Tallinna Ülikool
Digitehnoloogiate Instituut

VIIRUSETÕRJETE VÕRDLEV ANALÜÜS

Bakalaureusetöö

Autor: Talis Dreifeldt

Juhendaja: Edmund Laugasson

Autor: ...……“…….……”2017

Juhendaja: ...……..“..……...……”2017

Instituudi direktor: …….....……“…….……”2017

Tallinn 2017

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.

…… ……..

(kuupäev) (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 Ülikool Akadeemilise Raamatukogu repositooriumis.

2. olen teadlik, et punktis 1 nimetatud õigused jäävad alles ka autorile.

3. kinnitan, et lihtlitsenti andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest tulenevaid õigusi.

Tallinnas, _____

(allkiri ja kuupäev)

Sisukord

Sissejuhatus

Iga aastaga langeb järjest enam inimesi eri paigus maailmas pahavara rünnaku ohvriks. Võiks arvata, et see tuleneb viiruste marulisest kasvust aastast aastasse. Ometi on suurimaks riskiteguriks siiski inimene ise, kes oma andmeid ei soovinud või ei osanud kaitsta. Seega mida rohkem on maailmas internetiohtudest teadlikke inimesi, seda edukamalt me suudame kaitsta oma faile ja näidata pahavara kirjutajatele, et nende eesmärk kiirelt raha teenida või levitada oma loodud pahavara pole enam nii lihtsalt teostatav.

Antud bakalaureusetöö on edasiarendus autori seminaritööst, milles keskenduti ainult *Windows 8.1* operatsioonisüsteemile koos tasuta viirusetõrjetega. Seminaritööst on üle toodud mõistete seletused koos soovitustega kasutajatele. Bakalaureusetöös pidas autor vajalikuks laiendada operatsioonisüsteemide arvu ning testida lisaks *MS Windowsi* (edaspidi: *Windows*) viimasele versioonile ka *GNU/Linuxi* (edaspidi: *Linux*)*, Androidi* ja *iOS* operatsioonisüsteeme. Samuti on autor kaasanud lisaks tasuta viirusetõrjetele ka tasulised versioonid. Kuna viirusetõrjeid on väga palju erinevaid siis sellest tulenevalt oli üheks eesmärgiks näidata tasuliste ja tasuta viirusetõrjete erinevust, tehes sellega kasutajatel valiku langetamise lihtsamaks viirusetõrje osas. Samuti näha, kas üks viirusetõrje sobib kõikide operatsioonisüsteemide viirusetõrjeks. Teiseks eesmärgiks olen seadnud tõsta inimeste teadlikkust internetis varitsevate ohtude eest. Teadvustades kasutajad teguviisidest mida võiks muuta ja jälgida arvutit või mobiili kasutades.

Eesmärkide saavutamiseks olen ära seletanud erinevad viiruste liigid koos muude vajalike mõistetega. Arvuti operatsioonisüsteemide juures tõin esmalt välja soovitused kasutajatele, kuidas kasutatavat operatsioonisüsteem muuta veelgi turvalisemaks. Seejärel testisin iga operatsioonisüsteemi juures nelja viirusetõrjet, milles leidus nii tasulisi kui priivaralisi viirusetõrjeid. Viirusetõrjed olid valitud kas artiklite või allalaadimiskeskkondade tulemuste järgi. Viirusetõrjete puhul alustasin nõuete kirjeldamisest ning lõpetasin sisu ja omaduste loetlemisega. Eksperimentide hulgas sai testitud nii failide läbivaatamise kiirust, koormust arvuti protsessorile ja viirustega ümberkäimist. *Windowsi* ja *Linuxi* puhul sai läbi katsetatud ka kaksikkäivitus kus üritati ühest operatsioonisüsteemist teist viirustest puhastada. Analüüs hõlmab endas tabeleid punktidega ning autori poolset kommentaari. Põhjalikumad tabelid ja joonised asuvad lisades koos informatsiooniga pahavara ja soovituste kohta.

Mõistete seletused

Käesoleva bakalaureusetöö põhimõisted on defineeritud autori seminaritöös (Dreifeldt, 2015):

Viirusetõrje - Viiruste avastamiseks ja võimalike parandusmeetmete soovitamiseks või rakendamiseks määratud programm. Tavaliselt kontrollib viirusetõrje arvutis käimasolevaid protsesse ning mälus ja kõvakettal või välisel andmekandjal olevaid ja veebist allatõmmatavaid või elektronkirjadega saabuvaid faile, võrreldes neid varem teadaoleva pahavara koodinäidistega. Kui mõni osa kontrollitavast koodist sarnaneb viirusedefinitsioonis oleva näidisega, püüab viirusetõrje nakatunud osa eemaldada ja kui see aga ei õnnestu, paigutatakse nakatunud fail karantiini või kustutatakse.

Tulemüür - Tavakasutajal on tulemüürist põhiliselt vaja teada seda, kas tema arvuti tulemüür on sisse lülitatud või ei ole. Kui mõni uus rakendus üritab pärast paigaldamist esimest korda internetti pääseda, võib tulemüür üle küsida, kas sellenimelist rakendust peaks internetti laskma või mitte. Kui rakenduse nimi on tundmatu, tasuks enne loa andmist internetifoorumitest üle kontrollida.

Turvaaugud - 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. Enamik vigu lähtekoodis õnnestub välja selgitada ja kõrvaldada testimise käigus kuid kõikide mõeldavate vigade väljaselgitamine on tavaliselt ebamõistlikult kallis ja aeganõudev ja midagi jääb kindlasti märkamata. Tavaliselt ei mõjuta niisugused vead arvutisüsteemi tööd üldse või avalduvad vaid äärmusliku koormuse tingimustes. Samuti kaldub enamik programmeerijaid alahindama kasutajate leidlikkust ning eeldama, et nende loodud tarkvara kasutataksegi selleks, mida ta oli programmeeritud tegema.

Varukoopia - Meetod oluliste andmete säilitamiseks. Juhul, kui andmed kas õnnetuse tõttu või siis kogemata hävinevad, on võimalik need taastada ilma kõike uuesti sisestamata või paigaldamata. Varukoopia väärtus on seda suurem, mida värskem on koopia. Et värskeim koopia ei pärineks poole aasta tagusest ajast, tuleks andmete varundamine muuta automaatseks. Siinkohal ulatavad tasuta abikäe pilvepõhised lahendused, mis reaalajas varundavad (Best Free Online Backup, 2016) või (Fisher, 2016). Mõistagi ei ole kuigi tark oma varukoopiat DVD või CD-na lauanurgale, veel vähem väljajagatud võrgukettale, vedelema jätta. Rohkem kui ühe

varukoopia olemasolu oleks veelgi parem, muidugi peaks nad asuma geograafilises plaanis kahes täiesti erinevad kohas.

Viirused - Pahatahtliku küberkurjategija kirjutatud programmijupp, mis on lülitatud mingi programmi koosseisu ning põhjustab ootamatuid ja kasutajale sageli äärmiselt ebameeldivaid tagajärgi. Viirus põhjustab sageli kahjustusi või pahameelt ning teda võib käivitada mingi sündmus, näiteks etteantud kuupäeva saabumine. Mõned viirused on programmeeritud otseselt arvutit kahjustama - kas siis muutma programme, kustutama faile või vormindama kõvaketast. Ussviirused tegelevad ainult iseenda levitamisega, koormates niimoodi arvuti- ja võrguressursse. Kolmandad võivad olla lihtsalt nii viletsasti kirjutatud, et arvuti jookseb neid käitades kokku.

Lunavara - Krüptoviirus on selline pahavara, mis krüptib kasutaja arvutis kas teatud olulised andmed või terve kõvaketta, misjärel kurikaelad nõuavad andmete lahtikrüptimisvõtme eest lunaraha. Arvutisse satub lunavara, nagu mis tahes muu pahavara, kas rämpsposti, pahatahtliku koduleheküljе või hooletult arvutisse torgatud andmekandja kaudu. Lunavara vastu aitab toimiv viirusetõrje, eriti väärtuslikuks vasturohuks on aga värske varukoopia.

Nuhkvara - Nuhkvaraks nimetatakse faile ja programme, mis paigaldatakse teie arvutisse ilma teie teadmata ja mis võimaldab salaja jälgida teie arvutikasutamist. Sageli satub nuhkvara teie arvutisse koos mingi Internetist tasuta allalaaditava tarkvaraga kui te ei loe tähelepanelikult litsentsitingimusi ja kohe nõustute allalaadimisega. Nuhkvara võib jälgida kasutaja veebisurfamisharjumusi, aga ka salvestada salasõna, klahvivajutusi ja ekraanipilte.

Pahavara - Ka kurivaraks nimetatakse sellist tarkvara, mida kasutatakse ilma omaniku teadmata tema arvutisse tungimiseks ja/või selle kahjustamiseks. Pahavara võib arvutisse sattuda CD-plaadil või muul andmekandjal, olla kaasa pandud e-kirjale, peidetud mõnda programmi või dokumenti, olla veebilehitseja alla laetud või tulla ise, aukliku või puuduva tulemüüri kaudu. Nakatunud arvutil võib kahjustada kõvaketast, emaplaati või mõnda muud seadet, pahavara võib arvutist kustutada olulisi andmeid või kasulikke programme.

Operatsioonisüsteem - Tähtsaim süsteemitarkvara hulka kuuluv programm, mis laaditakse alglaadimisprogrammi poolt ning mis juhib arvutisüsteemi tööd ja teenindab rakendusprogramme (Vallaste, 2016).

Distributsioon - Linuxi kerneli ümber loodud tarkvara, dokumentatsiooni ja tugiteenuste kogum (Distributsioon, 2010).

Tuum(*kernel*) - Ressursijaotust ja muid põhifunktsioone hõlmav operatsioonisüsteemi keskne osa ehk südamik. Arvuti käivitamisel laaditakse tuum kõigepealt muutmällu spetsiaalselt selleks ettenähtud kohta. Tuumale reserveeritud mälupiirkond on kaitstud, nii et sinna pole võimalik midagi muud salvestada. Kuna kernel jääb muutmällu kuni arvuti väljalülitamiseni siis peab ta olema võimalikult väike kuid samal ajal suutma teenindada operatsioonisüsteemi kõiki ülejäänud osi ja rakendusprogramme. Tüüpiline tuum vastutab mäluhalduse (*memory management*), protsessi- ja tegumijuhtimise (*process and task management*) ning kõvaketta halduse (*disk management*) eest (Vallaste, 2016).

Rakendusprogramm - Rakendus on lõppkasutaja tarbeks kirjutatud iseseisev tervilik programm (Vallaste, 2016).

Alias - Alias on lühikäsk, mis asendab pikema käsu või käskude jada (Alias, 2012).

Repositoorium - Repositooriumid ehk varamud on serverid, mis hoiavad endas Linuxile sobivat tarkvara. Varamute kasutamine annab eeldused, et need on kontrollitud, alati kõige uuema versiooniga ja sobivad kasutatava Linuxi versiooniga (Ubuntu server - SSH ühendus ja tarkvara repositoorium, kuupäev puudub). Tarkvara Linuxi varamutes on digiallkirjastatud ja iga tarkvarapaketi paigaldamisel seda kontrollitakse ning erinevuse korral paigaldamine peatatakse ja teavitatakse sellest. Sellist kaitsemehhanismi *Windows* puhul ei ole.

Metoodika - Korrastatud lähenemine suuremale tegevusele. Metoodika jaotab protsessi väiksemateks osadeks, püstitab osadele eesmärgid ning võib näidata ära meetodid nende eesmärkide saavutamiseks (Metoodika, 2013).

Metoodika

Autor kasutab sarnast metoodikat nii antud bakalaureusetöös kui ka juba valminud seminaritöö juures. Kuna metoodika on korra juba läbi proovitud, siis oli küllalt hea näha, mida muuta oleks vaja ning kus saaks täiustada. Samuti sai uuritud teiste teostatud uurimuste metoodikaid, millest lähtuvalt ka bakalaureusetöös kasutatud metoodikat sai parendada (Linux Security Review, 2015).

Töö peamiseks uurimisprobleemiks oli välja selgitada, kas alati on tasuline viirusetõrje parem kui tasuta viirusetõrje versioon ja seda erinavatel levinud tarkvaraplatvormidel (*MS Windows*, *GNU/Linux*, *Android* ja *iOS*). Iga viirusetõrjet testitakse järgnevate sammude järgi.

Kõigepealt toob autor välja testitava viirusetõrje kodulehe. Antud kodulehelt tuuakse välja nõuded, mida antud tõrje esitab arvutile või mobiilile. Näiteks millist operatsioonisüsteemi toetatakse või kui palju vaba ruumi programm vajab kõvakettal. Välja on toodud ka mälu vajadus puhtalt jooksmiseks ning kui võimsat protsessorit oleks vaja omada.

Teise sammuna tutvustatakse paigaldamise protsessi, mis algab allalaadimisest ja lõppeb esimese käivitamisega. Autor kirjeldab kõiki samme ja valikuid, mida läbima peab. Näiteks keele valik, millised lisad kaasa tulevad ning mida huvitavat kuvatakse paigaldamise käigus.

Järgmisena kuvatakse pilt, mis autoril avaneb esimest korda viirusetõrjet avades. Seejärel autor seletab, mis antud pildil kuvatud on. Lisaks tutvustatakse ülejäänud programmi ehk räägitakse sellest, millest pilti tegema ei hakatud. Selle osa üldnimeks on kasutajaliides.

Eripärade all toob autor välja põhilised funktsioonid, mis tasuvad ära mainimist. Samuti leiab seal funktsioone mida igal viirusetõrjel ei pruugi leiduda või on ainult testivale omased. Samuti peaks vastuse saama ka küsimusele kas antud viirusetõrjet oli mugav kasutada või ilmnes mingeid murekohti, millele peaks tähelepanu pöörama (Joonis 1).

Viimane osa jaguneb neljaks eksperimendiks viirusetõrjega (Joonis 2). Esimeses näeb kontrollimise tüüpe ning nende kiirust failide kontrollimisel. Teiseks näeme kui suurt mõju avaldab viirusetõrje arvuti protsessorile. Selleks jälgis autor kontrollide käigus protsessori kasutust(*CPU Usage*) ja protsessori maksimaalset sagedust(*Maximum Frequency*), mõlemaid ajaliselt seni, kuniks kogunes vähemalt 200 näitajat ning kirja läks tulemus, mida esines vähemalt viis korda. Testitaval arvutil on Intel® Pentium® CPU B960 @ 2.20GHz. Siin toon

välja näitajad *Linuxi* operatsioonisüsteemi puhul kui viirusetõrje veel ei kontrollinud(protsessori kasutus: 4-11% ja protsessori koormus: 36-56%) ja *Windowsi* operatsioonisüsteemil kui viirusetõrje veel ei kontrollinud (protsessori kasutus: 1-4% ja protsessori koormus: 36-44%). Kolmandaks katseks tuli allalaadida failid, mis kujutasid näiliselt endast viirust. Seda selleks et katsetada viirusetõrje käitumist kui viirus satub süsteemi ja näha kas viirusetõrje reaalselt kontrollib faile, mida kasutaja alla laadis. Kui ei suudetud allalaadimisel tuvastada viirust, kas siis hilisema kontrolli käigus avastatakse viirus. Testimiseks kasutasin EICAR(*European Institute for Computer Anti-virus Research*) faile. Tegemist on failidega, kus esineb ainult üks rida teksti, mis peaks aga äratama iga viirusetõrje tähelepanu. Arvutisse sai allalaaditud neli dokumenti: eicar.com, eicar.com.txt, eicar_com.zip ning eicarcom2.zip (Anti-Malware Testfile, kuupäev puudub). Antud faile sai kasutatud testimiseks kahel põhjusel. Esiteks soovitavad ja õpetavad viirusetõrjete tootjaid ise kasutajaid, kuidas antud failidega testida kasutatavat viirusetõrjet. Näiteks avasti juhend (Testing whether Avast Antivirus protects your computer against malware, 2016). Teine põhjus peitub turvalisuses, sest antud failid ei sisalda reaalset viirust. Seega muutes testimise protsessi kiireks ja ohutuks. Eicari testist ja kontrollitud failide arvust sekundis saab kokkuvõtteid vaadata lisast 1 (Joonised 31-36).

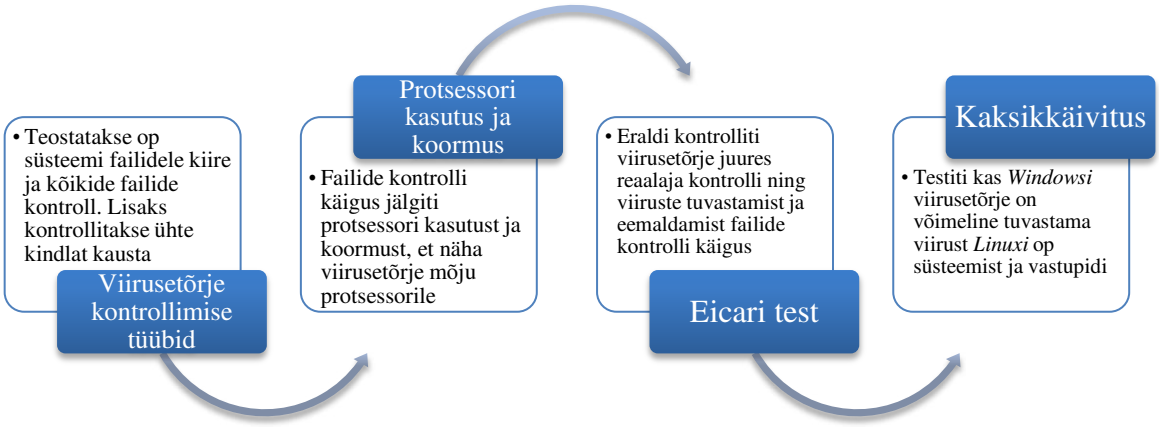
Neljandaks eksperimendiks on autor loonud kaksikkäivitusega süsteemi, mille käivitamisel saab kasutaja valida kas *Windows* 10 või *Linuxi* operatsioonisüsteemi. Kasutades reaalset viirust, mille nii *Windowsi* kui ka *Linuxi* puhul kopeeris kõvakettale. Teise viiruse jättis autor töölauale ning seejärel proovis viirust tuvastada ja eemaldada teisest operatsioonisüsteemist. Eesmärgiks oli näha, kas viirusetõrjed on võimelised leidma ja seejärel puhastama teist operatsisüsteemi.

Kõike hõlmavad tabelid ilmuvad lisa 1 all koos punktisüsteemiga (Tabelid 5-8), millest lühemat kokkuvõtet saab näha ja lugeda analüüsi all (Tabelid 1-4) koos punktijaotusega (Joonised 27-30).

Lisa 2 all saab tutvuda statistikaga, mis kujutavad endast pahavara kasvu nii arvutite kui telefonide puhul. Peale antud statistikaga tutvumist peaks iga kasutaja olema kindel viirusetõrje vajalikkuses ning seejärel paigaldama viirusetõrje nii oma telefoni kui arvutisse. Seejärel kontrollima uuendusi oma operatsioonisüsteemis ja varundama faile, muutes sellise teguviisi tavapäraseks iga teatud aja tagant.

Kolmanda lisa all on kasutajal võimalik tutvuda soovitustega, mida edaspidi jälgida võiks. Kõiki soovitusi järgides väheneb viirustega nakatumise oht märkimisväärselt!

Joonis 1. Metoodika



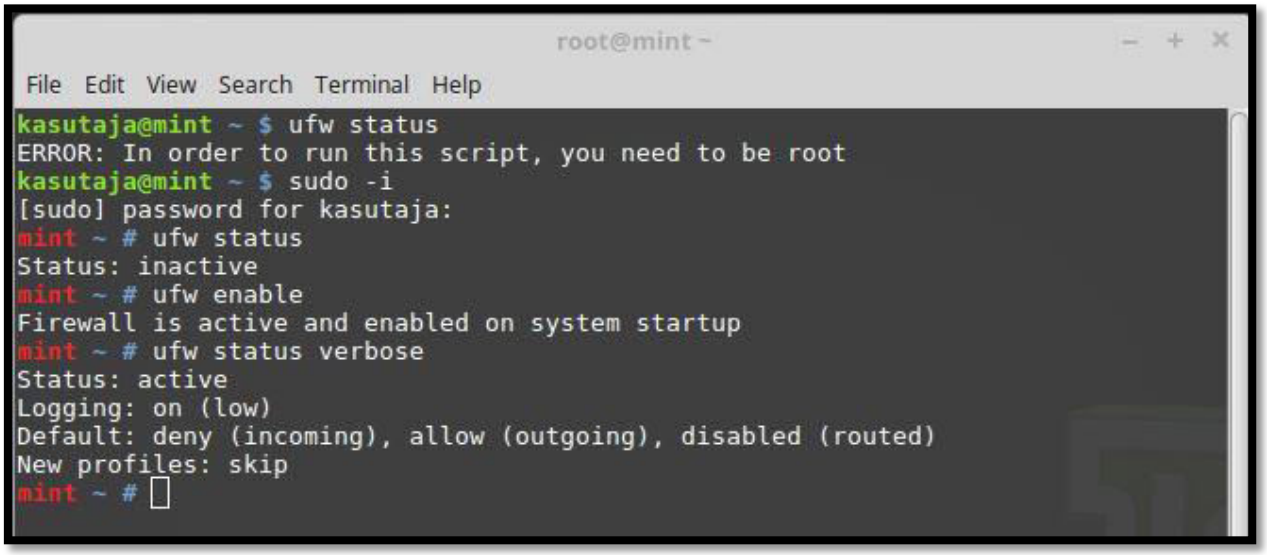
Joonis 2. Eksperimendid

1. Linux

Alustuseks mainiks ära, et tänapäeval on olemas pahavara ka *Linuxile*. Kui rääkida pahavarast suuremas plaanis, siis teada fakt on, et enamus pahavara on suunatud siiski *Windowsi* operatsioonisüsteemi kasutajatele (Linux Security - How Can Your Linux Be Hacked Using Malware, Trojans, Worms, Web Scripts Etc, 2015). *Windowsi* rakendused *Linuxis* ilma abita ei käivitu. Siinkohal tasuks ära nimetada ühilduvuskiht *Wine* ja tema edasiarendus nimega *PlayOnLinux* (Wine (software), 2016). *PlayOnLinux* on põhiliselt mängude paigaldamiseks ja kasutamiseks, mis on mõeldud *Windowsi* operatsioonisüsteemile, aga samuti leiab erinevaid rakendusi (I'd like to learn more about PlayOnLinux, kuupäev puudub). *Wine* suudab samuti paigaldada ja käivitada *Windowsile* mõeldud tarkvara *Linuxis*, kaasaarvatud viirusi (Wine and Linux Security, 2015). Seetõttu tuleks kindlasti kasutada viirusetõrjet siis kui kasutaja käivitab *Windowsi* tarkvara läbi ühilduvuskihi *Wine* või *PlayOnLinux*i oma *Linuxi* distributsiooni juures pidevalt või kasutab paralleelselt *Linuxiga Windowsi* operatsioonisüsteemi. Või vahetab tihedalt faile *Windowsi* kasutajatega.

Samuti on mõistlik luua *Linuxis* tavakasutaja(*Standard*), kellel on kasutajaõigused ning ta ei saaks näiteks paigaldada midagi ilma juurkasutaja salasõnata. Seegi muudaks viiruse leviku võimalikkust kasutatavas süsteemis märgatavalt. Siiski soovin ära mainida põhilise asjad, mida jälgida, et vältida pahavara sattumist oma süsteemi. Samuti tuleks tutvuda mõningate soovitustega kasutajale (Lisa 3).

