti, jäävad vähemalt andmed, dokumendid ja pildid alles.

7. Olge ettevaatlik mälupulkade ja teiste andmekandjatega, kontrollige neis sisalduvat kindlasti pärast seda, kui olete neid vöõras arvutis kasutanud. Vöõrast andmekandjat ärge oma arvuti lähedale laske!

8. Kui te oma sülearvuti vöi mobiiltelefoni sinihammast parasjagu ei kasuta, lülitage see parem välja.

9. Ärge jagage oma paroole mitte kellegagi!

10. Seal, kus vöimalik, kasutage ID-kaarti. Ärge seda pärast kasutamist lugejasse unustage!

11. Kasutage oma tervet mõistust – ärge registreeruge kahtlastesse keskkondadesse; ärge osalege kui tahes ahvatlevates loosimistes; ärge saatke edasi kettkirju; ärge klikkige kõike, mida teile näidatakse ning ärge jagage oma andmeid kõigile, kes neid küsivad.

12. Kontrollige alati, kui miski tundub kahtlane, vajadusel küsige nõu ja abi.

•Täpsemaid juhiseid leiate arvutikaitseportaalist www.arvutikaitse.ee

Kasutatud materjal

- Kasutatud materjal: Arvutikaitse ABC (Aare Kirna)

Täna kuulamast.
Turvalist arvutikasutust!