Esimeseks tuleks sisse lülitada tulemüür, mis tavaliselt on välja lülitatud. Lisaks tuleks tulemüür ka seadistada vastavalt reaalsetele vajadustele. Minu poolt kasutatav süsteem on Linux Mint 18. Selleks pole vaja teha muud kui avada terminal. Logida sisse juurkasutajaga. Kontrollimaks kas tulemüür on sisse lülitatud kasutame käsku *ufw status*. Kui saame vastuseks *Status: inactive,* kirjutame terminali *ufw enable*. Kontrollimiseks sisestame käsu *ufw status verbose,* et näha kas tulemüür on nüüd sisse lülitatud. Lisaks näeme kas tulemüür keelab kõik sissetulevad ühendused aga lubab kõigil ühendustel väljuda (Joonis 3). Kui ühendused ei ole paigas peale tulemüüri sisselülitust, saame nad seada paika käskudega *ufw default deny incoming* ja *ufw default allow outgoing*, peale mida tuleks kontrollimiseks sisestada uuesti *ufw status verbose* (How to configure UFW, 2016). Lisaks võiks kasutajatele ära keelata ajastatud toimingute kasutamise - tekitada failid /etc/cron.deny ning kui on kasutusel siis ka /etc/at.deny ning iga kasutajanimi neisse failidesse eraldi realt.



Joonis 3. Tulemüüri sisse lülitamine Linux Mint 18 puhul

Teiseks tuleks *Linuxi* süsteemi pidevalt uuendada. Kuna uuendamine toimub läbi terminali, tuleks see muuta võimalikult kiireks ja mugavaks. Selleks avame terminalist sätetefaili käsuga *nano ~/.bashrc*. Kerides kogu faili läbi, peaksime leidma järgmised read:

if [-f ~/.bash_aliases]; then
. ~/.bash_aliases
fi

Samuti võivad antud ridade ees olla #, mis tuleks eemaldada, et kogu asi tööle hakkaks. Kui avatud sätetefail on tühi, siis kopeerige antud read tühja faili ning vajutage enter, et jätta tühi rida faili lõppu. Et salvestada avatud fail tekstiredaktoris *nano*, tuleks vajutada F3 ning klahvi enter ja seejärel väljuda klahviga F2. Järgmiseks loome uue faili terminalis käsuga *nano ~/.bash_aliases*. Sisestame sinna mõned aliased. Alias on lühikäsk, mis näeb välja selline: *alias lühend ='käsk 1 && käsk 2'*, samas võib piirduda ka ainult ühe käsuga. Sõna *sudo* kasutamine aliases käskude ees on vajalik siis kui luuakse käsud tavakasutajale. Juurkasutajale loodud aliastel pole seda vaja lisada. Järgnevas loetelus toon välja aliased, mis on loodud tavakasutaja jaoks:

alias u='sudo apt update && sudo apt upgrade && sudo apt clean', millega saame kätte kõik uuendused ja lisaks korrastame faile,

alias i='sudo apt install' ehk paigalda,

alias ae='sudo apt -y autoremove' ehk pakettide eemaldamine, mida ei vajata enam ning

alias f='sudo apt install -f', millega parandatakse sõltuvusi (Joonis 4).

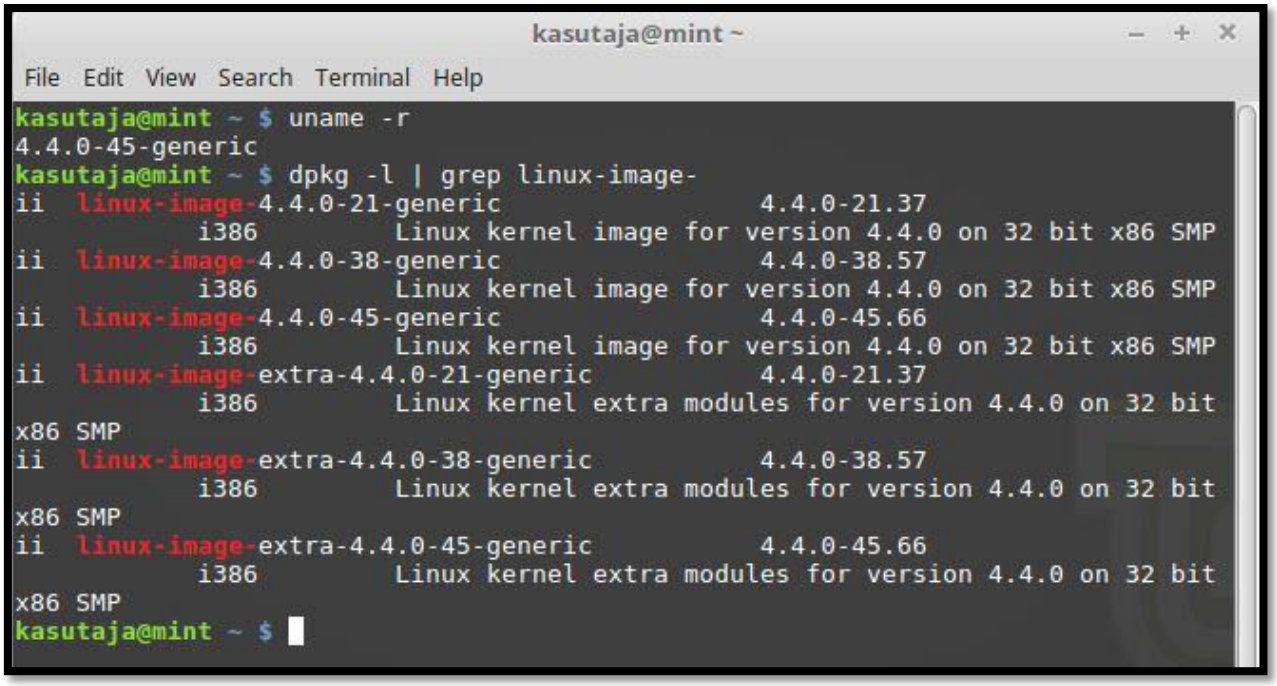
Jätke faili lõppu üks tühi rida ning salvestamiseks F3 ja klahvi enter. F2-ga väljume failist taaskord. Et kõik aliased tööle hakkaks, tuleb kasutajast välja logida ning seejärel kohe tagasi sisse logida. Peale seda võime kopeerida failid ka külaliste ning veel loomata kasutajate jaoks. Selleks kirjutame terminali *sudo cp .bashrc /etc/skel/* ning *sudo cp .bash_aliases /etc/skel/* (Alias, 2012). Kui nüüd soovime käivitada näiteks uuendamise ja korrastamise protsessi, siis avame terminali ning sisestame lihtsalt tähe u ja sisestame juurkasutaja salasõna.

Joonis 4. Fail *.bash_aliases* tavakasutaja jaoks Linux Mint 18 puhul

Uuendamisega kaasneb ka uute kernelite paigaldamine - turvakaalutlustel tuleks vanad kernelid eemaldada ja jätta alles vaid uusimad. Selleks on vaja kindluse mõttes sisestada terminali *sudo update-grub* peale tarkvarauuendust, et kindlustada järgmise taaskäivitusel juba uusima kerneli pealt laadimine. Peale taaskäivitust tuleks eemaldada vanad kernelid, et ei jääks turvariski süsteemi. Enne eemaldamist veenduda, et uus kernel toimib kõikides vajalikes funktsionaalsustes. Nii mõnigi viirusetõrje võib kompileerida paigaldamise käigus kerneli moodulid, mis ongi juhtprogrammid ehk *draiver'id*. Selle protsessi automaatseks toimimiseks peaks olema paigaldatud ka programm *dkms - Dynamic Kernel Module Support*. Kui sisestada terminali *which dkms*, siis programmi olemaolul kuvatakse asukoht arvutis. Kui nimetatud programmi ei leidu süsteemis, siis paigaldamiseks sisestame terminali *sudo apt install dkms* ning järgneb juurkasutaja salasõna. Kui vanad kernelid on eemaldatud, siis ei hakata nende jaoks ka enam kerneli mooduleid kompileerima ja tarkvara paigaldamine muutub kiiremaks. Ehk mis kasu on uuest ja turvalisest kernelist kui vanad ja auklikud on endiselt süsteemis ning nende kaudu saab ikka süsteemi sisse murda.

Vanade kernelite eemaldamiseks uurime kõigepealt välja, millise kerneli pealt hetkel laadimine toimub. Selleks sisestame terminali käsu *uname -r*, mis peaks kuvama kasutatava kerneli

versiooni. Kui kerneli versiooni ei kuvata, sisestame terminali juba varem mainitud *sudo update-grub* peale mida taaskäivitame arvuti. Peale taaskäivitust uuesti sisse logides peaks käsk *uname -r* töötama. Järgmiseks sisestame terminali käsu, millega kuvatakse kõik süsteemis olevad kernelid. Terminali kirjutame *dpkg -l | grep linux-image-* (Joonis 5).



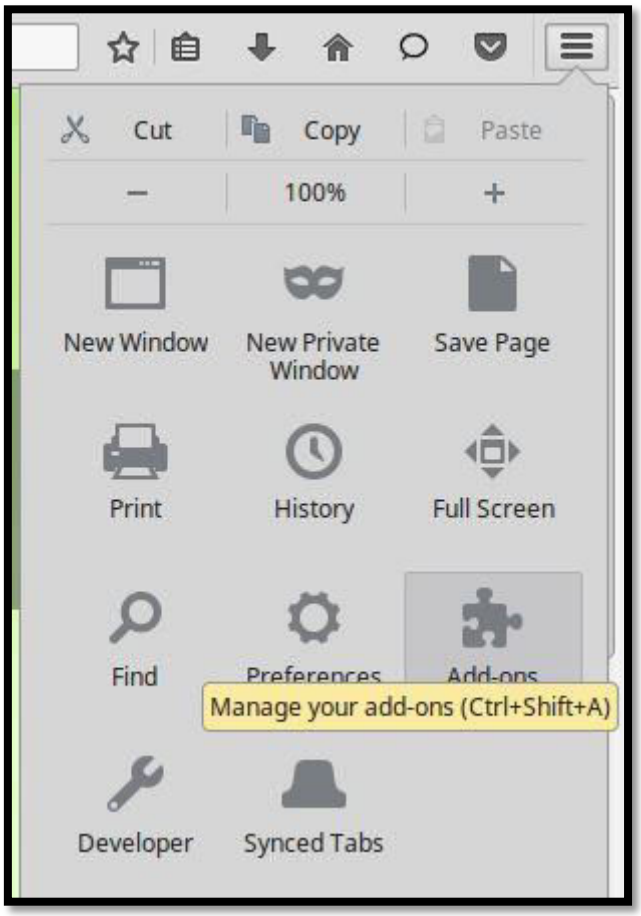
Joonis 5. Kõigi kernelite kuvamine Linux Mint 18 puhul

Enne eemaldama asumist tasub mainida, et alles tasuks jätta ka eelmise versiooni kernelid. Näiteks kui autori kasutatav süsteem kasutab kerneli versiooni *4.4.0-45-generic*, siis alles tasuks jätta ka versiooni *4.4.0-38-generic*. Eemaldama peaks kindlasti versiooni *4.4.0-21-generic*. Selleks sisestame terminali *sudo apt autoremove linux-image-4.4.0-21-generic* ning juurkasutaja salasõna. Veel peab kasutaja kinnitama oma otsust tähega y (*yes*) ja vajutama klahvi enter. Sarnaselt tuleks ka eemaldada *linux-headers*. Kuvamaks kõiki versioone kirjutame terminali *dpkg -l | grep linux-header*. Seekord peame eemaldama kaks 4.4.0-21 versiooni käsuga *sudo apt autoremove linux-headers-4.4.0-21 && sudo apt autoremove linux-headers-4.4.0-21-generic*. Taaskord tuleb lõplikuks eemaldamiseks sisestada nii juurkasutaja salasõna kui kasutaja nõusolekut näitav y ehk *yes* koos klahviga enter.

Samuti võiks olla kursis arvutiturvalisust puudutavate uudistega. Ettevaatlik tasub olla ja mitte paigaldada või käivitada kahtlast tarkvara. Selleks tuleks kontrollida interneti otsimootorist faili tausta ega selline tarkvara pahavara sisalda või uurida asjatundjate käest, kas selline tarkvara on neile tuttav ja turvaline kasutada. Samuti tasuks enne paigaldamist tarkvara viirusetõrje poolt

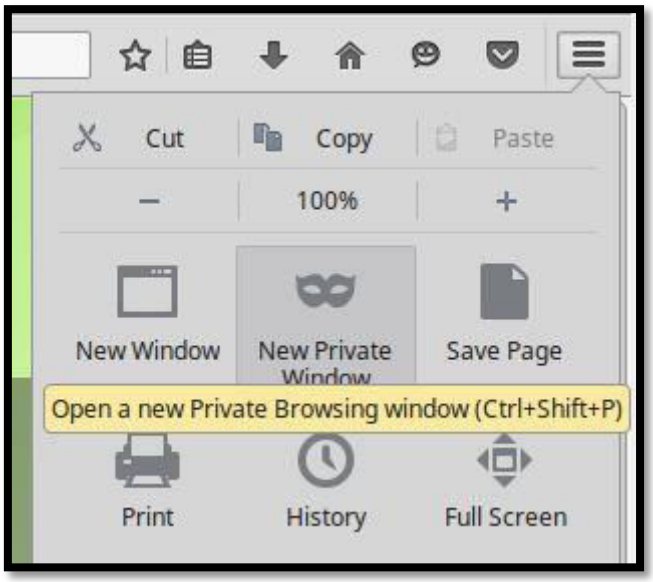
lasta üle kontrollida (Arvutikaitse ABC, kuupäev puudub). Samuti tuleks kasutada e-postiaadressi, mis sisaldaks eesnime punkt perekonnanime ätt(@) domeen punkt ee, sest seeläbi tekitame robotitele takistusi, kes veebilehti skaneerivad ja e-postiaadresse koguvad.

Järgmiseks liigume kõikidele levinud operatsioonisüsteemidele saadaoleva veebilehitseja juurde, milleks on *Firefox*. Kuna võib esineda erinevaid rünnakuid läbi *JavaScripti*, mis töötab otse veebilehitsejas. Esimene abinõu oleks paigaldada veebilehitsejasse lisa nimega *NoScript*. Selleks tuleb avada lehitseja ülevalt paremast nurgast seaded ning valida *Add-ons*, kust leiab otsides nimetatud lisa (Questions about Defragging or Antivirus, 2009). Samast kohast leiab ka lisa *Adblock*, mis on mõeldud reklaamide blokeerimiseks (Joonis 6). Näiteks eestikeelsete reklaamide tõrjumiseks leiab nimekirja siit http://adblock.ee/.



Joonis 6. *Add-ons* Linux Mint 18 puhul

Kasuks tuleb ka kui avada veebilehitseja privaatses režiimis. Antud režiimi saab avada veebilehitseja tööriistades alt, valides *New Private Window* või siis klahvidega CTRL+SHIFT+P (Joonis 7). *Google Chrome* ja *Chromiumi* puhul CTRL+SHIFT+N.



Joonis 7. Privaatse režiimi käivitamine Linux Mint 18 puhul

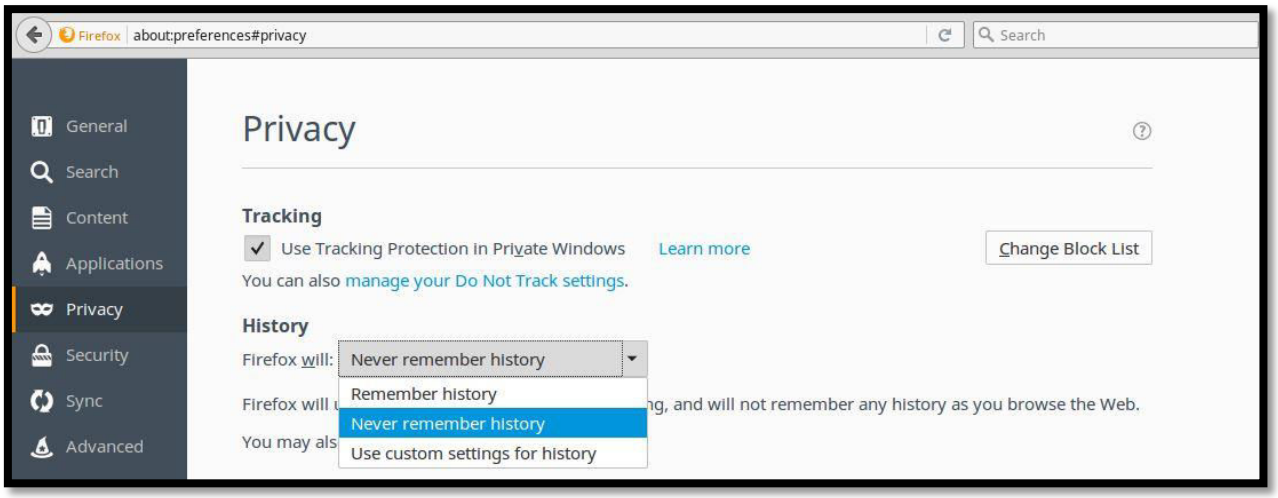
Et privaatne režiim koguaeg töötaks, tuleks muudatused sisse viia seadetes. Selleks tuleks avada ülevalt paremalt tööriistad ning valida *Preferences* > *Privacy* ning valik *Firefox will: Never remember history* (Can I set Firefox to always use Private Browsing, kuupäev puudub). Peale lehitseja taaskäivitust käivitub privaatne režiim. Võime ka aadressiribale kirjutada *about:preferences#privacy*, et avada antud seaded (Joonis 8). Võimalus on ka käivitusikooni teksti muuta selleks, et tagada privaatne režiim kohe Firefoxi käivitudes. See on sobilik eriti suure hulga kasutajate korral, nt organisatsioonis kus ei jõua iga kasutajakeskkonda eraldi seadistada. Siis on mõistlik seadistada vaikimisi kasutaja profiil (/etc/skel/) enne uute kasutajate loomist või domeenikasutajate sisselogimist. Järgnevaid tegevusi saab skriptide abil ka automatiseerida ja rakendada korraga suure hulga arvutite korral. Selleks tuleks kopeerida fail /usr/share/applications/firefox.desktop asukohta ~/.local/share/applications/firefox.desktop (siis ei muudeta rakenduste uuendamise käigus seda esialgseks tagasi) ja seejärel avada see tekstiredaktoriga (nt Gedit, Geany vms):

Exec=firefox **-private** %u (lisatud on rasvaselt märgitud parameeter)

Otsida *Exec* kirjet veel sellest failist - seda on vaja mitmes kohas muuta.

Google Chrome, Chromiumi puhul:

Exec=chromium-browser **--incognito** %U



Joonis 8. Privaatse režiimi sisse lülitamine *Firefoxis*

Autorina olen järgnevalt katsetanud nelja viirusetõrjet. Valik viirusetõrjete osas sai tehtud juba varem võrreldud andmete järgi, mille puhul kasutati sarnast metoodikat antud bakalaureusetööga. Kuna antud testid on läbi viidud aasta tagasi ja selle ajaga on paljud tootjad lõpetanud *Linuxi* viirusetõrje versiooni arendamise või toetamise. Seepärast jälgis, et viirusetõrje oleks endiselt toetatud tootja poolt (Linux Security Review, 2015). Operatsioonisüsteemiks sai valitud Linux Mint 18. Kui küsida, miks just see süsteem. Tegu on lihtsalt hetkel enam kasutatava Linuxi distributsiooniga ning selle uusima versiooniga (Linux Mint, 2016). Pean veel ära mainima siinkohal, et kui soovida uut tarkvara paigaldada mõnda kasutatavasse *Linuxi* süsteemi, siis *Linuxi* puhul on kõige ohutum kasutada selleks repositooriume ehk varamuid. Kui sealt endale antud tarkvara ei leita, siis üldjuhul ei jäägi muud üle kui tootja kodulehelt tarkvara allalaadida aga eelnevalt tuleks kindlasti konsulteerida spetsialistiga, enne kui paigaldama asutakse. Samuti tuleks jälgida tundmatute rakenduste paigaldamise või käivitamise puhul *sudo* kasutamist käskude ees, kuna läbi selle omistate juurkasutaja õigused. Selline tegevus on ebavajalik ja ülimalt ohtlik. Taaskord soovitaks enne küsida spetsialisti arvamust (Avoid 10 fatal mistakes in Linux Mint and Ubuntu, kuupäev puudub). Lisaks leidub turvalisi operatsioonisüsteeme, mille puhul on rohkem tähelepanu pööratud turvalisusele (Security-focused operating systems, 2016).

Paljud kasutajad arvavad ekslikult, et *Linuxit* kasutatakse veel väga vähe. Tegelikult kasutatakse *Linuxit* serverites ja just serverid on need, mis missioonikriitilist infot sisaldavad ja kogu taristut üleval hoiavad. Kui oleks suudetud, siis oleks serveritesse massiliselt sisse murtud pahavara abil. Ometi on *Linuxi* ülesehitus ja arhitektuur selleks piisavalt turvalised, et seda takistada.

1.1 Dr.Web anti-virus for Linux

Nõuded arvutile

Koduleht: http://www.drweb.com/

Operatsioonisüsteem: GNU/Linux koos kerneli versiooniga 2.6.x või hilisem

Vaba ruumi vajadus kettal: 512 MB (Dr.Web anti-virus for Linux, 2016).

Paigaldamine

Enne paigaldama asumist on rangelt soovitatav süsteemi uuendada kas aliase käsu abil või sisestades terminali: *sudo apt update && sudo apt upgrade && sudo apt clean*. Kuna antud viirusetõrjet kuskilt varamust allalaadida ei saa, peame leidma ta tootja kodulehelt. Turvalisuse kaalutlustel tuleks alla laadida ainult tootja kodulehelt ja enne allalaadimist tasub kontrollida ja veenduda veebilehe turvalisuses ja usaldusväärsuses. Seda kontrollida kas otsimootorite abil või mõne spetsialistiga konsulteerides. Paigaldamise alustamiseks vajutame hiire parema klahviga allalaaditud failile ning valime *Properties* ehk antud faili seaded. Valime *Permissions* ehk faili õigused. Sealt tuleks otsida rida *Execute: Allow executing file as program*, kuhu ette tuleks linnuke teha. Sellist tegevust oleks soovitav sooritada siiski ainult failiga, mille puhtuses kasutaja täiesti kindel on. Enne oleks siiski soovitav uurida faili kohta läbi interneti otsimootorite kui lubada neid käivitada või küsida mõne spetsialisti arvamust. Peale faili turvaliseks kuulutamist teeme topeltklõpsu allalaaditud failil, et alustada paigaldamist ning valime *Run in Terminal.* Teine võimalus paigaldamiseks on esimesena anda allalaaditud failile käivituse õigused käsuga *chmod +x faili_nimi.run*. Järgmiseks sisestame käsu faili käivitamiseks *./faili_nimi.run.* Viirusetõrje pakub võimaluse ühendada pilvega ning kasutaja peaks kindlasti lugema läbi litsentsilepingu enne kui edasi liigume paigaldamise protsessiga. Kuna tegu on tasulise viirusetõrjega, mida saab testida 30 päeva. 5 litsentsi hind 1 aastaks maksab €130.00, mis teeb ühe aastase litsentsi hinnaks €26.00. Peale edukat uuendust näeb viirusetõrje välja selline (Joonis 9).

Joonis 9. Dr.Web anti-virus for Linux

Kasutajaliides

Kui nüüd avakuvast (*Main page*) rääkida, siis vasakul küljel asub neli ikooni. Kaks neist ülemises ja kaks alumises nurgas. Kõige esimesele ikoonile vajutades kuvatakse avakuva. Teine ikoon kuvab karantiini (*Quarantine*) ja seal asuvad failid. Alumises nurgas esimene ikoon sisaldab endas viirusetõrje seadeid (*Settings*). Et seadeid muuta tuleb sisestada juurkasutaja salasõna. Seadete juures saab paika panna kui tihti kontrollitakse uuendusi automaatselt, kuidas reageerib viirusetõrje viiruse leidmise puhul, lisada erandeid, mida viirusetõrje kontrollima ei pea ning seada planeeritud kontrolle. Samuti paigaldada lisa *Link Checker*. Nimetatud lisa on võimalik seada blokeerima reklaame ja *flash* lisamooduleid ning kontrollima veebilehekülgi, et kasutaja kohta liiga palju andmeid ei kogutaks näiteks *Google Analyticsi* poolt. Välja lülitada ühenduse tootja pilvega (*Dr.Web Cloud*). Viimane ikoon mis kujutab endas küsimärki. Sealt saame avada viirusetõrje dokumentatsiooni, kus probleemidele lahendust otsida. Samuti on probleemide otsimiseks võimalik kasutajal avada tootja foorum. Kolmandaks võimaluseks abi otsida on helistada tehnilisele toele, mille info numbrite ja keelte kohta asub tootja kodulehel. Neljandaks on kasutajal võimalus registreerida kasutaja tootja kodulehel, et näiteks oleks võimalus soetada endale tootja tarkvara kunagi. Viimasena veel kuvatakse informatsioon

viirusetõrje kohta: milline viirusetõrje ja viirusetõrje mootori versioon on kasutusel ja millal viimane uuendus toimus.

Kui nüüd paremale poole liikuda, siis järgmiseks on kasutajal võimalik lohistada fail või kaust kontrolli. Võimalik on ka valida manuaalselt kaust või fail, mida viirusetõrje kontrollima peaks (*Drag files here or click to select*).

Avakuva paremal poolel on viis funktsiooni. Esimene neist nimega *SpIDer Guard*, mis kontrollib uusi ja muudetud faile ning blokeerib ohtlikke faile. Kuvatud on ka failide läbivaatamise kiirus.

Teine sarnase nimega *SpIDer Gate*, mis kontrollib juurdepääsu internetile ning blokeerib kõik sissetulevad ohtlikud objektid. Samuti on kuvatud failide kontrollimise kiirus.

Kolmandaks funktsiooniks on *Scanner*, kus on võimalik alustada erinevaid kontrolle. Esimene tüüp kannab nime *Express scan*, mis kontrollib kriitilisi süsteemi objekte. Järgmiseks on *Full scan* ehk kõigi süsteemis olevate failide kontroll. Kolmandaks on taaskord võimalik lohistada faile või kaustu kontrolli. Samuti on võimalik valida kasutajal mida viirusetõrje kontrollida võiks.

Neljas funktsioon on *Last update*, kus kuvatakse informatsioon, millal viidi läbi viimane uuendamine ja millal toimub järgmine. Samuti on võimalik manuaalselt käivitada kasutajal uuendamise protsess.

Viimaseks on *License* ehk litsents. Siin kuvatakse litsentsi informatsioon. Näiteks litsentsi number, omanik ning millal aktiveeriti ja kui millal litsents lõppeb. Samuti on kuvatud kui mitu päeva on litsentsi lõpuni ning võimalus soetada uus litsents (Joonis 9).

Keelte valikust niipalju, et valikuid on 9 ja eesti keel esindatud ei ole. Viirusetõrje keele muutmiseks tuleb muuta tootja kodulehe keel vastavaks kasutaja sooviga viirusetõrje keele osas.

Eripärad

Viirusetõrje seadete muutmiseks tuleb sisestada juurkasutaja salasõna. Uuendamine toimub vaikimisi iga 30 minuti tagant. Kolme tüüpi kontrolle ja võimalus seada planeeritud kontroll. Samuti saab faile või kaustu lohistada viirusetõrjesse kontrolli. Lisa nimega *Link Checker* ja funktsioonid *SpIDer Guard* ning *SpIDer Gate*. Tegu on tasulise viirusetõrjega.

Eksperimendid

1. Kontrollid

Express scan ehk kriitiliste süsteemi objektide kontroll - Objekte: 47 207, Aeg: 00:42:06

Custom scan ehk valikuline kontroll(kontrollin Home kausta) - Objekte: 330, Aeg: 00:00:32

Full scan ehk kõikide failide kontroll - Objekte: 213 915, Aeg: 02:55:57

2. Protsessor kasutus ja koormus kontrollide ajal

Protsessori kasutus: 52-60%

Protsessori koormus: 99%

3. Antud viirusetõrje test oli edukas. Kõikidele failidele reageeris kohe ning allalaadida ei õnnestunud ja leht, kust allalaadida üritasin faile, blokeeriti.

4. Viirusetõrjega asuti otsima viirust just valikulise kontrolli abil. Enne veel muudeti seadeid. Esiteks lülitati sisse pakitud faililaiendite kontroll ning määrati ajaline piirang kui kaua viirusetõrje ühe faili kontrollimine maksimaalselt võiks kesta. Tulemus tuli negatiivne ehk viirust *Windowsi* operatsioonisüsteemist ei suudetud tabada.

1.2 ClamAV Antivirus

Nõuded arvutile

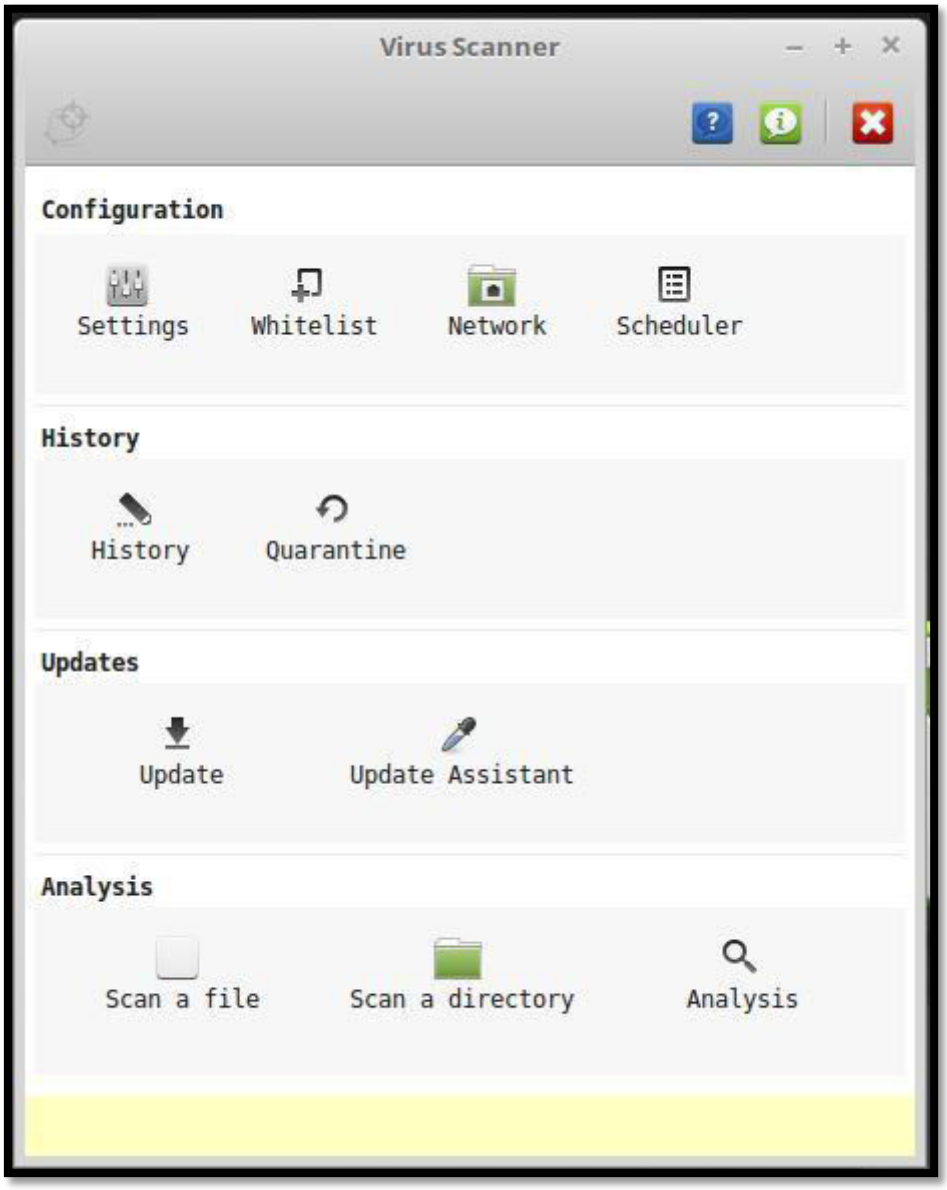
Koduleht: https://www.clamav.net.

Operatsioonisüsteem: Ubuntu, Debian, SuSE, RedHat & Fedora, Fedora & EPEL, Mandriva, Gentoo, Pardus (Linux Signatures, 2015).

Paigaldamine

Taaskord tuletan enne paigaldamise algust meelde uuendada süsteemi aliase käsu abil või kasutades terminali (*sudo apt update && sudo apt upgrade && sudo apt clean*). Viirusetõrje paigaldamiseks sisestame terminali *sudo apt install clamav clamav-daemon clamav-freshclam*.

Vahepeal küsitakse veel kasutaja nõusolekut. Piisab kui sisestada *y (yes)* ehk jah. Allalaaditud failidest niipalju et *clamav* on viirusetõrje mootor, *clamav-daemon* laeb vajalikud failid kontrollimiste korraldamiseks ning *freshclam* aitab viirusetõrjet uuendada(vaikimisi on seatud, et kontrollitakse uuendusi iga tunni tagant). Eraldi paigaldame graafilise viirusetõrje töölaua käsuga *sudo apt install clamtk*. Taaskord küsitakse kasutaja nõusolekut ehk sisestada tuleb *y (yes)* ehk jah. Kui nüüd avada start menüü töölaua alt vasakust nurgast ning valida *Accessories*, leiab viirusetõrje nimega *ClamTk* (Joonis 10).



Joonis 10. ClamTk

Kasutajaliides

Viirusetõrje on jagatud neljaks. Esimene on *Configuration* ehk konfiguratsioon, mis on omakorda jaotatud neljaks. Neljast esimene on *Settings* ehk seaded. Siin saame seada, mida viirusetõrje täpsemalt kontrollib ning seada faili suuruse ülempiiri. Järgmine funktsioon kannab nimetust *Whitelist*, kuhu saab lisada kaustu või faile, mida viirusetõrje kontrollima ei pea. *Network* all saab seada üles proksi võrgu kui kasutaja seda vajalikuks peab. Viimaseks on *Scheduler*, kus saame seda ühe planeeritud kontrolli kodukaustale ning panna paika, millal kontrollitakse viirusetõrje uuendusi. Uuendustele saab kasutaja kellaaega määrata vaid siis kui automaatne uuendamine on välja lülitatud kasutaja poolt.

Teiseks on *History* ehk ajalugu. Jaguneb kaheks, millest esimene kannab samuti nime *history*, kus kuvatakse kõik kontrollid ja uuendused, mis viirusetõrje on sooritanud. Teiseks funktsiooniks on *Quarantine* ehk karantiin, kuhu kogunevad kahjulikud failid, mis viirusetõrje avastanud on.

Kolmas funktsioonide kogum kannab nime *Updates*. Ka see jaguneb kaheks. Esimese funktsiooni *Update* all kajastub, kas uuendused on automaatsed või manuaalsed. *Update Assistenti* all saame muuta seda, kas viirusetõrje kontrollib ise uuendusi või teeb seda kasutaja manuaalselt. Kuigi viirusetõrje kuvab, et uuendus on saadaval, siis terminalist kontrollides logi käsuga *sudo nano ~/. /var/log/clamav/freshclam.log* kuvatakse informatsioon, et uuendused on allalaaditud. Samas käivitades uuendused manuaalselt käsuga *sudo freshclam -v*, kuvatakse kaks viga. Kui lülitada välja *freshclam* käsuga *sudo /etc/init.d/clamav-freshclam stop*. Ning seejärel sisestada uuesti käsk *sudo freshclam -v,* laaditakse uuendused alla kui neid on. Seejärel tuleks kindlasti *freshclam* uuesti sisse lülitada käsuga *sudo /etc/init.d/clamav-freshclam start*. Et muuta kui tihti kontrollitakse uuendusi automaatselt, tuleb muuta *freshclami* käsuga *sudo dpkg-reconfigure clamav-freshclam* (How to stop automatic freshclam execution, 2016).

Viimane on *Analysis*. Erinevaid funktsioone on siin kolm. Esimene neist on *Scan a file*, millega saame faile kontrollida. Järgmine kannab nime *Scan a directory*, mis erineb eelnevast selle poolest, et nüüd saan kontrollida failide asemel kaustu. Viimane funktsioon *Analysis*, kus on võimalik kontrollida failide mainet (Joonis 10).

Eripärad

Planeeritud kontrolli saab seada, aga ainult ühe. Saan küll kontrollida uuendusi ja isegi viirusetõrje kuvab info, et uuendused on saadaval, aga paigaldada ma neid läbi graafilise töölaua ei saa. Tegelikult viirusetõrje on uuendatud ja vajadusel saab käivitada uuenduste kontrolli ka manuaalselt. Failide puhul saab analüüsida nende mainet. Tegu on tasuta viirusetõrjega.

Eksperimendid

1. Kontrollid

File System kontroll - Objekte: 183 261, Aeg: 02:39:40

Custom Scan ehk valikuline kontroll(kontrollin Home kausta) - Objekte: 292, Aeg: 00:01:05

2. Protsessor kasutus ja koormus kontrollide ajal

Protsessori kasutus: 53-60%

Protsessori koormus: 99%

3. Antud viirusetõrje puhul oli test läbikukkumine. Sain kõik failid allalaadida ja avada ilma, et viirusetõrje oleks reageerinud. Kui lasin arvutit kontrollida, leidis kõigist midagi ohtlikku ning võimalus oli nad eemaldada või lisada karantiini. Kasutades antud viirusetõrjet, tuleks lasta viirusetõrjel kontrollida failid ja kaustad üle enne käivitamist!

4. Antud viirusetõrjel puudub valikuline kontroll, aga saab valida kaustu mida kontrollida. Seega kontrollisin kõiki kaustu mis asusid kõvakettal. Enne veel seadistasin viirusetõrje otsima ebavajalikke rakendusi, samuti faile mis algavad punktiga, 20 MB suuremaid faile ka kontrollima ning kaustu kontrollima rekursiivselt ehk vaadatakse üle ka kõik alamkataloogid. Viirusetõrje suutis tuvastada viiruse *widowsi* kõvakettalt, aga mitte töölaualt. Kahjuks ei olnud antud viirusetõrje võimeline eemaldama leitud viirust *Windowsi* operatsioonisüsteemist.

1.3 eScan Anti-Virus for Linux Desktops

Nõuded arvutile

Koduleht: http://www.escanav.com

Operatsioonisüsteem: RHEL 4 ja hilisem(32 & 64 bit), CentOS 5.10 ja hilisem(32 & 64 bit), SLES 10 SP3 ja hilisem(32 & 64 bit), Debian 4.0 ja hilisem(32 & 64 bit), OpenSuSe 10.1 ja hilisem(32 & 64 bit), Fedora 5.0 ja hilisem(32 & 64 bit), Ubuntu 6.06 ja hilisem(32 & 64 bit)

Protsessor: 1 GHz või kõrgem

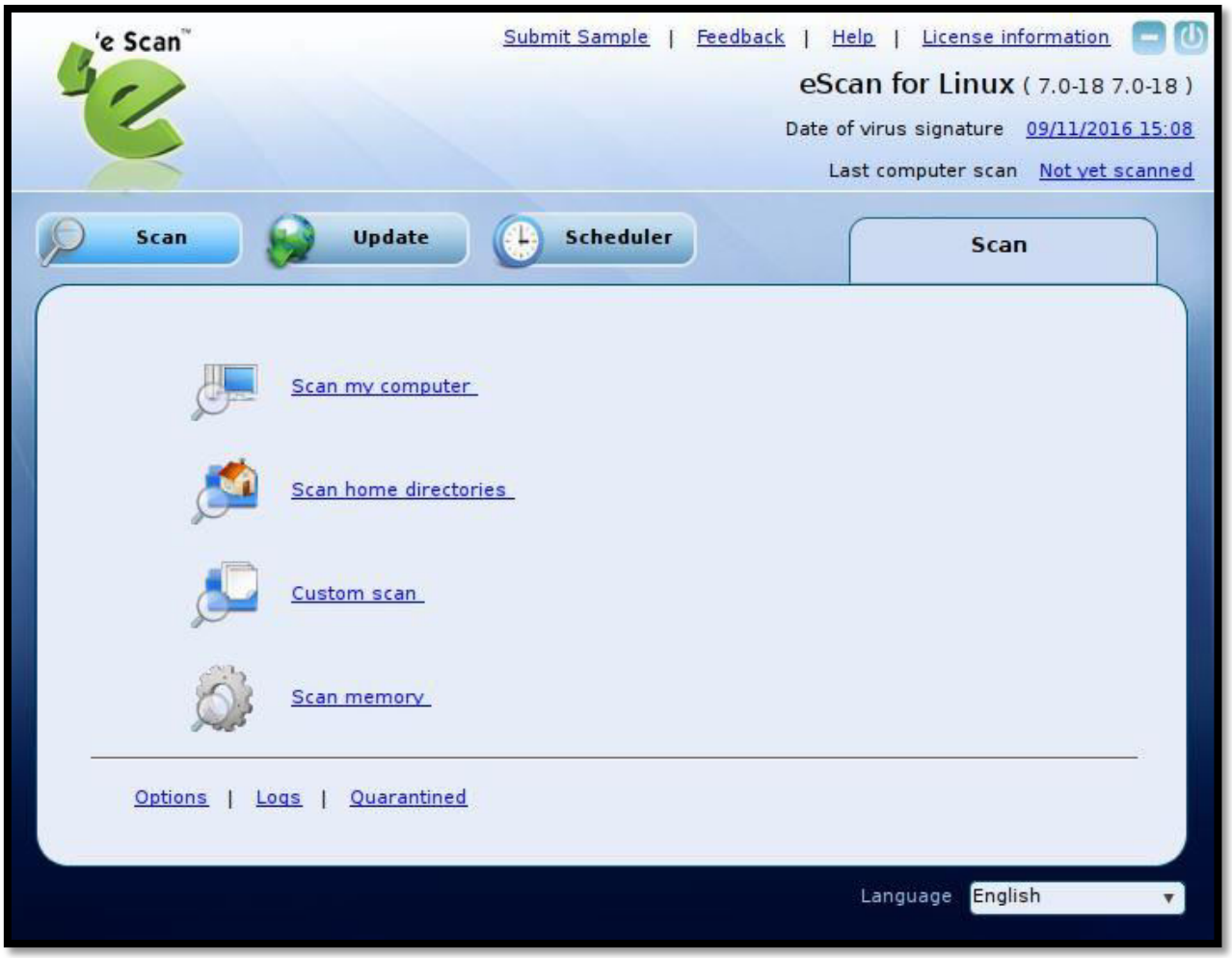
Mälu: 1 GB RAM või rohkem

Vaba ruumi vajadus kettal: 1 GB või rohkem (Will Your System Support This Software, 2016)

Paigaldamine

Kõigepealt uuendame süsteemi käsuga *sudo apt update && sudo apt upgrade && sudo apt clean* või kasutame aliase käske. Kuskil varamust ma antud viirusetõrjet ei leidnud. Kodulehel tuleb sisestada täisnimi, firmanimi, e-postiaadress ja elukohariik. Paigaldamiseks avan allalaaditud faili *GDebi Package Installeri* abiga. Kuvatakse sõltuvustega seotud viga veel enne paigaldamist: *Error: Dependency is not satisfiable libgcrypt11 (>= 1.2.2)*. Esimesena autor üritab probleemi lahendada paigaldades uusima *libgcrypt11* versiooni. Teiseks võimaluseks on muuta sõltuvusi, mida viirutõrje nõuab. Sõltuvuste muutmine peaks olema viimane abinõu sõltuvustega seotud probleemide lahendamiseks. Kui kasutaja otsustab antud võimaluse kasuks, siis kindlasti tuleb kasutajal kasutada enne interneti otsimootorite abi või konsulteerida mõne spetsialistiga, kes oskaks probleemi lahendada. Parimal juhul ilma sõltuvusi muutmata. Kõigepealt üritab autor siiski kasutada esimest võimalust ehk ise paigaldada nõutav sõltuvus. Selleks tuleb kasutajal mainitud sõltuvuse esmalt allalaadida. Veel enne alustamist mainin autorina ära, et testitav on 32-bitine operatsioonisüsteem ning sellest sõltuvalt on ka paigaldatav sõltuvuse versioon 32-bitine. Kasutaja peab kindlasti vastavalt tema arvutis kasutatavale süsteemile valima sõltvuse versiooni! Mitte ilmtingimata jälgima täpselt autori poolt tehtud paigaldamise protsessi. Kui nüüd liikuda edasi paigaldamise juurde, siis selleks sisestame esimesena terminali: *wget*

http://mirrors.kernel.org/ubuntu/pool/main/libg/libgcrypt11/libgcrypt11_1.5.3-2ubuntu4_i386.deb. Järgmiseks paigaldame antud sõltuvuse süsteemi: *sudo dpkg -i libgcrypt11_1.5.3-2ubuntu4_i386.deb*. Seejärel paigaldada viirusetõrje sarnase käsuga: *sudo dpkg -i Downloads/viirusetõrje_faili_nimi.deb* (Unable to install Springseed 2 on Ubuntu 15.04, 2015). Paigaldamise käigus kasutaja midagi viirusetõrje juures seadma ei pidanud. Peale edukat paigaldamist tekkis töölauale otsetee *eScan administrator*. Et muuta ja avada antud viirutõrje kõiki seaded, peame avama *eScan administration (root)*, mis asub start menüü *eScan Antivirus* all. Kuna tegu on tasulise viirusetõrjega, siis esimesel käivitusel soovitakse litsentsi sisestamist või võimalusel litsentsi soetamist. Võimalus on ka keelduda litsentsi sisestamisest/soetamisest ning seeläbi saab kasutaja viirusetõrjet 30 päeva testida. Ühele seadmele üheks aastaks maksab antud viirusetõrje €17.60. Järgmiseks soovitakse käivitada uuendus. Peale mõningate seadete sättimist viirusetõrje käivitus juurkasutaja õigustes ning viirusetõrje näeb välja selline (Joonis 11).



Joonis 11. eScan administration (root)

Kasutajaliides

Alustades kõige ülevalt, kus asub *Submit Sample*, millele vajutades avatakse veebilehitseja, kus tuleb täita mõned väljad ja võimalus lisada fail, mida kasutaja soovib saata analüüsi. Järgmine *Feedback* ehk tagasiside võimaldab kasutajal anda oma hinnang viirusetõrjele, mis aitab tulevikus tootjal paremat toodet toota. Kolmandaks on *Help*, kus abi saamiseks on neli võimalust. Esimeseks võimaluseks on alustada vestlust tootjaga. Teiseks võimaluseks on tutvuda viirusetõrje enda vikipeediaga. Kolmas võimalus on külastada tootja foorumit ning viimaseks pakutakse diagnostika sooritamist viirusetõrjele ja tulemuste saatmist tootjale. Neljandaks on viirusetõrje paremas nurgas *License information*, kus on on välja toodud kehtiv litsents ja tema kestvus. Samuti on võimalik sisestada uus litsents või uus litsents soetada.

Paremalt alla tulles on välja toodud viirusetõrje versioon. Järgmisel real on viimane uuenduste kontrolli aeg ning kolmandal viimase tehtud kontrolli kellaaeg.

Kui nüüd vasakule tagasi liikuda, siis esimene on *Scan*, mille kõik valikud on kujutatud avakuval. Neist esimene on kõigi failide kontroll ehk *Scan my computer*. Järgmiseks on *Scan home directories*, mis kontrollib sisselogitud kasutaja kodu kausta. Kolmandaks on kontroll, mis laseb kasutajal valida millist kausta või faili kontrollitaks ehk *Custom scan*. Viimane *Scan memory* kontrollib arvutis käivitatud ja töötavaid protsesse. *Options* ehk valikud lasevad kasutajal paika panna, kuidas tegutseb viirusetõrje viiruse leidmisel ning määrata faile või kaustu, mida ei kontrollita. Samuti on võimalik määrata faililaiendeid, mida ei kontrollita ja sisse lülitada kontroll, mis vaatab üle kõik käivitatud protsessid arvuti käivitusel. Logide ehk *Logs* alla tekivad kõikide kontrollide kokkuvõtted ning karantiinis (*Quarantine*) on kõik failid, mis on viirusetõrje poolt tuvastatud ohtlikud failid, mida ei ole õnnestunud puhastada pahavarast.

Järgmiseks on *Update*, kus näeb, millal toimus viimane uuenduste kontroll ning kas protsess on automaatne või manuaalne. Veel saab kasutaja algatada uuendamise protsessi ning muuta kui tihti kontrollitakse uuendusi ja panna paika kui mitu päeva vanad võivad olla viiruse signatuurid enne kui viirusetõrje hoiatab kasutajat. Samuti vaadata logisid, kus kuvatakse viimaste uuenduste kokkuvõtted.

Kõige alt paremast nurgast on võimalik vahetada keele eelistust. Valikuid on 10, kuid eesti keel puudub (Joonis 11).

Eripärad

Saab seada planeeritud kontrolle ja faili saab saata toojale analüüsi. Keeltevalik on olemas ja automaatne uuendamine ka. Reaalaja kaitse ei tööta ning esines probleem sõltuvustega paigaldamisel. Probleemide lahendamiseks on erinevaid võimalusi. Tegu on tasulise viirusetõrjega.

Eksperimendid

1. Kontrollid

Valikuline kontroll(kontrollin Home kausta) - Objekte: 4079, Aeg: 00:03:44

Kõigi failide kontroll - Objekte: 463 235, Aeg: 03:06:05

2. Protsessor kasutus ja koormus kontrollide ajal

Protsessori kasutus: 56-63%

Protsessori koormus: 99%

3. Antud viirusetõrje puhul oli test ebaõnnestumine. Kõik failid sain allalaadida ning avada ilma, et viirusetõrje kuidagi neile reageeriks. Kui lasin kontrollida arvutit, siis leidis kõigist midagi ja lisas failid karantiini. Kui kasutada antud viirusetõrjet, siis taaskord kontrollige failid ennem üle, kui hakkate paigaldama või käivitama.

4. Kasutan taaskord valikulist kontrolli, mille sean kontrollima kõvaketast. Enne veel seadistan viirusetõrje maksimaalse tulemuse saavutamiseks. Selleks lülitan sisse valiku, mis tagab et kontrollitakse ka alamakatalooge ja pakitud faile. Tulemuseks on kahe viiruse leidmine ning eemaldamine *Windowsi* operatsioonisüsteemist. Antud viirusetõrje suutis leida viiruse nii kõvakettalt kui ka töölaualt.

1.4 ESET NOD32 Antivirus 4 for Linux Desktop

Nõuded arvutile

Koduleht: https://www.eset.com

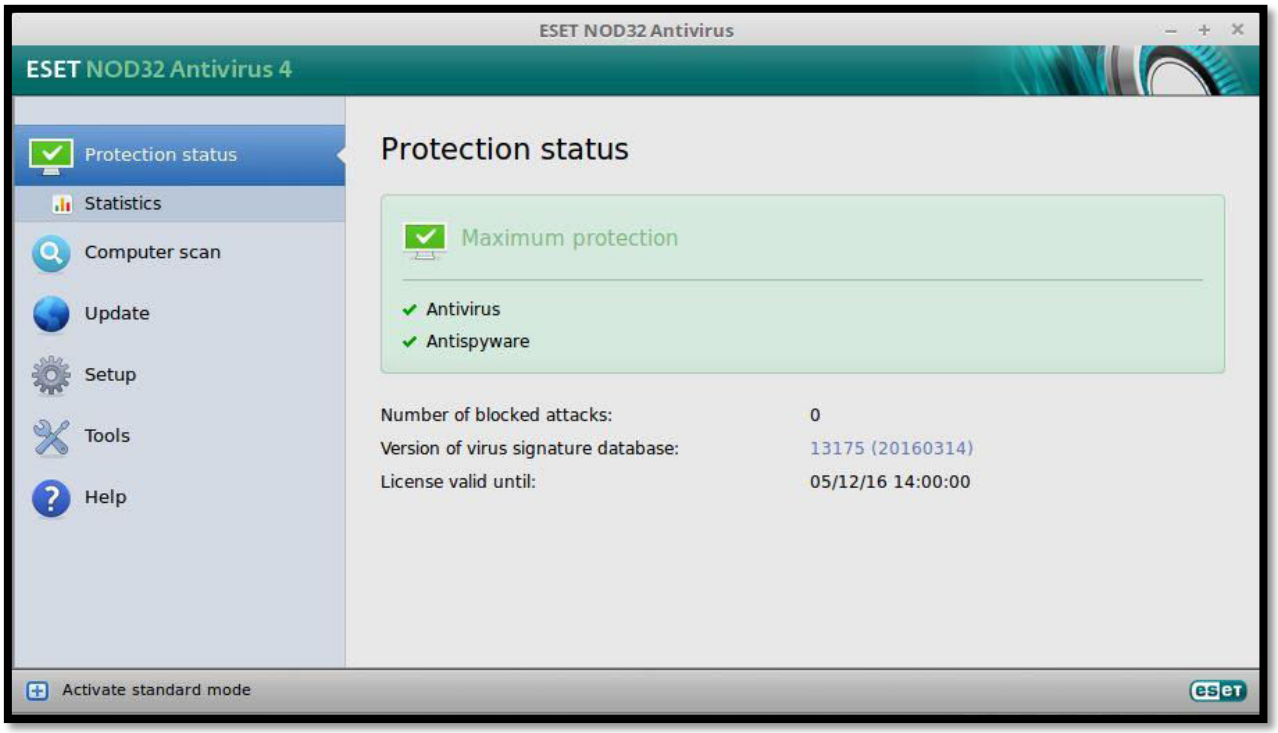
Operatsioonisüsteem: Debian 6.0.7, Fedora 18, Mandriva, Red Hat, SuSE, Ubuntu 12.10 ning kernel 2.6 või kõrgem

Protsessori arhitektuur: 32bit ja 64bit (ESET NOD32 Antivirus 4 for Linux Desktop FAQ, 2016)

Paigaldamine

Kõige esimesena uuendame süsteemi kasutades terminali (*sudo apt update && sudo apt upgrade && sudo apt clean*). Samuti on võimalik kasutada aliase käske kui kasutaja need seadnud on. Kuna taaskord ei õnnestunud viirusetõrjet varamutest leida, tuleb viirusetõrje allalaadida tootja kodulehelt. Veel enne kui edasi liigume, mainin ära, et antud viirusetõrje on tasuline. Üheks aastaks ühele arvutile maksab $39.99 (u. €36.10). Tasuta saab proovida 30 päeva. Keeli, mille vahel valida on tervelt 20, kuid eesti keel sinna ei kuulu. Viirusetõrje versioone on kaks: 32-bit või 64-bit. Paigaldamise alustamiseks vajutame hiire parema klahviga allalaaditud failile ning valime *Properties* ehk antud faili seaded. Nüüd *Permissions* ehk faili õigused. Sealt tuleks otsida rida *Execute: Allow executing file as program*, mille ette tuleks linnuke teha. Sellist tegevust soovitan sooritada siiski ainult failiga, mille puhtuses kasutaja täiesti kindel on. Enne oleks soovitavalt uurida faili kohta läbi interneti otsimootorite kui lubada faili käivitada või uurida mõne spetsialisti käest lisainformatsiooni. Kui fail on turvaline, teeme topeltklõpsu allalaaditud failil, et alustada paigaldamist. Küsitakse veel juurkasutaja salasõna. Kuvatakse nõuded arvutile ja muu informatsioon viirusetõrje kohta. Esialgu tuleb vajutada *Next* ehk järgmine. Vajalik on läbi lugeda ja seejärel nõustuda lõppkasutaja litsentsiga. Paigaldamiseks saab valida kas *Typical* ehk tüüpilise meetodi, mis on viirusetõrje poolt soovitav. Antud valik teeb kõik otsused kasutaja eest ära. Kui kasutaja soovib mõnda asja ise paika panna, siis saab valida ka *Custom* ehk võimalus näiteks paika panna kasutajad, kes saavad viirusetõrje seadeid muuta hiljem. Lõpuks saamegi vajutada *Install* ehk paigalda. Peale edukat paigaldamist soovitakse veel teha taaskäivitus. Peale taaskäivitust peame viirusetõrje aktiveerima. Kui kasutajal on ostetud litsents, siis võite kasutajaga sisse logida ja seeläbi litsentsi aktiveerida. Teine võimalus on proovida prooviversiooni. Prooviversiooni aktiveerimiseks tuleb sisestada eesnimi, perekonnanimi, e-

postiaadress ning kodukohariik (How do I Download and Install ESET NOD32 Antivirus 4 for Linux Desktop, 2016). Peale küsitud info sisestamist viirusetõrje käivitub ning hakkab ennast kohe uuendama. Viirusetõrje näeb välja selline (Joonis 12).



Joonis 12. ESET NOD32 Antivirus 4 for Linux

Kasutajaliides

Antud viirusetõrjel on kaks erinevat režiimi. Esimene neist on *standard*, mille avakuva jaotub viieks. *Advanced* režiim jaotab viirusetõrje kuueks, tuues juurde erinevaid funktsioone, millest kohe lähemalt räägin. Nimetatud režiime saab kasutaja muuta viirusetõrje all vasakus nurgas.

Esimene on *Protection status*, kus näeme, et viirusetõrje töötab. Samuti blokeeritud rünnakute arvu, viirusetõrje versiooni ning kaua litsents veel kehtib. Siit saame veel avada *Statistics* ehk statistika, kus kuvatakse viirusetõrje töö kohta informatsiooni. Näiteks kui palju on nakatunud-, puhtaid- või puhastatud objekte.

Teiseks on *Computer scan*, kus saame valida kahe kontrollimise tüübi vahel. Esimene neist on *Smart scan*, mis kontrollib kohalikku ketast. Teiseks tüübiks on *Custom scan*, kus kasutaja saab valida mida täpsemalt kontrollitakse.

Kolmandaks ülevalt on *Update*. Seal saab uuendada viirusetõrjet ja litsentsi. Samuti näha, millal viimati uuendati antud viirusetõrjet ning andmebaasi versiooni.

Neljas kannab nime *Setup*, kus näeb ära, et reaalaja kaitse on sisse lülitatud. Saab selle vajadusel välja lülitada või muuta mõningaid seadeid.

Järgmiseks on *Tools* ehk tööriistad, kus saab tutvuda viirusetõrje poolt loodud kontrollimiste logidega. Kontrollida faile, mis asuvad karatiinis ning planeerida uuendusi või kontrolle. Samuti saab tootjale saata kahtlase faili lähemalt uurimiseks.

Viimaseks on *Help*, kuhu saab pöörduda kui peaks probleeme tekkima viirusetõrjega. Saame avada probleemide lahendamiseks faili või otsida abi internetist läbi viirusetõrje. Samuti näeme viirusetõrje versiooni ning kaua litsents veel kehtib (Joonis 12).

Eripärad

Kontrollide planeerimine ning automaatne uuenduste kontroll. Statistika eraldi välja toodud. Reaalaja kaitse ja faili saab saata põhjalikumale uurimisele. Kaks erinevat režiimi, mis erinevad üksteisest funktsioonide arvu poolest. Tasuline viirusetõrje.

Eksperimendid

1. Kontrollid

Smart scan ehk kohalikku ketta kontroll - Objekte: 379 083, Aeg: 01:00:16

Custom scan ehk valikuline kontroll(kontrollin Home kausta) - Objekte: 821, Aeg: 00:00:07

2. Protsessor kasutus ja koormus kontrollide ajal

Protsessori kasutus: 41-60%

Protsessori koormus: 99%

3. Antud viirusetõrje puhul oli test edukas. Esimesele kahele failile reageeris kohe. Laiendiga .zip lasi esialgu allalaadida ning reageeris lahti pakkimisel. Käivitades faile viirusetõrje reageeris koheselt. Samuti leiti hilisema kontrolli käigus failid laiendiga .zip olevat ohtlikud ning eemaldati süsteemist.

4. Viiruste tabamiseks kasutan valikulist kontrolli. Lasen viirusetõrjel kontrollida kõvaketast, aga enne seadistan natukene. Juurde lisan ebavajalike rakenduste otsimise koos reklaami ja nuhkvara tabamisega. Samuti panen paika limiidid kui suurt faili kontrollitakse kui pikalt ajaliselt faili maksimaalselt kontrollitakse ning mitut taset pakitud faili puhul kontrollitakse. Sellele kõigele järgnes positiivne tulemus sest viirusetõrje suutis leida ja eemaldada mõlemad viirused *Windowsi* operatsioonisüsteemist.

2. Windows

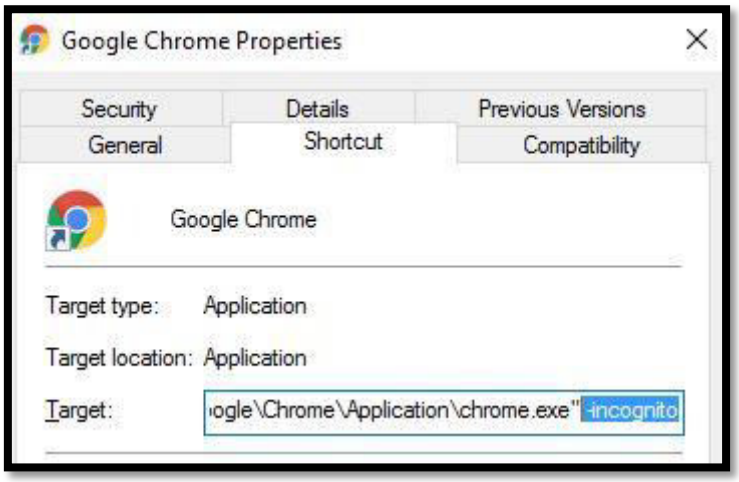
Hetkel kui *Windows* on endiselt üks populaarsemaid operatsioonisüsteeme maailmas, siis tänu sellele rünnatakse sageli just *Windowsi* kasutajaid rohkem kui teisi operatsioonisüsteeme (Hoffman, 2013). *Windows* on teinud suuri samme tagamaks oma kasutajatele ohutust. Selleks on loodud programmid *Windows Defender*, *Windows Hello* ja kodukasutajatele veel arendatav *Device Guard*, mis hetkel töötab ainult Enterprise versiooniga. Viimane mainitud programm ei lase tundmatutel failidel käivituda (Hallum, 2015). *Windows Hello* ei tööta samuti kahjuks kõikidel arvutitel. Selleks peab olema arvuti varustatud kas sõrmejäljelugejaga või kaameraga, mis toetab sõrmejäljelugemist. Seljuhul suudab kaamera teha vahet nägudel või silma iiristel, mille kaudu tulevikus arvutisse sisse logida (Mis on Windows Hello, 2016). *Windows Defender* saab iga *Windowsi* versiooniga uuendusi, aga ometi ei piisa sellest, et hoida arvuti kaitstud ning just sel põhjusel on soovitav eraldi paigaldada endale viirusetõrje ning tutvuda lähemalt soovitustega kasutajale (Lisa 3).

Autorina mainiksin ära mõningaid tähelepanekud, kuidas enda arvutit ja andmeid veelgi kindlamalt kaitsta. Alustame kasutajatest millega arvutisse sisenetakse. Soovitav oleks omada kahte kasutajakontot. Ühel, millel on administraatori õigused ja teisel, millel neid pole ehk piiratud õigustega kasutaja. Mõlemal kasutajal peaks kindlasti olema seatud salasõna. Administraatorina logida sisse ainult siis kui see on hädavajalik. Igapäevatöö tegemiseks kasutage piiratud õigustega kasutajat (Dreifeldt, 2015). Piirantud õigustega kasutajasse sisenemiseks võime näiteks kasutada *microsofti* kontot. Seljuhul võiks kasutaja lisada *microsofti* konto alla mõne teise kasutatava e-postiaadressi või telefoninumbri. Seda selleks, et parooli ununemisel või seadme varastamise tõttu saaksite ennast tõendada läbi lisatud e-posti või telefoninumbri ja salasõna kiiresti ära muuta või unustamise korral taastada. Igatahes salasõnu ei tohi mistahes ettekäändel jagada mitte kellegiga!

Teise asjana tuleks tähelepanu pöörata, et operatsioonisüsteem ja rakendusprogrammid, mida kasutate oleksid uuendatud viimasele versioonile. Samuti võiks rakendusprogrammide puhul jälgida tootjat ja otsida lisainformatsiooni tootja kohta (Dreifeldt, 2015). Kui tootja kohta palju informatsiooni ei leidu, jätke antud programm paigaldamata või uurige lisa spetsialisti käest.

Kolmandaks soovituseks oleks arvutis kasutatav veebilehitseja käivitada privaatses režiimis. Privaatse režiimi saab kiirelt käivitada: *Internet Explorer*, *Microsoft Edge* ja *Mozilla Firefox* - CTRL+SHIFT+P, *Google Chrome* ja *Opera* - CTRL+SHIFT+N (Turvaline surfamine, kuupäev

puudub). Privaatne režiim tagab selle, et veebilehitseja ei jäta tundlikku infot meelde - külastatud aadresside ajalugu, sessioonide küpsiseid, sisestatud vormide infot ning salasõnu. Et muuta näiteks *Google Chrome* koguaeg privaatses režiimis avatavaks, ei tule teha muud kui avada töölaual oleva ikooni seaded(*Properties*), vajutades ikoonil hiire parema klahviga ning lisada avatava faili asukohale(*Target*) lõppu tühikuga eraldatud märge *-incognito* (Joonis 13).



Joonis 13. Privaatse režiimi aktiveerimine *Google Chrome* puhul

Neljandaks soovituseks oleks regulaarsete varukoopiate tegemine arvutist. Hoiustage neid eraldi andmekandjal, näiteks plaadil või välisel kõvakettal. Soovitav oleks neid hoida teises ruumis või koguni teises hoones. Veelgi parem oleks omada mitut varukoopiat, mis asuksid üksteisest eraldi (Dreifeldt, 2015). Peale varukoopiate on võimalik *Windows 10 PRO* omanikel krüpteerida kõik kasutusel olevad kettad lisaga *BitLocker*. Krüpteeritud andmed on loetavad ja käivitatavad alles peale võtmega avamist (Paul, 2016). Näiteks varastatud arvutil, mille andmed on krüpteeritud ei saa varas andmeid kuritarvitada ilma võtmeta. *Windows 10 HOME* ja teiste versioonide kasutajatel on kaks võimalust. Kas kasutada mõnda teist krüpteerimise tööriista või soetada endale PRO versioon. Enne andmete krüpteerimist on rangelt soovitatav luua varukoopia süsteemist!

Nagu varem mainitud, peaks igas arvutis olema lisaks *Microsoft Defenderile* veel üks viirusetõrje. Viirusetõrjete valikust niipalju, et eesmärgiks oli valida kaks tasuta versiooni (The Best Free Antivirus Preotection of 2016, 2016) ning kaks tasulist versiooni (The Best Antivirus Protection of 2016, 2016). Operatsioonisüsteemiks sai valitud *Windows 10.*

2.1 Avast Free Antivirus 2016

Nõuded arvutile

Koduleht: https://www.avast.com

Operatsioonisüsteem: Windows 10, 8.1, 8, 7, Vista, XP SP3

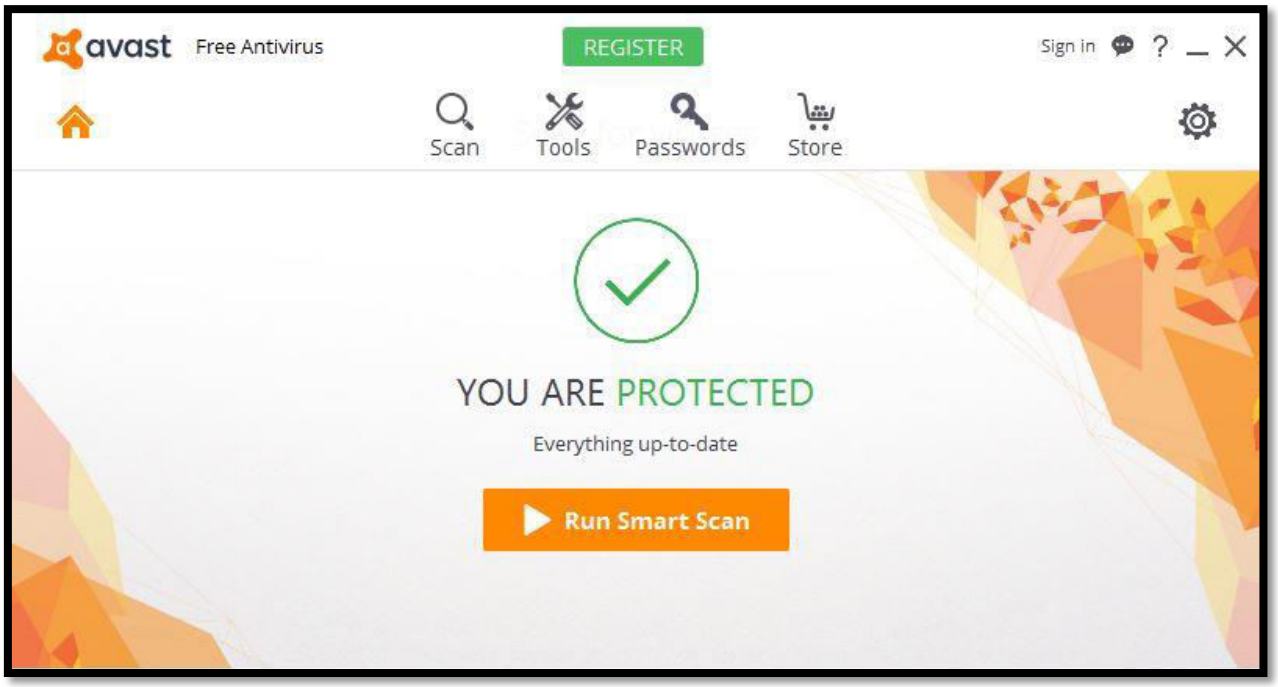
Mälu: 256 MB RAM

Vaba ruumi vajadus kettal: 2 GB (What are the system requirements for Avast 2016, kuupäev puudub).

Paigaldamine

Käivitades viirusetõrje kodulehelt allalaaditud faili, siis esimese asjana tuleb kindlasti läbi lugeda litsentsileping. Järgmiseks tuleb valida kas *Install* ehk paigalda, kus kõik valikud tehakse kasutaja eest ära. Teiseks variandiks *Customize* ehk kohandatud paigaldamine. Teise variandi puhul saab kasutaja paika panna, kuhu paigaldatakse ning mis lisad paigaldadakse koos viirusetõrjega. Esimesel käivitusel viirusetõrje annab teada, et tootja kogub viirusetõrje kasutajate kohta informatsiooni. Veel pakutakse *Androidi* telefonile *avasti* viirusetõrjet. Edasi liikudes saame lõpuks viirusetõrjet kasutama hakata.

Peale paigaldust otseselt kasutajat tegema ei sunnita, aga ilma kasutajat tegemata üle 30 päeva antud tõrjet kasutada ei saa. Peale kasutaja tegemist saab kasutaja kasutada viirusetõrjet terve aasta. Registreerimiseks tuli lihtsalt sisestada oma e-postiaadress. Keelte pakette saab juurde paigaldada, aga ainult administraatori kasutajas olles. Eesti keel on esindatud ja välja näeb ta selline (Joonis 14).



Joonis 14. Avast Free Antivirus

Kasutajaliides

Viirusetõrje on jaotatud kuueks osaks, millest esimene märgike asub üleval vasakus nurgas viirusetõrje nime all ning meenutab maja. Et liikuda avakuvale tagasi ükskõik millise funktsiooni seadete juures olles, tuleb vajutada kaks korda antud märgile. Esimene vajutus toob tagasi keskmised neli viirusetõrje osa ning teine vajutus taastab terve avakuva. Veel saame avakuvalt alustada nutikat kontrolli ehk *Smart Scan*, mida pikemalt tutvustab hiljem. Samuti kuvatakse informatsioon, et arvuti on kaitstud ning hetkel kasutatakse uusimat versiooni viirusetõrjest. Kasutajat saame registreerida viirusetõrje avakuva üleval keskel, kus asub roheline nupp *Register*. Kasutaja on vajalik registreerida kui viirusetõrjet soovitakse testida üle 30 päeva. Kasutaja registreerimiseks piisab ainult e-postiaadressi sisestamisest.

Järgmiseks antud reas on *Scan* ehk kontroll, kus saab samuti käivitada nutikat kontrolli. Antud kontroll hõlmab endas ühilduvuse kontrolli. Lisaks kontrollitakse viiruseid, otsitakse vananenud tarkvara. Veel kontrollitakse veebilehitseja lisasid ning võrgu turvalisust, jõudlusega seotud probleeme ja nõrku salasõnu. Lisaks saame arvutis olevatele failidele teha nii kiire kontrolli kui ka kõik arvutis olevad failid üle kontrollida ning muuta kui põhjalikult kontroll tegutseb failidega. Samuti läbi vaadata kindlat faili või kausta ning planeerida kontrolle. Nutika kontrolli osasid on võimalik ka eraldi käivitada. Näiteks kontrollida ainult veebilehitsejate lisasi, vananenud tarkvara, võrgu turvalisust ning jõudluse probleeme. Arvuti jõudluse suurendamiseks

otsib viirusetõrje üleliigseid faile ja rakendusi ning seadeid, mida muutes suurendataks arvuti kiirust. Kui aga kasutaja soovib neid probleeme lahendada, mida viirusetõrje leidis, tuleb osta tasuline lisa *Avast Cleanup*. Antud lisa on võimalik soetada üheks, kaheks või kolmeks aastaks. Ühe aasta litsents maksab $23.88 (u. €21.7), kahe aasta $45.36 (u. €41.2) ja kolmeks aastaks $60.84 (u. €55.2).

Kolmandaks osaks on *Tools* ehk tööriistad. Siin asub viis lisa, millest kolme saame tasuta versiooniga kasutada. Tasuta versiooni juurde kuulub *SecureLine VPN*, mis peaks aitama traadita võrgus andmeid turvata kui kasutaja on ühendatud avaliku võrguga. Jõudes õpetuse lõppu selgub, et antud lisa siiski ei ole tasuta viirusetõrje osa. Antud lisa saab proovida seitse päeva, aga edaspidi muutub tasuliseks. Kui kasutaja soovib edaspidi nimetatud lisa kasutada, siis on võimalik soetada *SecureLine VPN* kuuks ajaks hinnaga $7.99 (u. €7.3), üheks aastaks $39.99 (u. €36.3) ning kaheks aastaks $59.99 (u. €54.4). Teiseks lisaks on *SafeZone Browser*, mis ilmub lisana arvuti töölauale. Tegemist on eraldi veebilehitsejaga, kus panga külastused ja internetis maksmised on rangema kontrolli all. Kolmandaks kasutatavaks lisaks on *Rescue Disk*, mis kuvab valiku, kas USB või CD ehk millisele andmekandjale luuakse varukoopia süsteemist. Ülejäänud kaks kuuluvad tasulise versiooni juurde. Nendest esimene on *Firewall* ehk tulemüür ning teine *Sandbox* ehk liivakast.

Neljas osa on *Passwords*, kus tehakse võimalikuks sisselogimine igale poole internetis vaid ühe klahvi vajutusega. Selleks tuleb esmalt sisestada ülemsalasõna, mis kaitseb salvestatud kasutajanimesid ja salasõnu. Ülemsalasõna ei ole võimalik kuidagi taastada hiljem! Järgmiseks paigaldab viirusetõrje valitud veebilehitsejale lisa nimega *Avast Passwords*. Igakord kui kasutaja siseneb kuhugi veebilehele, siis pakutakse võimalust salvestada sisestatud kasutajanimi ja salasõna. Järgmisel korral minnes samale veebilehele on kasutajanime ja salasõna lahter täidetud ning sisse saab logida ühe nupuvajutusega. Kõik kasutajanimed ja paroolid asuvad viirusetõrjes ning nende muutmiseks tuleb sisestada ülemsalasõna. Kasutaja ja salasõna kustutamiseks ei ole vaja sisestada ülemsalasõna, muudatuste tegemiseks aga küll. Samuti on võimalik salvestada märkmeid, mida ei ole kaitse ülemsalasõna.

Viies osa antud viirusetõrjest kannab nime *Store*. Tegu on kohaga, kus saab tasuta versiooni asemele soetada tasuline versioon. Samuti on võimalik soetada tasulisi lisasi.

Viimane ikoon meenutab hammasratast ning asub viirusetõrje paremas nurgas. Seal asuvad viirusetõrje seaded ehk *Settings*. Seadete alt saab paika panna näiteks, mida viirusetõrje

kontrollib ja mida mitte. Seada viirusetõrjele seadetele salasõna ning muuta kasutatavate lisade seadeid. Samuti vahetada keelt ja sisse lülitada mänguri režiimi. Antud režiimis saab kasutaja keskenduda mängimisele, sest viirusetõrje ei tülita oma teadetega ning ei raiska nii palju ressursse kui tavaliselt töödates (Joonis 14).

Eripärad

Saab seada viirusetõrje seadetele salasõna ning mänguri režiimi olemasolu. Kasutaja lihtne registreerimine. Varundamise võimalus ja kasutajakontode salvestamine. Nutikas kontroll ja planeeritud kontrollide seadmise võimalus. Tegu on tasuta viirusetõrjega. Keelte pakettide lisamiseks pean sisenema administraatori kasutajasse, ei piisa sellest kui viirusetõrjet käivitada administraatori õigustega.

Eksperimendid

1. Kontrollid

Quick scan ehk kiire kontroll - Objekte: 169 850, Aeg: 00:20:28

Custom scan ehk valikuline kontroll(kontrollisin *Windows* kausta) - Objekte: 426 478, Aeg: 00:25:33

Full scan ehk kõikide failide kontroll - Objekte: 1 341 367, Aeg: 01:53:06

2. Protsessor kasutus ja koormus kontrollide ajal

Protsessori kasutus: 6-16%

Protsessori koormus: 37-54%

3. Antud viirusetõrje puhul saab testi pidada pigem õnnestunuks. Ühtegi faili allalaadida ei õnnestunud, sest veebilehekülg blokeeriti ning kuvati hoiatus.

4. Viiruseid asus *Linuxi* operatsioonisüsteemist otsima valikulise kontrolli abil. Seeläbi sai autor valida kõvaketta, mida kontrollida oli vaja. Veel enne kontrolli algust muudeti mõningaid seadeid viirusetõrje juures, et viirus tabataks suurema tõenäosusega. Esimese asjana lisati linnuke ette valikule, mis kontrolliks kõiki faile. Seejärel lisati kõik viirusetõrje poolt pakutud

faililaiendid otsitavate hulka. Kolmandaks lasti viirusetõrjel ka otsida võimalikke ebavajalikke rakendusi(*Potentially unwanted programs* ehk *PUPs*). Tulemuseks oli ebaõnnestumine ehk viiruseid ei tuvastatud.

2.2 Panda Free Antivirus

Nõuded arvutile

Koduleht: http://www.pandasecurity.com/

Operatsioonisüsteem: Windows 10(32-bit & 64-bit), Windows 8.1(32-bit & 64-bit), Windows 8(32-bit & 64-bit), Windows 7(32-bit & 64-bit), Windows Vista(32-bit & 64-bit) ja Windows XP (32bit) SP3 või hilisem

Mälu: 256 MB RAM

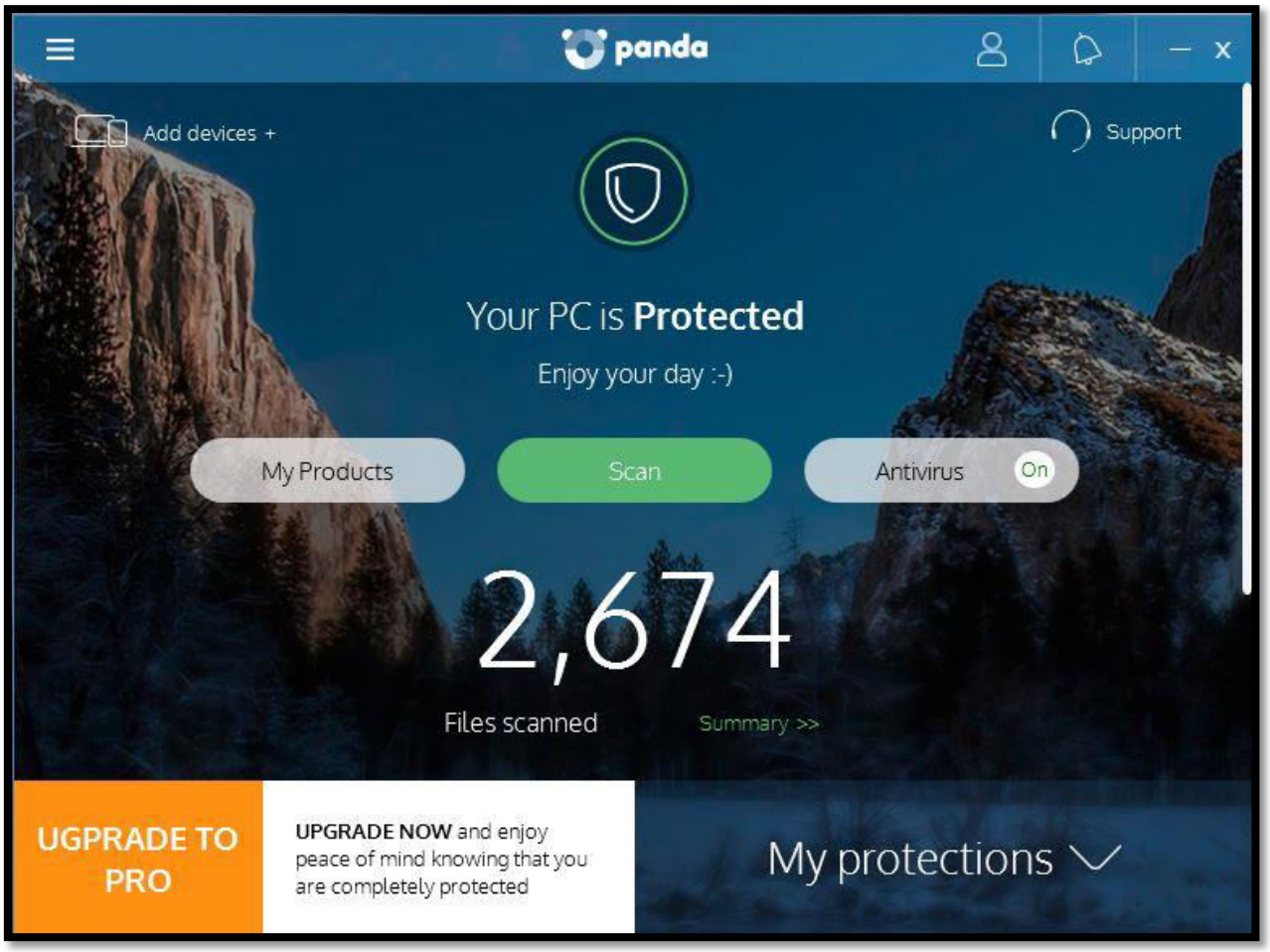
Protsessor: 300 MHz või kiirem

Vaba ruumi vajadus kettal: 240 MB

Veebilehitseja: Internet Explorer 6.0 või hilisem, Mozilla Firefox 2 või hilisem ja Google Chrome (Technical requirements, kuupäev puudub).

Paigaldamine

Kõigepealt tuleb kasutajal valida paigaldamise asukoht arvutis või jätta viirusetõrje poolt pakutud asukoht. Seejärel tuleb valida keel 22 erineva hulgast. Eesti keel esindatud pole. Pakutakse ka lisa nimega *Safe Web protection*, mis kaitseb kasutajat ohtlike veebilehtede eest. Soovib ka kasutaja registreerimist, mille jaoks tuleb sisestada e-postiaadress. Kohustuslik kasutaja registreerimine pole, aga iga kord viirusetõrjet käivitades küsitakse uuesti. Peale paigaldamist näeb viirusetõrje välja selline (Joonis 15).



Joonis 15. Panda Free Antivirus

Kasutajaliides

Alustame avakuva tutvustamist viirusetõrje ülevalt vasakust nurgast, kus asuvad kolm kriipsu üksteise all. Antud nupule vajutades avaneb viie valikuga menüü. Esimeseks neist on *Share ideas and solutions*, millele vajutades avaneb tootja foorum, kus saab enda probleemidest antud viirusetõrjega teada anda ning võimalik on ka lahendusi leida. Järgmiseks on *Online tech support*, kus kuvatakse ette erinevad artiklid probleemidest koos lahendustega. Samuti on võimalus saata kiri tootjale. Kolmandaks avatud menüüs on *Help*, mis avab viirusetõrje dokumentatsiooni. Neljandaks valikuks on *Settings* ehk seaded. Üldiste seadete alt on kasutajal võimalik vahetada keelt, määrata viirusetõrjele salasõna, näha kuhu tekivad viirusetõrje poolt loodud logifailid ning lülitada välja viirusetõrje teated kui mõni programm käivitus täisekraanil. Viirusetõrje seadete juures saab kasutaja paika panna, kas kontrollitakse ka kokkupakitud faile ja otsitakse soovimatuid programme. Samuti saab kasutaja määrata, mida teeb viirusetõrje kui leidakse viirus ning kui tihti puhastatakse karantiini ja lisada erandeid, mida viirusetõrje ei pea kontrollima. Samuti saame sisse lülitada kaks funktsiooni, millest esimene kannab nime *USB*

Protection. Antud funktsiooni saame panna automaatselt kontrollima üle iga arvutisse sisestatud USB pulga või välise kõvaketta. Teine funktsiooni nimega *Process Monitor*, mille saame seada jälgima iga töötava protsesse juurde pääsevaid veebilehekülgi. Viiendana *About Panda Protection* kuvab ette pahavatõrje hetkel kasutatava versiooni. Kolme kriipsu all asub pildike kirjaga *Add devices* +. Siin pakub viirusetõrje tootja oma tooteid teistele seadmetele peale *Windowsi*. Näiteks *iOS* versiooni viimane uuendus oli rohkem kui aasta tagasi ja *Androidi* puhul pole tegu väga populaarse viirusetõrjega.

Paremas nurgas asuvad kaks märki, millest esimene võimaldab registreerida kasutaja mille jaoks on vajalik sisestada e-postiaadress. Sisestatud e-postiaadressile saadetakse aktiveerimislink, kuhu tuleb sisestada salasõna ja kasutaja elukohariik. Teine märk kuvab hoiatusi. Märkide all asub kiri *Support*, mis avaneb kahe valikuna, millest aga reaalselt ainult esimene on tasuta versiooni poolt kasutatav. See on võimalus külastada tootja foorumist. Tasulise versiooni omanikel on võimalik kirjutada tehnilisele toele.

Avakuva keskele on kuvatud hetkel seis turvalisuse kohapealt. Järgnevad kolm ümarate nurkadega kasti. Neist esimene kannab nime *My Products* ehk minu tooted. Siin kuvatakse kõik kasutaja poolt kasutatavad viirusetõrje tootja erinevad tooted. Hetkel asub seal ainult tasuta viirusetõrje arvutile, mida on võimalus uuendada tasulisele versioonile.

Keskel asub kast nimega *Scan* ehk kontroll. Võimalik on alustada kolme sorti kontrolle. Esimeseks valikuks on *Critical areas*, mis otsib aktiivseid viiruseid näiteks arvuti mälust, töötavatest protsessidest ja veebilehitseja poolt salvestatud küpsistest. Järgneb *Full scan* ehk kõigi failide kontroll. Kolmandaks variandiks on *Custom scan*, mis laseb kasutajal valida faili või kausta mida kontrollida.

Viimane kast paremal on *Antivirus*. Vajutades kastile avaneb uus aken, kus saab kasutaja alustada kontrolle, seada planeeritud kontrolle ja tutvuda nii karantiinis olevate failidega kui ka kõigi viirusetõrje sündmustega.

Järgmiseks on välja toodud kontrollitud failide arv, mille kõrvalt on võimalik avada *Summary* ehk kõik viirusetõrje sündmused.

Avakuva kõige all paremal on kasutajal võimalik uuendada tasuliseks. Vasakule jääb *My protections*, millele vajutades kuvatakse uuel lehel kolm funktsiooni. Kaks esimest sai sisse lülitatud seadete alt. Nendeks olid *USB Protection* ja *Process Monitor*. Kolmandaks

funktsiooniks on *Rescue Kit*, mille abil saab kasutaja luua varukoopia oma süsteemist USB pulgale või välisele kõvakettale. Lisaks asub siin lisa nimega *Panda Cloud Cleaner*, mis tuleb eraldi paigaldada. Samuti on siin teistkordselt välja toodud kontrollitud failide arv ning võimalus alustada erinevaid kontrolle (Joonis 15).

Eripärad

Saab viirusetõrjele salasõna seada. Arvutiga ühendades kontrollitakse kohe ühendatud USB seada üle. Jälgitakse arvutis töötavaid protsesse. Kriitiliste alade kontroll ja lisa *Panda Cloud Cleaner*. Samuti varukoopia loomise võimalus. Planeeritud kontrolle saab seada. Tasuta viirusetõrje.

Eksperimendid

1. Kontrollid

Critical areas ehk aktiivse pahavara kontroll - Objekte: 54 006, Aeg: 00:11:00

Custom scan ehk valikuline kontroll(kontrollisin *Windows* kausta) - Objekte: 572 956, Aeg: 00:53:00

Full scan ehk kõigi failide kontroll - Objekte: 1 162 397, Aeg: 02:18:00

2. Protsessor kasutus ja koormus kontrollide ajal

Protsessori kasutus: 43-100%

Protsessori koormus: 85-99%

3. Antud viirusetõrje puhul saab testi pidada edukaks. Avastas peale allalaadimist viirused kolmest failist ja eemaldas koheselt. Laiendiga .txt tuvastati hilisema kontrolli käigus ning seejärel eemaldati arvutist.

4. Pahavara asus taaskord otsima valikulise kontrolli abil, et saaks valida kontrollitavaks süsteemi kõvaketta. Seadete alt lülitas sisse ebavajalike rakenduste otsimise ning samuti pakitud failide läbivaatuse. Tulemus oli negatiivne sest viirusetõrje ei avastatud viiruseid.

2.3 Bitdefender Antivirus Plus 2017

Nõuded arvutile

Koduleht: https://www.bitdefender.com

Operatsioonisüsteem: Windows 10, Windows 8, Windows 8.1, Windows 7(SP1)

Mälu: 1 GB RAM

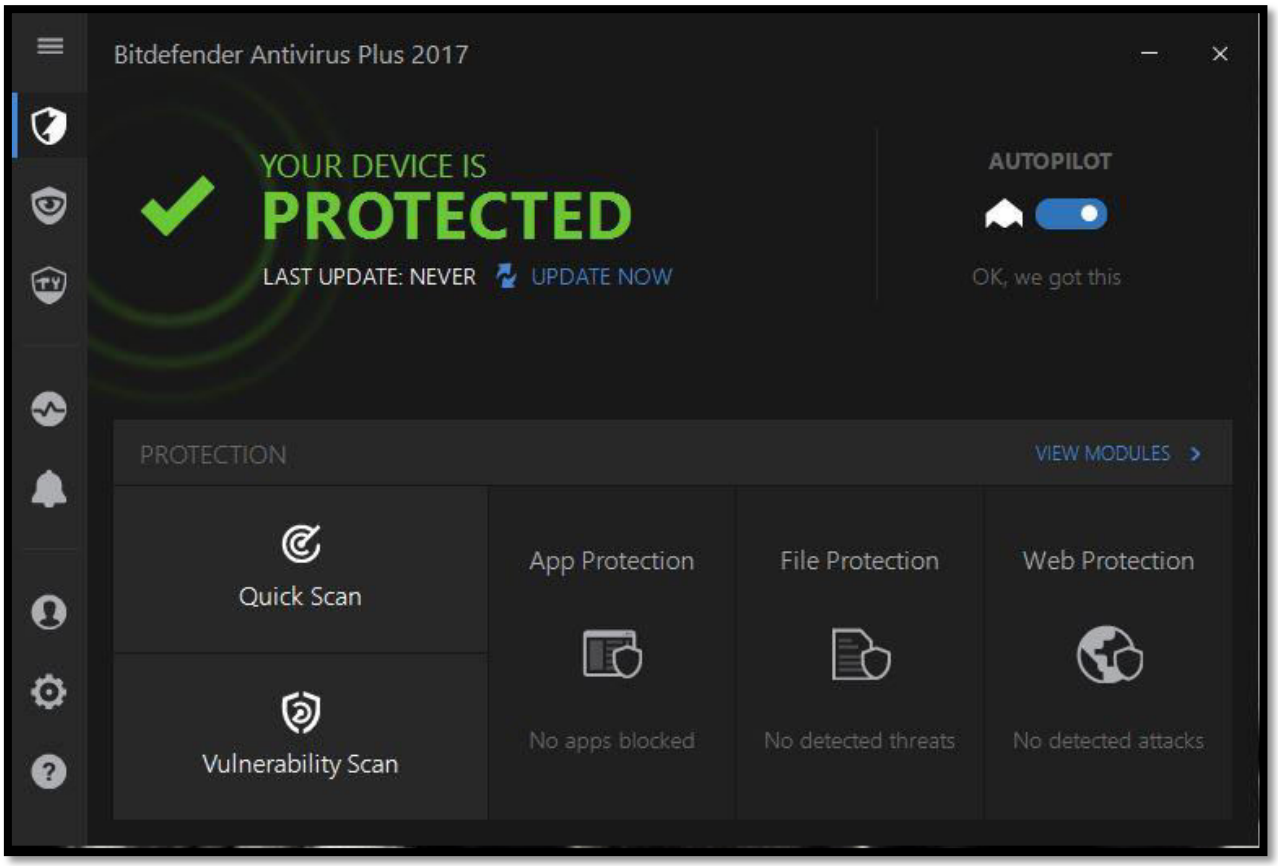
Protsessor: 1.6 GHz

Vaba ruumi vajadus kettal: 1.5 GB

Veebilehitseja: Internet Explorer 10 või uuem, Mozilla Firefox 30 või värskem, Chrome 34 või kõrgem (Minimal System Requirements, kuupäev puudub).

Paigaldamine

Esialgu paigaldamise protsess peatub ja nõutakse teiste viirusetõrjete arvutist eemaldamist. Peale edukat eemaldamist järgneb arvuti taaskäivitus ning jätkub viirusetõrje paigaldamine. Enne paigaldamise algust peame valima viirusetõrjele keele. Erinevaid valikuid on 9 ning eesti keel sinna ei kuulu. Samuti peame tutvuma lõppkasutaja litsentsilepinguga ning otsustama, kas soovime tootjale saata anonüümseid aruandeid viirusetõrje tööst. Seejärel peame valima paigaldamise viisi. Esimeseks võimaluseks on vajutada *Install,* mis teeb kõik otsused kasutaja eest ära. Teine võimalus on valida *Custom Installation,* kus kasutaja saab valida näiteks paigaldamise asukoha arvutis ning sisse või välja lülitada võimaluse, mis paigaldamise käigus arvuti üle kontrollib. Veel enne kui viirusetõrje käivitub esimest korda, tuleb registreerida kasutaja. Selleks sisestame eesnime, perekonnanime, e-posti ja salasõna. Peale litsentsi valikut hakkab viirusetõrje mõningaid seadeid veel paika sättima. Tegu on tasulise viirusetõrjega, millega saab 30 päeva tutvuda. Aastane litsents ühele seadmele maksab €29.99. Viirusetõrje avakuva on selline (Joonis 16).



Joonis 16. Bitdefender Antivirus Plus 2017

Kasutajaliides

Kui vajutada viirusetõrje üleval vasakul nurgas kolmele joonele, siis kuvatakse kõik viirusetõrje osad. Osasid on kokku kaheksa ning esimene nimega *Protection* on kujutatud viirusetõrje avakuvana, kus on näha arvuti hetkeseis turvalisuse kohapealt. Samuti näeme, millal toimus viimane uuendus. Paremalt saame sisse või välja lülitada autopiloodi(*Autopilot*). Tegu on viirusetõrje ühe profiiliga, mis taastab viirusetõrje kõigi funktsioonide töö. Taolisi profiile on veel, aga nendest tuleb juttu hiljem. Avakuva alumises osas näeme kahte kontrolli. *Quick Scan* ehk kiire arvuti failide kontroll ning *Vulnerability Scan*, mis otsib arvutis olevaid turvaauke. Seda läbi vananenud tarkvara või paigaldamata operatsioonisüsteemi uuenduste. Samuti otsitakse nõrku salasõnu nii kasutajate kui võrgu puhul. Liikudes paremale näeme mitu programmi või faili on blokeeritud ning mitu rünnakut internetist on tuvastatud. Vajutades *View Modules*, kohtame veel lisasi. Moodulid on jaotatud neljaks. Esimene moodul kannab nime *Antivirus* ning siit leiame veel ühe kontrolli liigi nimega *System Scan*, mis kontrollib kõik arvutis olevad failid üle. Järgmiseks *Manage Scans*, kus saame seada, millal mingi kontroll käivitub ning määrata taseme kui põhjalikult failid läbi kontrollitakse. Samuti valida kaustu ja faile, mida

kasutaja kontrollida soovib. Järgmine lisa *Rescue Mode* sooritab arvutile taaskäivituse. Enne muidugi küsitakse kinnitust kasutajalt. Esimese mooduli seadete alt näeme veel mitu faili asuvad karantiinis ning milliseid faile ja kaustu kasutaja arvates viirusetõrje kontrollima ei pea. Teine moodul nimega *Vulnerabilty* sisaldab lisa nimega *Wi-Fi Security Advisor*, mis kontrollib üle arvutisse salvestatud traadita võrgud ning annab hinnangu kas tegu on turvaliste või ebaturvaliste võrkudega. Kolmas moodul *Web Protection* sisaldab ühte lisa nimega *Whitelist*, kuhu kasutaja saab lisada veebilehekülgi, mida viirusetõrje kontrollima ei peaks. Viimane lisa nimega *Ransomware Protection* omab endas kahte lisa. Esimene *Trusted applications*, kuhu koondub turvaline tarkvara, millele on heakskiidu andnud viirusetõrje. Teine lisa, *Blocked applications,* koondab tarkvara, mis üritas muuta või kustutada arvutis olevaid faile. Sedasi käituv tarkvara blokeeritakse koheselt viirusetõrje poolt. Veel asuvad siin kaks lisa *Firewall* ehk tulemüür ja *Antispam* ehk ebaturvaliste kirjade kaitse. Nimetatud lisade proovimiseks tuleb soetada tasuline versioon.

Teine osa nimega *Privacy*, hõlmab endas kolme lisa. Esimene on *Safepay*, mis avab täiesti uue veebilehitseja, kus kasutaja saab sooritada ohutult oste või teha pangaülekandeid. Ebavajalikke faile või kausta saame eemaldada järgmise funktsiooniga *File Shredder*. Neid faile või kaustu ei saa enam hiljem taastada! Kolmas lisa nimega *Wallets*, kuhu saame salvestada enda kõik kasutajad ja salasõnad. Kõike seda kaitseb ülemsalasõna. Antud lisa abil saab kasutaja igale poole siseneda, ilma kasutajat ja salasõna sisestamata. Kasutaja ja salasõna lahtrid täidetakse automaatselt veebilehitsejasse paigaldatud lisa abil. Moodulite all leidub veel kaks lisa mida saab kasutada ainult tasulise versiooni puhul(*File Encryption* ehk failide krüpteerija ja *Parental Advisor*, mis aitab seada internetis sirvimise piirangud ning näha vanematel, millega laps arvutis olles tegeles).

Kolmas osa kannab nime *Tools*. Siin ei pakuta viirusetõrje tasulist versiooni, vaid versiooni, mis on mõeldud peale *Windowsi* ka teistele operatsioonisüsteemidele nagu näiteks *Androidi*.

Activity on järgmise osa nimi. Kuvatakse informatsiooni mitu rakendust või ohtu on blokeeritud ning mitu rünnakut internetist ära hoitud.

Viies osa *Notifications* toob välja kogu viirusetõrje tegevuse. Saab kontrollida, millal sooritati viimane uuendus ja kas see oli edukas. Sama kehtib kontrollide kohta.

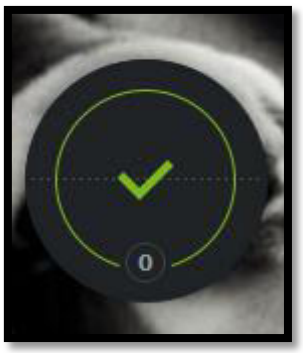
Osa number kuus nimega *Account* kuvab paigaldamise käigus loodud kasutaja info. Lisaks saame soetada tasulist versiooni või vahetada viirusetõrje kontot.

Seitsmes osa nimega *Settings*. Siit saame sisse või välja lülitada viirusetõrje väiksema versiooni mis jookseb koguaeg töölaual (*Security Widget*). Lisaks kuvatakse, et uuenduste kontroll toimub automaatselt iga tunni aja tagant. Peale eespool nimetatud autopiloodi profiili asub seadete all veel viis profiili. Esimeseks neist on *Work* ehk töö profiil. Antud profiili sisselülitamisel pakutakse samal hetkel arvutis töötavatele programmidele rohkem ressursse. Teiseks profiiliks on *Movie* ehk filmi profiil. Sisselülitusel korral muudetakse ekraani heleduse seadeid ning samuti luuakse rohkem ressursse filmi ilma pausideta edastuseks. Sama kehtib kolmanda profiili *Game* puhul, ainult et rohkem ressursse suunatakse mängu jooksutamiseks. Neljas profiil nimega *Public Wi-Fi*, mille puhu pööratakse suuremat tähelepanu võrgu turvalisusele. Viimane profiil *Battery Mode* töötab ainult tasulist versiooni omades.

Viimane osa *Support,* kus saame avada toote dokumentatsiooni, et kasutatavast viirusetõrjest rohkem teada saada. Probleemide korral suunatakse kasutaja tootja kodulehele, kust lahendust otsida (Joonis 16).

Eripärad

Põhilised kontrollide liigid olemas (kiire, põhjalik ja valikuline). Huvitav lisa turvaliseks pangas käimiseks ja ostlemiseks internetis. Failide ja kaustade täielik eemaldamise võimalus. Erinevad profiilid ning salasõnade turvamiseks lisa. Tegu on tasulise viirusetõrjega. Lisaks töötab töölaua all paremas nurgas koguaeg viirusetõrje, kus saab näha kas viirusetõrje parajasti teeb kontrolli või uuendab ennast. Kui nimetatud protsesse ei tehta, kuvatakse arvuti üldine seis (Joonis 17).



Joonis 17. Bitdefender Antivirus Plus 2017 Security Widget

Eksperimendid

1. Kontrollid

Quick scan ehk kiire kontroll - Objekte: 2166, Aeg: 00:00:20

Custom scan ehk valikuline kontroll(kontrollisin *Windows* kausta) - Objekte: 152 288, Aeg: 00:04:23

System scan ehk kõigi arvuti failide kontroll - Objekte: 1 695 914, Aeg: 03:15:18

2. Protsessor kasutus ja koormus kontrollide ajal

Protsessori kasutus: 9-15%

Protsessori koormus: 39-49%

3. Antud viirusetõrje puhul saab testi pidada igati edukaks. Faile allalaadida ei õnnestunud sest iga faili puhul viirusetõrje reageeris kohe ja suunas mujale ehk taaskord blokeeris veebilehekülje, kust autor allalaadida üritas.

4. Enne otsima asumist valikulise kontrolliga, panen paika viirusetõrje kontrolli seaded, et kontrolli teostatakse maksimaalse võimsusega. Selleks muutsin kontrollimise seaded kõige kõrgema taseme peale, milleks oli *agressive* ehk agresiivne. Kontrollimise pikkus küll pikenes suurel määral, aga kindlustas kõikide failide kontrolli kõvakettal. Taaskord ei avastatud midagi ohtlikku.

2.4 ESET Smart Security Premium

Nõuded arvutile

Koduleht: http://www.eset.com

Operatsioonisüsteem: Windows 10, 8.1, 8, 7, Vista ja Home Server 2011

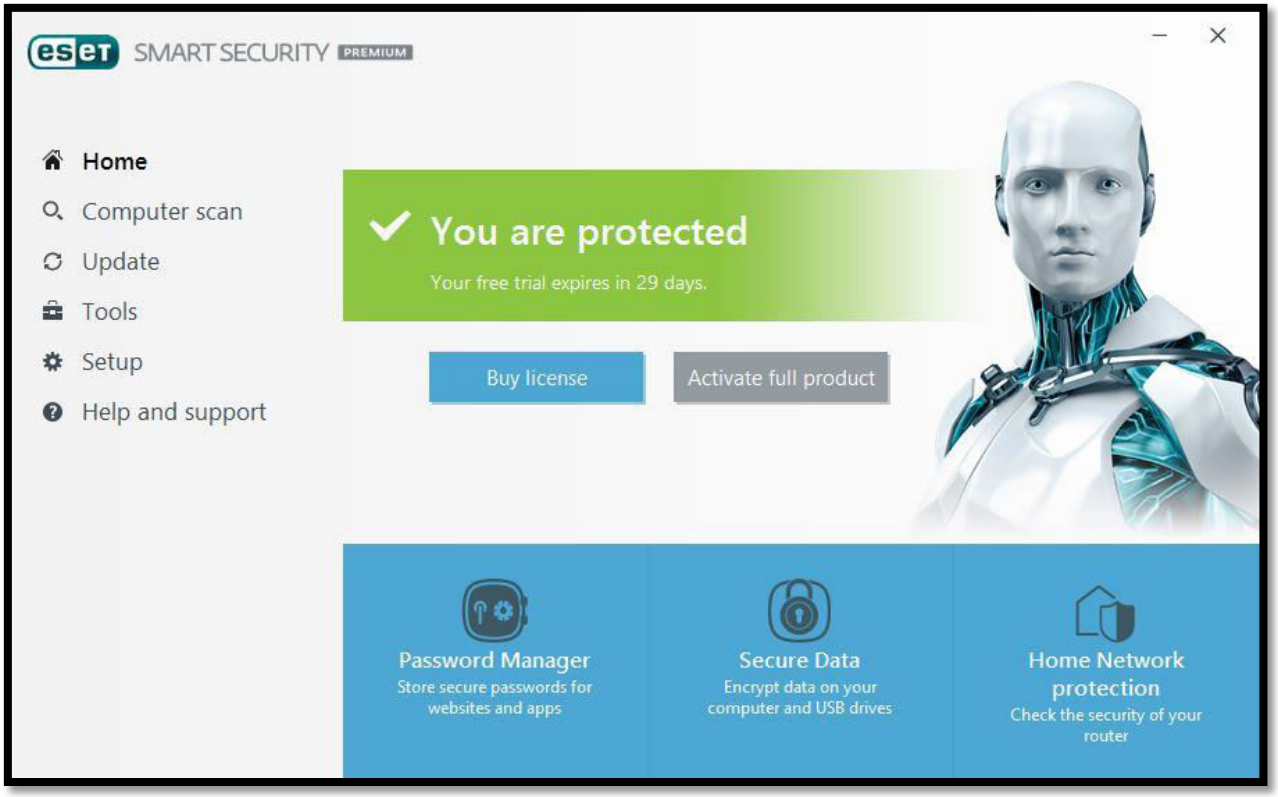
Mälu: 512 MB RAM, 1 GB RAM Vista jaoks

Protsessor: 1 GHz

Vaba ruumi vajadus kettal: 320 MB (System Requirements for Windows ESET home products, 2016).

Paigaldamine

Käivitades allalaaditud faili tuleb kõigepealt kasutajal valida keel. Kokku on võimalik valida 36 keele hulgast ning eesti keel on esindatud. Järgmiseks kuvatakse lõppkasutaja litsentsileping, millega tuleks kindlasti enne nõustumist lähemalt tutvuda. Veel uuritakse, kas kasutaja soovib saata infot tootjale. Linnukese eemaldamisega sellega ei nõustuta. Samuti saab sisse lülitada ebavajalike rakenduste tuvastuse ning muuta asukohta, kuhu viirusetõrje paigaldatakse arvutis. Viimasena tuleb veel valida tasuta prooviversiooni litsents, sest tegu on tasulise viirusetõrjega. Aastane litsents ühele arvutile maksab €37.74. Tasuta prooviversiooni kasutamiseks tuleb litsents registreerida, selleks sisestame e-postiaadressi ning valime elukoha riigi. Viirusetõrjega tuli kaasa lisa nimega *ESET Banking & Payment protection*, mis avab kasutaja peamise veebilehitseja, aga sel juhul turvab seda viirusetõrje. Veebilehitseja on mõeldud pangatehingute sooritamiseks või internetis ostude tegemiseks. Viirusetõrje ise näeb välja selline (Joonis 18).



Joonis 18. Eset Smart Security Premium

Kasutajaliides

Viirusetõrje jaotub kuueks osaks, mis kõik asuvad vasakul. Esimene neist on kodu ehk *Home*. Siin näeme, kas arvuti on hetkel kaitstud või mitte. Saame soetada või aktiveerida tasulise versiooni. Lisaks näeme kaua veel tasuta prooviversiooni kasutada saame. Veel saame sisselülitada lisa nimega *Password Manager*, millele esimesena seame ülemsalasõna. Antud lisa alla on võimalik salvestada kasutajad koos salasõnadega ning järgmine kord veebilehele sisenedes on väljad juba täidetud. Teine lisa nimega *Secure Data*, millega kasutaja saab nii arvuti ketaste sisu kui ka USB kõvakettaid krüpteerida. Kolmandaks on *Home Network protection*, mis kuvab kõik ruuteriga ühendatud seadmed. Nimetatud kolm lisa leiame ka tööriistade alt, millest tuleb hiljem juttu.

Teiseks osaks on *Computer scan* ehk arvuti kontroll. Saab käivitada kolme erinevat kontrolli, millest esimene on *Scan your computer,* mis kontrollib kõiki arvuti kohalikke kettaid. Teiseks on *Custom scan* ehk kohandatud kontroll. Siinjuhul saab kasutaja valida kontrollimise sihtmärgi(d). Viimaseks on *Removable media scan* ehk USB-, DVD-, CD-seadmete ja muude arvutist eemaldavate andmekandjate kontroll. Saame ka paika panna, mis tehakse peale kontrolli lõppemist. Näiteks on võimalik arvuti välja lülitada või sooritada taaskäivitus.

Kolmas osa on uuendamine ehk *Update*. Siin saame käivitada uuendamise protsessi nii viirusetõrje andmebaasidele kui ka versioonile.

Neljandaks on tööriistad ehk *Tools*. Siin asuvad kolm lisa, millest esimeses osas juba sai räägitud. Veel saame avada ohutu veebilehitseja pangatehingute tegemiseks (*Banking & Payment protection*). Viiendaks lisaks on *Anti-Theft*, mille kasutamiseks on vaja kasutaja registreerida. Nimetatud lisaga saame tootja kodulehel oma varastatud arvutil kaamera käivitada või selle asukohta määrata. Sisenedes tootja kodulehele, pakutakse veel kahte lisa. Esimest lisa nimega *Parental Control* pakutakse *Androidi* nutitelefonile. Antud lisa võimaldab vanematel seadistada laste nutitelefonis internetis sirvimist ja rakenduste kasutust. Vanemad saavad jälgida kogu nutitelefoni tegevust kas isiklikust seadmest või tootja kodulehelt. Teine lisa nimega *Social Media Scanner,* mis kaitseb kasutaja *twitteri* profiili ohtlike veebilehekülgede eest. Viirusetõrje juurde tagasi tulles saame avada veel tööriistu(*More tools*). Avanenud aknast saab kasutaja üle vaadata viirusetõrje poolt loodud logifailid, näha nii pahavara ja rämpsposti blokeerimise statistikat ning loodud võrguühenduste ülevaadet. Samuti kuvatakse hetkel töötavad protsessid ja kui aktiivsed on failisüsteem või võrgutegevus. Veel saame esitada mõnda faili põhjalikumaks

analüüsiks ning seada planeeritud kontrolle ja vaadata üle, mis failid on karantiinis. Veel leiduvad siin kaks tööriista, millest esimene on süsteemi kohta üksikasjaliku teabe kogumiseks (*ESET SysInspector*) ning teine ründevara eemaldamiseks (*ESET SysRescue Live*).

Eelviimaseks on *Setup* ehk häälestus. See on jaotunud omakorda neljaks. Esimeseks on *Computer protection* ehk arvutikaitse. Siin saame sisse või välja lülitada nii reaalajakaitse kui ka mänguri režiimi. Samuti arvuti sissetungi vältimise süsteemi ja arvuti veebikaamera kaitse. Järgmiseks on *Internet protection* ehk interneti-kaitse, kus saame samuti sisse või välja lülitada näiteks nii meilikliendi kaitse, veebikasutuse kaitse, andmepüügivastase kaitse kui ka rämpspostitõrje. Kolmandaks on *Network protection* ehk võrgukaitse. Saame üle vaadata tulemüüri seaded ning sisse või välja lülitada kaitse võrgurünnakute ja robotivõrgu eest. Kuvatud on nii blokeeritud veebilehekülje kui rakendused ja seadmed. Viimaseks on *Security tools* ehk turbetööriistad. Kasutaja saab muuta pangatehinguteks ja ostlemiseks mõeldud veebilehitseja seadeid koos vargusevastase tehnoloogia (*Anti-Theft*) omadega. Vajadusel sisse lülitada vanema kontrolli funktsiooni arvutis (*Parental Control*), millega saab ebasobivaid veebilehekülgi blokeerida. Veel asuvad siin kaks lisa, millest juba varem juttu olnud. Nendeks on *Secure Data* ehk krüpteerimise abi ning *Password Manager,* mis aitab kasutajal igale poole kiirelt siseneda, ilma salasõna ja kasutajat sisestamata.

Viimaseks osaks on *Help and support* ehk tugi ja spikker. Koht, kuhu pöörduda probleemide tekkimisel viirusetõrjega. Samuti kuvatakse toote- ja litsentsiteave (Joonis 18).

Eripärad

Kontrollide tüüpe vähevõitu. Pangatehingute ja ostlemiseks on mõeldud eraldi veebilehitseja. Vargusevastane tehnoloogia kui kasutaja registreerid. Mänguri režiim ja vanemate kontrolli funktsiooni olemasolu. Suur keeltevalik ning saab seada planeeritud kontrolle. Arvutist eemaldavate seadmete kontroll ja faile võimalik saata analüüsi. Tegu on tasulise viirusetõrjega.

Eksperimendid

1. Kontrollid

Scan your computer ehk kohalike ketaste kontroll - Objekte: 252 410, Aeg: 00:24:53

Custom scan ehk valikuline kontroll(kontrollisin *Windows* kausta) - Objekte: 388 694, Aeg: 00:34:26

2. Protsessor kasutus ja koormus kontrollide ajal

Protsessori kasutus: 38-56%

Protsessori koormus: 76-99%

3. Antud viirusetõrje puhul saab testi pidada väga edukaks. Kõigi nelja faili puhul allalaadimine ei õnnestunud. Ühendus veebilehega peatati.

4. Viimase *Windowsi* viirusetõrje seadete juures polnud vaja seadeid muuta kuna kõik vajalik oli juba sisse lülitatud. Autoril tuli vaid valida valikuline kontroll ja kõvaketas, mida kontrollida. Kahjuks kordus sama stsenaarium ka neljandal korral ning midagi ohtlikku ei leitud.

3. Android

Selleks, et katsetada viirusetõrjed antud operatsioonisüsteemil kasutan nutitelefoni, mis sisaldab *Androidi* viimast versiooni Galaxy seeriale, milleks hetkel on 6.0.1 "Marshmallow". Testitava nelja viirusetõrje valik sõltus nii viirusetõrje üldhindest kui ka inimeste hulgast, kes antud toodet oli hinnanud *Google Play* rakenduses. Samuti oli oluline viimase värskenduse kuupäev, mis pidi olema mitte vanem kui 1 kuu.

Kui nüüd rääkida lähemalt *Androidi* turvalisusest, siis tuleb tunnistada et *iOS* on mõnevõrra turvalisem. Jutt on seadmetest mida pole lahti murtud ehk avatud (*jail-break*). Suurim erinevus kahe konkurendi vahel tuleneb tootmisprotsessist. *Androidi* operatsioonisüsteemi kasutavad mitmed erinevad telefonitootjad, kuid *iOSi* puhul ainult tootja *Apple*. See muudab operatsioonisüsteemi killustatuks ehk kasutusel on palju erinevaid versioone operatsioonisüsteemist. Lisaks tuleb süsteemi kohendada vastavalt tootjale või seeriale. Samuti ei maksa unustada seda, et tänu mitmele tootjatele kelle telefonid kasutavad *Androidi* operatsioonisüsteemi, valitseb hetkel telefoniturgu *Android*, mis muudab antud operatsioonisüsteemi sagedamate rünnakute ohvriks. Viimaste aastatega on tehtud tõhusaid samme turvalisuse osas, aga soovitav oleks siiski omada viirusetõrjet kasutatavas *Androidi* seadmes (Forrest, 2016). Lisaks tuleks rakendusi allalaadida ainult teadatuntud keskkondadest, sest *Androidi* puhul kontrollitakse näiteks *Google Play* rakendusi, enne kui need lõppkasutajani jõuavad. *Androidi* puhul on küll jäetud rakenduste autoritele palju vabamad käed kui *iOSi* juures, aga siiski on väiksem nakatumise võimalus (Armendariz, 2016). Samuti tuleks tutvuda soovitustega kasutajale (Lisa 3).

3.1 Avast Mobile Security & Antivirus

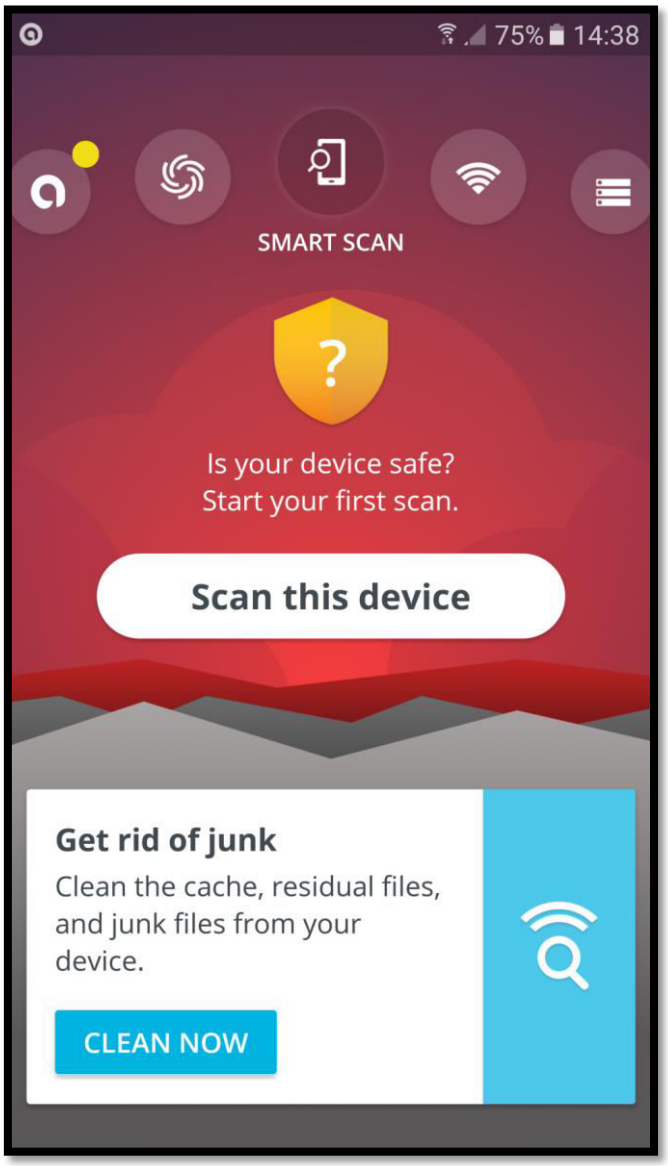
Nõuded telefonile

Koduleht: http://www.avast.com

Telefoni operatsioonisüsteem: Android 4.0.3 või hilisem. Ei toeta Androidi versioone 2.3, 2.3.x ja 3.x (What are the system requirements for Avast Mobile Security, kuupäev puudub).

Paigaldamine

Et paigaldada antud viirusetõrje tuleb kõigepealt avada *Play pood*. Otsingusse sisestame märksõnad *avast antivirus*. Valime esimese valiku, milleks on *Mobile Security & Antivirus*. Valime *Intall* ehk paigalda. Antud viirusetõrje soovib juurdepääsu 6 õigusele. Esimesel käivitusel tuleb lugeda läbi ja nõustuda lõppkasutaja litsentsilepinguga ning privaatsuspoliitikaga. Nõustumiseks tuleb vajutada *Continue*. Viirusetõrje keel valitakse sama, mis on telefonis kasutusel. Peaks olema üle 20 keele, aga eesti keel sinna ei kuulu. Viirusetõrje näeb välja selline (Joonis 19).



Joonis 19. Avast Mobile Security & Antivirus

Kasutajaliides

Nägu näha on antud viirusetõrje jaotatud viieks ringikeseks. Alustame keskmisest, mis kannab nime *Smart Scan* ehk nutikas kontroll. Antud kontroll koosneb kolmest osast. Esiteks kontrollitakse, kas viirusetõrje on uuendatud kõige viimasele versioonile. Järgmiseks vaadatakse üle ega telefonis pole turvaauke ning seejärel kontrollitakse kõik rakendused üle.

Liikudes edasi vasakule, siis esimesena tuleb vastu *Storage* ehk koht, kus näeb mitu protsenti on kasutatud telefoni kogu mälust. Samuti saab allalaadida lisa nimega *Cleanup & Boost*. Ka nimetatud lisa esimesel käivitamisel tuleks veelkord tutvuda ja alles seejärel nõustuda lõppkasutaja litsentsilepinguga ning privaatsuspoliitikaga. Tegu on tasuta lisaga ning temaga saab väga edukalt eemaldada telefonist näiteks veebilehitseja vähemälu. Antud lisa teine pool *Boost* näitab ära, mis rakendused hetkel jooksevad telefonis. Võimalik on lõpetada rakenduste töö, mille töötamist taustal kasutaja vajalikuks hetkel ei pea. Siinkohal mainiksin ära, et kõiki rakendusi mida ei tunne pole mõtet kohe sulgema hakata, ennem tuleks pigem uurida otsimootoreid kasutades või küsida spetsialisti käest. Lisaks saame selle lisa alt oma pildid, videod ja muud failid pilve liigutada ja tutvuda lähemalt rakendustega, mis meil telefonis on.

Liikudes veelkord vasakule jõuame ringikeseni nimega *More By Avast*. Siin saame tutvuda kõigi lisadega, mis antud viirusetõrjel on. Neid on kokku kuus. Esimese lisaga me juba tutuvusime, milleks on *Cleanup*. Teine lisa kannab nime *Battery Saver*. Esimesel käivitusel tuleks taaskord enne nõustumist lugeda lõppkasutaja litsentsilepingut ning tutvuda privaatsuspoliitikaga. Antud lisas kuvatakse informatsioon aku kestvuse kohta ning kui jookseb ebavajalikke rakendusi, siis soovitakse nad sulgeda, pikendades sellega aku kestvust. Tegu on tasuta lisaga. Kolmandaks on *SecureLine VPN*, mida saab proovida seitse päeva ning peale seda muutub tasuliseks. Antud lisa kaitseb kasutajat kui telefoniga viibitakse avatud/avalikus traadita võrgus. Neljas lisa on *Anti-Theft*. Lisa aktiveerimiseks tuleb läbida kolm sammu. Neist esimene kannab nime *SMS control*, mille puhul tuleb seada salasõna, millega siseneme antud lisasse. Enne salasõna sisestamist peame valima e-postiaadressi, mille kaudu saame salasõna meelde tuletada kui see peaks meelest minema. Teine samm on *Web control*, mille käigus tuleb registreerida kasutaja läbi mille saame arvutist telefoni positsioneerida, kui ta peaks näiteks kaduma minema. Kasutaja saab registreerida kasutades kas *facebooki*, *google* või e-posti kontot. Viimane samm kannab nime *Allow permissions*, mille käigus tuleb lisale anda administraatori õigused telefonis. Nüüd saame lisaks positsioneerimisele ka telefoni sisu lukustada ja käivitada alarmi. Tegu on taaskord tasuta lisaga. Lisa number viis on *Passwords*. Esimese asjana tuleb seada ülemsalasõna, mille alla

koonduvad kõik ülejäänud. Järgmine kord kuskile sisse logides salvestatakse kasutaja koos salasõnaga krüpteeritud kujul. Järgmine kord sisenedes samale veebilehele on kõik väljad juba täidetud ja kasutaja saab koheselt sisse logida. Tegu on tasuta lisaga. Viimase lisa nimi on *Wi-Fi Finder*. Antud lisa aitab otsida ohutut ja kiiret traadita võrku. Samuti saab testida eraldi võrgu turvalisust ja kiirust. Tasuta lisa samuti.

Liikudes tagasi keskele ning seejärel paremale, kohtame esimenesena ringi nimega *Wi-Fi Check*. Siin saab kontrollida võrgu ohutust ja kiirust, millesse ollakse hetkel ühendatud. Kontrollitakse krüpteerimise taset, ruuteri salasõna ja otsitakse turvaauke.

Viimane ring paremal nimega *Tools* ehk tööriistad sisaldab nelja tööriista. *App Locking*, millega saab telefonis olevaid rakendusi lukustada salasõnaga. Teiseks *Call Blocker*, kuhu saab sisestada telefoni numbreid, keda kasutaja blokeerida soovib. Järgmiseks on *Privacy Advisor*, kust saab vaadata üle, millised rakendused telefonis on. Vajadusel saab neid eemaldada või uurida lähemalt kuhu rakendus ligipääsu nõuab. Neljandaks saab sisse lülitada *Firewalli* ehk tulemüüri. Veel saab näha infot registreeritud kasutaja kohta. Seadete ehk *Settings* alt saab näiteks muuta rakendustele seatud salasõna või tutvuda viirusetõrje poolt koostatud logidega. Samuti seada planeeritud kontrolle (Joonis 19).

Eripärad

Lisade süsteem sisaldab viit tasuta lisa, kuuendat saab proovida 7 päeva. Saab seada planeeritud kontrolle. Rakendusi lukustada salasõnaga, telefoni numbreid blokeerida, rakendustega lähemalt tutvuda ja vajadusel nad eemaldada. Tulemüüri olemasolu ei tohiks ka unustada. Tasuta viirusetõrje.

Eksperimendid

1. Nutikas kontroll ehk *Smart Scan*

Objekte: 53, Aeg: 00:00:07

Objekte: 53, Aeg: 00:00:07

Objekte: 53, Aeg: 00:00:07

2. Test oli pigem läbikukkumine. Kõik failid sain allalaadida ning avada ilma mingite probleemideta. Tehes nutika kontrolli, leidis esimesed kolm faili ja eemaldas nad. Viimane topelt zip fail jäi alles.

3.2 CM Security AppLock AntiVirus

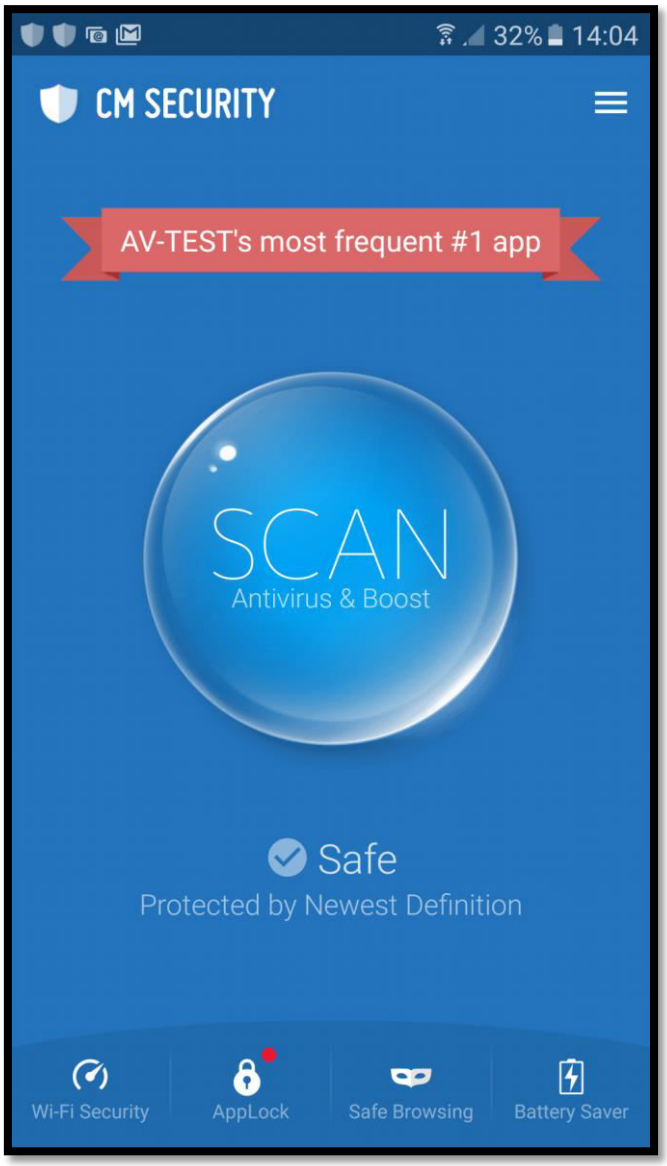
Nõuded telefonile

Koduleht: http://www.cmcm.com/en-us/

Telefoni operatsioonisüsteem: Puudub info

Paigaldamine

Taaskord avame telefonis rakenduse nimega *Play pood*, kuhu seekord kirjutame otsingusse *cm security*. Valime esimese valiku, milleks on *CM Security AppLock AntiVirus*. Vajutame *Install* ehk paigalda. Viirusetõrje taotleb juurdepääsu 7 õigusele. Esimesele käivitusel soovitakse sooritada esimene kontroll. Peale kontrolli on võimalik sisse lülitada reaalaja kaitse koos veebilehitseja kaitsega ning kuvatakse infoks kui palju vaba ruumi on juurde võimalik tekitada eemaldades ebavajalikke faile. Peale esimest kontrolli näeb viirusetõrje välja selline (Joonis 20).



Joonis 20. CM Security AppLock AntiVirus

Kasutajaliides

Alustame kõige ülevalt paremalt, kus asuvad kolm kriipsu üksteise all. Siit saame näha antud viirusetõrje kõiki funktsioone. Enne veel kui hakkame funktsioonidest lähemalt rääkima, tutvume seadetega. Seadete all saame seada planeeritud kontrolle, muuta keelt ja soetada tasuline versioon viirusetõrjest, mis kaotab ära kõik reklaamid. Selleks hinnaks on antud hetkel €0.99 kuu aja eest. Täishinnaks on €2.99 ühe kuu eest. Keelte valikust niipalju, et valikuid on 28, kuhu eesti keel ei kuulu.

Funktsioonidest esimeseks on *AppLock*, millega saame lukustada rakendusi kas salasõna või mustri sisestamisega. Sellega ainult ei piirduta, sest on võimalik lasta telefonil pildistada kui

keegi üritab mõnda lukustatud rakendusse pääseda, aga sisestab salasõna või mustri valesti. Lisaks saame valitud rakenduste puhul telefoni seadistada nii, et teate saabumisel kuvatakse ekraanile ainult rakenduse nimetus. Seega ei kuvata saatja nime ega sõnumit. Selleks tuleb telefoni sisse logida, et näha rohkem informatsiooni saabunud teate kohta. Samuti saame peale rakenduste lukustada ka sissetulevad kõned kui ka sinihamba ja traadita võrgu seaded. Veel asub siin funktsioon nimega *Vault*, mis võimaldab meil oma privaatsed pildid turvaliselt peita, et igaüks neid ei näeks.

Järgmiseks funktsiooniks on *Safe Browsing*, mille sisselülitamise tagajärel tekib telefoni uus veebilehitseja, mille vahemälu ja muu informatsioon eemaldakse iga 60s tagant.

Kolmandaks on *Wi-Fi Security*. See jaguneb omakorda kaheks. Esimene osa kannab nime *Wi-Fi Analyzer*, mis testib traadita võrgu turvalisust ja kiirust, millega telefon hetkel ühendatud on. Teine osa *Wi-Fi Connector* kontrollib teisi traadita interneti võrke, mis telefoni levialas leiduvad ning annab teada, millise võrguga oleks turvaline telefoni ühendada. Veel saame lasta üle kontrollida kõik telefoni salvestatud traadita võrgud ning eemaldada neist ebaturvalised traadita võrgud. Lisaks seada viirusetõrje kontrollima iga uut ühendatud traadita võrguühendust.

Neljas funktsioon kannab nime *Battery Saver*, mille abil on võimalik sulgeda üleliigsed rakendused ja sellega pikendada telefoni aku kestvust.

Phone Boost kontrollib telefoni mälu ehk *RAMi* kasutust ning võimalusel vähendab seda.

Kuuendaks funktsiooniks on *Clean Junk Files*, mis asub otsima üleliigseid faile, mida telefonist eemaldada. Näiteks veebilehitseja või süsteemi vahemälu. Samuti mõne rakenduse faile, mis on tekkinud või maha jäänud telefoni.

Järgnev funktsioon kannab nime *Notification Manager*. Seadete alt saame muuta milliste rakenduste teated ilmuvad ainult viirusetõrjes ja millised ilmuvad reaalselt telefoni ekraanile.

Oleme jõudnud kaheksanda funktsiooni juurde milleks on *Caller ID & Blocking*. Nagu nimi ütleb, siis saame blokeerida nii kasutaja poolt sisestatud kui ka telefoni kontaktide hulgast numbreid. Samuti on võimalik blokeerida näiteks privaatsed numbreid.

Scan Files kontrollib telefonis olevaid rakendusi, otsides neist pahavara. Seejärel kontrollitakse kasutaja privaatsust ning vaadatakse, kas telefonis leidub ebavajalikke faile mida eemaldada.

Kõige lõpuks annab viirusetõrje märku, kas kõik on hetkel turvaline või peaksime mõnele rakendusele või failile tähelepanu pöörama.

Kümnendaks funktsiooniks on *Download Security.* Antud funktsioon kontrollib pilte ja teisi faile, mis on saadetud läbi erinevate rakenduste kasutajale.

Viimane funktsioon kannab nime *Find Phone*. Selleks registreerime kasutaja. Võimalusi on kolm. Saame kasutada kas *google+* või *facebooki* teenuseid. Samuti on võimalik registreerida kasutades e-postiaadressi. Seejärel saame arvutist oma telefoni asukohta määrata, lukustada kogu sisu ning käivitada alarmi, mis aitab telefoni kadumise korral kiiremini üles leida. Antud funktsiooni autor tööle ei saanud, kuna kasutajat ei olnud võimalik registreerida ja läbi selle antud funktsiooni sisse lülitada. Kuna tootja kodulehelt lahendust ei leidnud, saatsin kirja tootjale ja nüüd jään ootama vastust. Kuu aega hiljem pole mingit tagasisidet tootja poolt tulnud.

Järgmiseks saame veel hinnata antud rakendust ning probleemide lahendamiseks avada tootja kodulehe, kus leiab vastuseid paljudele küsimustele. Viirusetõrje avakuva all on toodud välja neli funktsiooni, millest on juba räägitud. Avakuva keskelt saame alustada kontrolli (Joonis 20).

Eripärad

Planeeritud kontrolle saab seada ja rakendustele saab salasõna määrata. Keelte valik laialdane. Arvuti abil saab kadunud telefoni otsida, lukustada või käivitada alarmi. Numbreid võimalik blokeerida. Palju funktsioone, aga koos nendega ka palju reklaame. Tegu on siiski tasuta viirusetõrjega, mida saab reklaamide eemaldamiseks tasuliseks muuta hetkel €0.99 ühe kuu eest. Muidu maksab üks kuu €2.99.

Eksperiment

Test ei olnud edukas. Sain nii läbi telefoni veebilehitseja kui ka viirusetõrje veebilehitseja kõik failid probleemideta alla laadida ja avada. Hilisem kontroll ei tuvustanud samuti midagi ohtlikku.

3.3 360 Security - Antivirus Boost

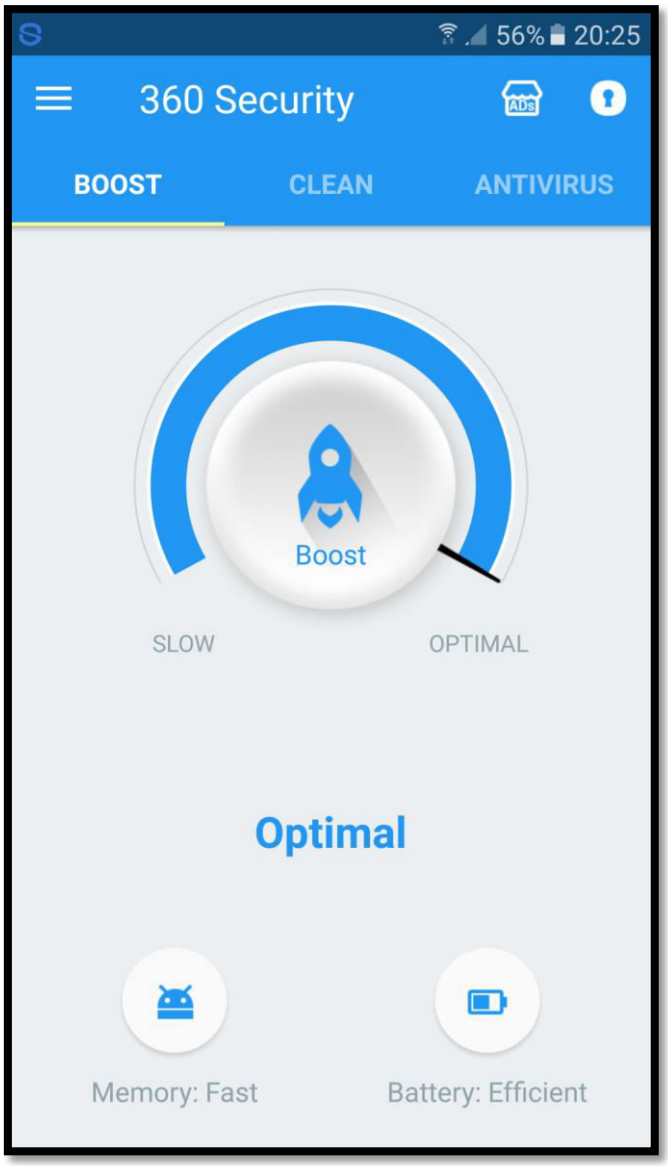
Nõuded telefonile

Koduleht: http://www.360securityapps.com/en-us

Telefoni operatsioonisüsteem: Puudub info

Paigaldamine

Avan rakenduse *Play pood* ning sisestan otsingusse *360 security*. Avan rakenduse nimega *360 Security - Antivirus Boost*. Vajutame *Install* ehk paigalda. Viirusetõrje nõuab juurdepääsu 12 õigusele. Esimesel käivitusel sooritati kontroll kui palju rakendusi kasutavad mälu(*RAM*) ning kui palju neist kulutavad taustal kasutult aku energiat. Peale seda näeb välimuselt viirusetõrje välja selline (Joonis 21).



Joonis 21. 360 Security - Antivirus Boost

Kasutajaliides

Alustades kohe ülevalt siis viirusetõrje nime kõrval vasakul on kolm kriipsu üksteise all. Kriipsudele peale vajutades ilmub vasakult menüü, mis sisaldab kõiki viirusetõrje funktsioone. Neist esimene on *Notification Manager*, mis peidab valitud rakenduste teated ja laseb telefonil kuvada ainult lubatud rakendustele saabunud teated.

Teine funktsioon on *AppLock*, millega saame rakendustele seada salasõna või mustri. Mustri seadmise puhul on võimalik kaotada mustri tekkimine ekraanil. Tootja on lahendanud selle vibratsiooniga. See tähendab et, iga kord kui mustrist punkt läbitakse, telefon vibreerib.

AppLocki seadete alt saab vibratsiooni välja lülitada, aga mingil põhjusel vibratsioon endiselt säilib. Vibratsioon kaob alles siis kui mustri tekkimine ekraanile tagasi lubatakse.

Kolmandaks funktsiooniks on *Full Scan*, millele vajutades käivitub kontroll. Peale kontrolli lõppu kuvatakse probleemid või kinnitatakse, et kõik on korras.

Järjekorras neljas funktsioon kannab nime *Phone Temperature*. Siin on kuvatud telefoni protsessori temperatuur. Kui temperatuur tõuseb liiga kõrgeks on võimalik vajutada *Cool Down*, mis sulgeb ebavajalikud rakendused, mis mõjutavad protsessori temperatuuri ja selle tegevuse tulemusena jahutab protsessorit.

Järgmine protsess nimega *Game Boost* lubab lisada kasutajal mänge telefonist antud funktsiooni alla. Järgnevalt luuakse töölauale ikooni nimega *Games*, mis nüüd tänu viirusetõrje sekkumisele käivitab kiiremini mänge. Peale selle ka mängud jooksevad puhtamalt sest sulgetakse kõiki ebavajalikud rakendused telefonis, et mälu(*RAM*) juurde tekitada.

Kuues funktsioon on *Space Cleaner*, mis kontrollib rakenduste vahemälu ning vajadusel suudab üleliigse sealt eemaldada. Samuti kuvatakse kui palju on hetkel kasutusel kogu telefonis olevast mälust(*Storage*).

Järgmiseks funktsiooniks on *App Manager,* kus saab näha kõiki telefonis olevaid rakendusi ning kasutaja vabal soovil neid eemaldada.

Kaheksandaks on *Find My Phone*, mille abil saame arvutist telefoni asukohta määrata, sisu lukustada või käivitada alarmi. Samuti annab viirusetõrje teada SIM kaardi vahetusest. Viimane võimalus on telefon sisu ära kustutada. Selleks tuleb aktiveerida *google* kasutaja.

Üheksas funkstioon nimega *Call & SMS Filter*, mis võimaldab kasutajal blokeerida telefoni numbreid, mis asuvad kontaktide hulgas. Samuti on võimalik kasutajal ise blokeeritavaid numbreid sisestada. *SMS Filter* testitavas telefonis ei tööta ning viirusetõrje kuvab informatsiooni, et antud funktsioon ei tööta *Android* 4.4 ja uuemate süsteemide peal.

Viimaseks funktsiooniks on *Data Monitor*, mille abil saan seada limiidi sellele kui palju kasutaja kuu aja jooksul mobiiliandmeside saab kasutada. Samuti saan päevade kaupa jälgida kasutust. Lisaks asub siin veel *Firewall* ehk tulemüür, mis töötab ainult siis kui viirusetõrjel on administraatori õigused telefonis. Lubades viirusetõrjele administraatori õigused, antud funktsioon ei käivitu, väites endiselt, et administraatori õigusi on vaja viirusetõrjel. Lisaks leidub

siin funktsioon nimega *Statistics*, mis minu kasutatava operatsioonisüsteemiga ei tööta(*Your phone does not support this feature*).

Veel saame anda tootjale tagasisidet. Kontrollida, kas viirusetõrje töötab ikka viimasel versioonil. Seadete alt saab viirusetõrje keelt muuta. Valikuid on 34, kuid eesti keel on puudu.

Viirusetõrje nimest paremal asub kaks ikooni. Esimene neist sisaldab sõna *ADs* ehk reklaamid. Sinna vajutades kuvatakse erinevad rakendused. Rakenduse peale vajutades, suunatakse teid *Play Poodi*, kus saate rakenduse telefoni paigaldada. Teiseks ikooniks on lukumärk, mis suunab teid funktsiooni *AppLock*, millest sai juba räägitud.

Tulles tagasi avakuvale, jaotub viirusetõrje kolmeks. Esimeseks on *Boost*, millest sai räägitud paigaldamise käigus enne esmase pildi tegemist.

Teiseks on *Clean,* mis otsib ning seejärel eemaldab süsteemi ja rakenduste üleliigset vahemälu.

Kolmas on *Antivirus*, millega käivitatakse *Full Scan*, millest oli varem juttu. Lisaks saame sisse lülitada funktsiooni nimega *Payment Protection*, mis reaalajas kontrollib rakendusi, millega saame teostada oste telefonis. Veel on siin all *Privacy*, mis avab varem mainitud funktsiooni *AppLock.* Viimaseks on siin *Malware*, mis taaskord käivitab kontrolli (Joonis 21).

Eripärad

Tegu on tasuta viirusetõrjega. Telefoni on võimalik arvuti teel lukustada, asukohta määrata, eemaldada kogu sisu ning käivitada alarmi. Saame telefoni numbreid blokeerida. Telefonis olevaid rakendusi lukustada ja eemaldada viirusetõrje abil. Saame kontrollida telefoni protsessori temperatuuri ja vajadusel seda jahutada. On võimalik seada limiit mobiiliandmeside kasutusele ühe kuu jooksul. Kuna esines teatud probleeme, siis teavitasin sellest ka tootjat ning ootan nendepoolselt tagasisidet, miks ikkagi nii juhtus. Kirjale järgnes automaatne vastus, et minu saadetud tagasisidet võetakse arvesse, aga vastust minu esitatud küsimustele ei ole autor saanud veel. Kirja saatis autor kuu aega tagasi.

Eksperiment

Test ebaõnnestus täielikult. Kõik failid sain allalaadida ning avada. Hilisem kontroll pahavara ei tuvastanud.

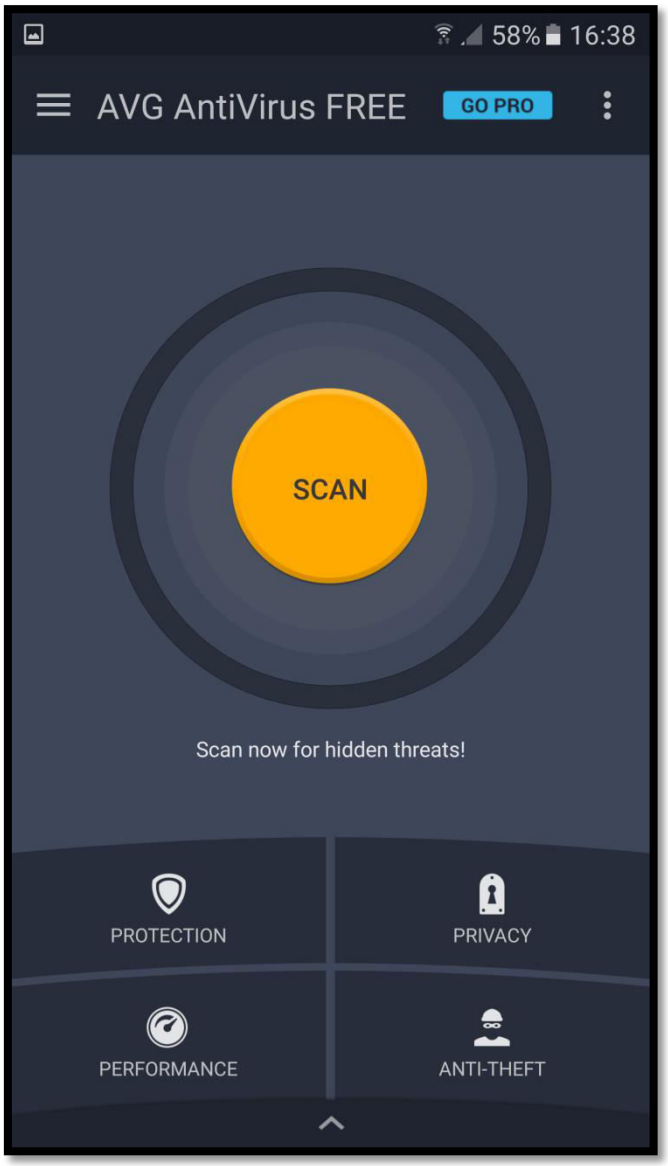
3.4 AVG AntiVirus FREE

Koduleht: http://www.avg.com/ww-en/homepage

Telefoni operatsioonisüsteem: Android 2.2 või hilisem (What are the minimum system requirements for installing and running AVG AntiVirus, kuupäev puudub).

Paigaldamine

Sisenen *Play poodi* ning otsingusse kirjutan *avg antivirus*. Avan esimese vastuse, milleks on *AntiVirus FREE 2016 - Android.* Jääb veel vajutada *Install* ehk paigalda. Saab juurdepääsu 14 õigusele. Enne kui käivitame viirusetõrje tutvume ja loeme läbi viirusetõrje kasutustingimused ja privaatsuspoliitika. Nõustumiseks vajutame *Get Started*. Järgmisena soovitatakse soetada viirusetõrje tasuline versioon reklaamide eemaldamiseks. Täishind kuuks ajaks tasulisele versioonile maksab €2.50 ning aastase versiooni hinnaks on €9.00. Tasuta versioon viirusetõrjest käivitus ning avakuva on selline (Joonis 22).



Joonis 22. AVG AntiVirus FREE

Kasutajaliides

Alustame kõige ülevalt viirusetõrje nime kõrvalt. Paremal on kolm punkti üksteise all, kus saame uuendada tasulisele versioonile ning avada abi faili, kuhu probleemide tekkimisel pöörduda. Kolme punkti kõrval asub sinise taustaga kast *GO PRO*, kuhu vajutades saame uuendada viirusetõrje tasulisele versioonile. Liikudes edasi vasakule poole, kus asuvad kolm kriipsu üksteise all, avaneb menüü kõikide viirusetõrje funktsioonidega, millega järgnevalt lähemalt tutvume.

Esimene *Log in* võimaldab meil registreerida uue kasutaja või siseneda juba varem registreeritud kasutajaga. Kasutajat on vaja funktsiooni *Anti Theft* kasutamiseks, millest tuleb hiljem juttu. Kasutaja registreerimiseks on vajalik e-postiaadressi ja salasõna sisestamine.

Järgmiseks on *Upgrade*, kus on võimalik tasuta versioon uuendada tasuliseks.

Esimeseks funktsiooniks on *App Lock*, mille puhul nõutakse kohe neljakohalise koodi sisestamist. Seejärel saame valida, millistele rakendustele telefonis määrame sisestatud koodi.

Teine funktsioon nimega *Vault*, mille puhul taaskord nõutakse neljakohalist koodi. Peale koodi sisestamist on võimalik lisada pilte telefonist, mis jäävad edaspidi sisestatud koodi kaitse alla teiste silmade eest varjatuks.

Nüüd olemegi jõudnud funktsioonini, mille jaoks alguses kasutaja registreerisime. Selleks on *Anti Theft*. Antud funktsioon vajab telefoni administraatori õigusi. Arvuti abil on võimalik määrata telefoni asukohta, käivitada alarmi või eemaldada kogu sisu. Lukustada telefon neljakohalise koodiga ning sisestada sõnum telefoni ekraanile. Lisaks kasutades kellegi teise telefoni on võimalik sõnumi abil kadunud telefonil käivitada alarm, eemaldada kogu sisu, lukustada seade või määrata asukoht. Näiteks alarmi käivitamiseks piisab sõnumist, mis sisaldab *AVGSHOUT PIN*.

Neljandaks funktsiooniks on *Battery Usage*. Kõigepealt kuvatakse info aku hetke seisust ning tuuakse välja aku temperatuur. Samuti on võimalik valida *Power Save*, mis tuleb kasuks kui aku on kohe tühjaks saamas, aga oleks vaja veel mõni minut vastu pidada. Selleks lülitatakse välja näiteks traadita võrk ja sinihammas ning reguleeritakse ekraani heledust ja heli tugevust. Lisaks saame seada viirusetõrje hoiatama kui aku protsent jõuab alla teatud taseme. Veel kuvatakse informatsioon sellest, kaua ma saan antud aku taseme juures telefoniga rääkida, vaadata videoid või kuulata muusikat.

Viies funktsioon kannab huvitavat nime milleks on *Task Killer*. Funktsioon kuvab ette kõik hetkel töötavad rakendused. Kasutaja saab nad mugavalt ühe nupuvajutusega ükshaaval sulgeda. Võimalus on ka vajutada all olevat nuppu *Boost*, mis sulgeb kõik rakendused ise.

Järgmiseks pakutakse teisi tootja tooteid telefonile (*More AVG Apps*).

Seadete ehk *Settings* alt saame muuta turvalisuse seadeid. Näiteks seada planeeritud kontrolli. Kontrolli on võimalik seada tegema kas iga päev või nädalas korra. Samuti saame valida

kontrolli tundlikkust. Valikusteks on madal(*Low*), kõrge(*High*) või väga kõrge(*Extra Sensitive*). Lisaks saame sisse lülitada lisa veebilehitsejaga turvaliseks sirvimiseks(*Safe Web Surfing*). Teise lisa sisse lülitamisel kontrollitakse ka telefoni välismälu(*Scan External Storage*). Veel saame muuta funktsiooni *Anti Theft* seadeid ning privaatsuse seadeid. Antud seadete alt saame sisse lülitada kõnede logi kustutamise, tundlikele rakendustele koodiga kaitse ning, et privaatsed pildid oleksid funktsiooni *Vault* koodiga kaitstud.

Viimaseks saame avada abi faili kuhu probleemide korral pöörduda. Samuti on võimalik saata tootjale tagasisidet.

Ekraani keskel asub suur ümmargune nupp nimega *Scan* ehk kontroll. Kontrollitakse kõiki rakendusi ja telefonis olevaid faile. Lisaks otsitakse privaatsusega seotud probleeme.

Viirusetõrje alumine pool jaotub neljaks kastikeseks. Vasakult esimene nimega *Protection* sisaldab failide ja rakenduste kontrolli. Saame algatada ka uuendamise protsessi ning vaadata veelkord üle turvalisuse seaded.

Temast paremale jääb kast nimega *Privacy* ehk privaatsus. Siin on kuvatud kõik kasutaja privaatsusega seotud funktsioonid. Samuti näeme, et funktsioonid *App Lock, Vault* ja *App Backup* on tasulise versiooni osad ning nimetatud funktsioone saame proovida 30 päeva. Lisaks saame siit avada viirusetõrje veebilehitseja, millega peaks olema turvalisem internetis ringi liikuda. Viirusetõrje veebilehitseja ei jäta andmeid meelde ja hoiatab kasutajat ebaturvaliste veebilehtede eest(*Secure Search*). Veel asub siin funktsioon nimega *Call Blocker*, mis teeb võimalikuks numbrite blokeerimise. Võimalus on ka eemaldada telefonist kõik kontaktid või kõnede logi. Vajadusel saame eemaldada kogu telefoni sisu ning muuta privaatsuse seadeid.

Liikudes edasi kasti juurde *Performance*. Siia alla on koondunud juba nimetatud lisadest *Task Killer* ja *Battery Usage*. Järgnevad *Data Usage*, mis aitab jälgida kulutatud mobiiliandmeside hulka ning *Storage Usage*, mis kuvad kui palju telefoni mälu on kasutatud. Samuti saame eemaldada rakendusi. Et puhastada telefoni üleliigsetest failidest, siis selleks pakub tootja tasuta lisa nimega *Cleaner 2016 - Clean & Boost*. Nimetatud lisa peab eraldi allalaadima. Nagu juba mainitud saame antud lisa abil eemalda ebavajalikud failid ja rakenduste vahemälu, mis suurendavad telefoni kiirust ja aitavad säästa akut. Aku koha pealt veel nii palju, et kuvatud on protsessori temperatuuri ja aku kestvust ajaliselt. Lisaks vaadatakse üle telefonis olevad pildid ning paljude korduste puhul soovitakse mõningad eemaldada.

Viimaseks kastikeseks on juba tuttav funktsiooni *Anti Theft* (Joonis 22).

Eripärad

Viirusetõrje tasuta versioon omab vähe funktsioone. Tasulise versiooni funktsioone saame proovida 30 päeva. Planeeritud kontrolle saab seada ning viirusetõrje seest avada veebilehitseja. Telefoni aku temperatuuri ja kestvust jälgida. Saab rakendusi sulgeda ning tasuta lisa üleliigsetele failide eemaldamiseks. Kõnesid blokeerida ja kontrollidele tundlikust määrata. Kaotamise korral sai nii telefoni lukustada kui ka alarmi käivitada nii arvuti kui teise telefoni abil. Tasuta viirusetõrje.

Eksperiment

Test algas ebaõnnestunult, sest kõik failid sain allalaaditud ja avada. Kontrolli käigus avastati kõik failid ja kasutaja nõusolekul failid eemaldati telefonist.

4. iOS

Mainitud operatsioonisüsteemi viirusetõrjete testimiseks kasutan nutitelefoni, mis jookseb versioonil iOS 10.0.2 (14A456). Nelja testitava väljavalimiseks sisestasin *App Store* otsingusse sõna *antivirus* ning neli populaarsemat saigi valitud. Samuti oli tähtis viirusetõrje reiting kui see oli tekkinud. Jälgisin ka, et viimane uuendas viirusetõrjele oleks tehtud käimasoleval aastal ning mida hiljem, seda parem.

Kui nüüd võrrelda kahte testitavat telefoni operatsioonisüsteemi turvalisuse kohapealt, siis hetkel on *iOS Androidist* üle. Seda sel lihtsalt põhjusel, et *iOSi* puhul tegeleb kõigega telefoni juures selle tootja *Apple*. See tähendab, et tootja tegeleb operatsioonisüsteemi vigade parandamisega, rakenduste turvalisusega ning püsivaraga. Rakendusi saab allalaadida vaid selleks ettenähtud kontrollitud keskkonnast. Tasuks ka ära mainida, et *iOS* ei ole hetkel sama populaarne oma konkurendiga, mistõttu pigem satub rünnakute alla *Androidi* kui *iOSi* operatsioonisüsteemi kasutav seade. Kuna *iOSi* tarkvara kasutavad ainult *Apple* tooted, siis operatsioonisüsteemi killustatus on väiksem kui *Androidi* puhul ja seeläbi enamus *Apple* toote kasutajad kasutavad sama operatsioonisüsteemi. See kõik on tore, aga ei tähenda mingil juhul, et viirusetõrjet antud operatsioonisüsteemi puhul ei peaks kasutama (Murdock, 2016). Ka rakenduste kontrolli osas on *Apple* valinud selgelt rangema poliitika, sest autorid rakendus peab läbima põhjaliku kontrolli enne kui keegi kasutajatest saab seda oma telefoni allalaadida (Armendariz, 2016). Lisaks sellele tuleks tutvuda ka soovitustega kasutajale (Lisa 3).

4.1 McAfee Mobile Security

Nõuded telefonile

Koduleht: https://www.mcafee.com

Telefoni operatsioonisüsteem: iOS 8.0 või hilisem (CompatibiltyA, 2016).

Paigaldamine

Avan *App Store* ning kirjutan otsingusse *mcafee mobile security*. Valin *get* ning järgmisena *install* ehk paigalda. Sisestame *Apple ID* salasõna. Esimesel käivitusel peaks iga kasutaja läbi lugema nii litsentsilepingu kui ka privaatsuse seaded. Järgmiseks tuleb registreerida kasutaja.

Selleks sisestame e-postiaadressi koos salasõnaga. Veel pakutakse lisa, mille abil on võimalik ühendada viirusetõrje seadmega *Apple Watch*. Seejärel on kasutajal võimalik jälgida kella abil aku taset ning käivitada alarmi. Arvutist on lisaks võimalik seada kood kaitsmaks telefonis olevaid pilte ja videoid, varundada telefoni salvestatud kontakte ning sisse lülitada asukoha määramine, et oleks võimalik telefoni asukohta määrata. Peale seda kõike käivitus viirusetõrje esimest korda ja viirusetõrje avakuva näeb välja selline (Joonis 23).

Joonis 23. McAfee Security

Kasutajaliides

Alustame tutvustust kõige ülevalt vasakust nurgast, kus asuvad kolm kriipsu üksteise all. Sinna vajutades avaneb uus menüü vasakult. Sealt saame esimesena avada seaded, kus näeme registreeritud kasutaja e-postiaadressi. Saame määrata kuuekohalise koodi piltide ja videode kaitsmiseks. Sellega seotult saame sisse lülitada lisa nimega *CaptureCam*, mis pildistab kasutajat, kes on kolm korda koodi valesti sisestanud ning saadab selle registreeritud kasutaja e-postiaadressile. Samuti on võimalik kõik telefonis olevad pildid ja videod varundada pilve (*iCloud*). Veel saame telefoni ühendada seadmega *Apple Watch*. Järgmiseks on võimalik taaskord kuvada lisade tutvustus, mis avanes esimesele käivitusel. Kolmandaks on võimalus tutvuda antud viirusetõrjega lähemalt ehk avatakse viirusetõrje dokumentatsioon. Kasutajale on antud ka võimalus hinnata antud toodet ning jagada tagasisidet tootjale. Kui kasutajal jäi alguses litsentsileping ja privaatsuse seadmed lugemata, siis saab dokumente uuesti lugeda siit.

Ülejäänud avakuva on jaotunud kolmeks funktsiooniks. Kõige suurem neist kannab nime *Vault*. Siia saab kasutaja lisada oma telefoni pildid ja videod, mida soovitakse koodiga kaitsta. Seejärel soovitakse need pildid ja videod eemaldada telefonist. Tasub veelkord mainida, et sissetungija tabamiseks on võimalik seadete alt sisse lülitada lisa *CaptureCam*, mis kolme vale koodi sisestamise korral teeb pilti ja saadab pildi kasutaja registreeritud e-postiaadressile.

Teises kastis olev funktsioon kannab nime *Contacts Backup*, mis varundab telefoni salvestatud kontaktid.

Kolmandaks funktsiooniks on *Device Security*. Telefoni asukoha sisse lülitamisel salvestatakse telefoni asukoht iga 24 tunni järel. Minimaalselt on kasutajal võimalik määrata näiteks iga 1 tunni tagant asukoha informatsiooni salvestama. Samuti on võimalus sisse lülitada lisa nimega *S.O.S*, mis salvestab telefoni viimase asukoha, enne kui telefoni aku tühjaks sai. Telefoni kaotamise korral on võimalik asukohta määrata arvutist. Kui logida sisse registreeritud kasutajaga on kasutajal võimalik määrata telefoni asukoht või kuvatakse viimane asukoht, enne kui aku tühjaks sai. Veel saab kasutaja käivitada alarmi, eemaldada või varundada kõik kontaktid ja kirjutada sõnumi telefoni ekraanile (Joonis 23).

Eripärad

Kasutaja vaja registreerida. Lisadest tasuks ära märkida *Vault* ja *CaptureCam*. Samuti *Device Security*, millega telefon kadumise korral üles leida ja ühildub seadmega *Apple Watch*. Kontaktide varundamise võimalus ka. Tasuta viirusetõrje.

Eksperiment

Test oli ebaõnnestumine, kuna viirusetõrje poolt ei tulnud mingit reageeringut ohule.

4.2 Lookout

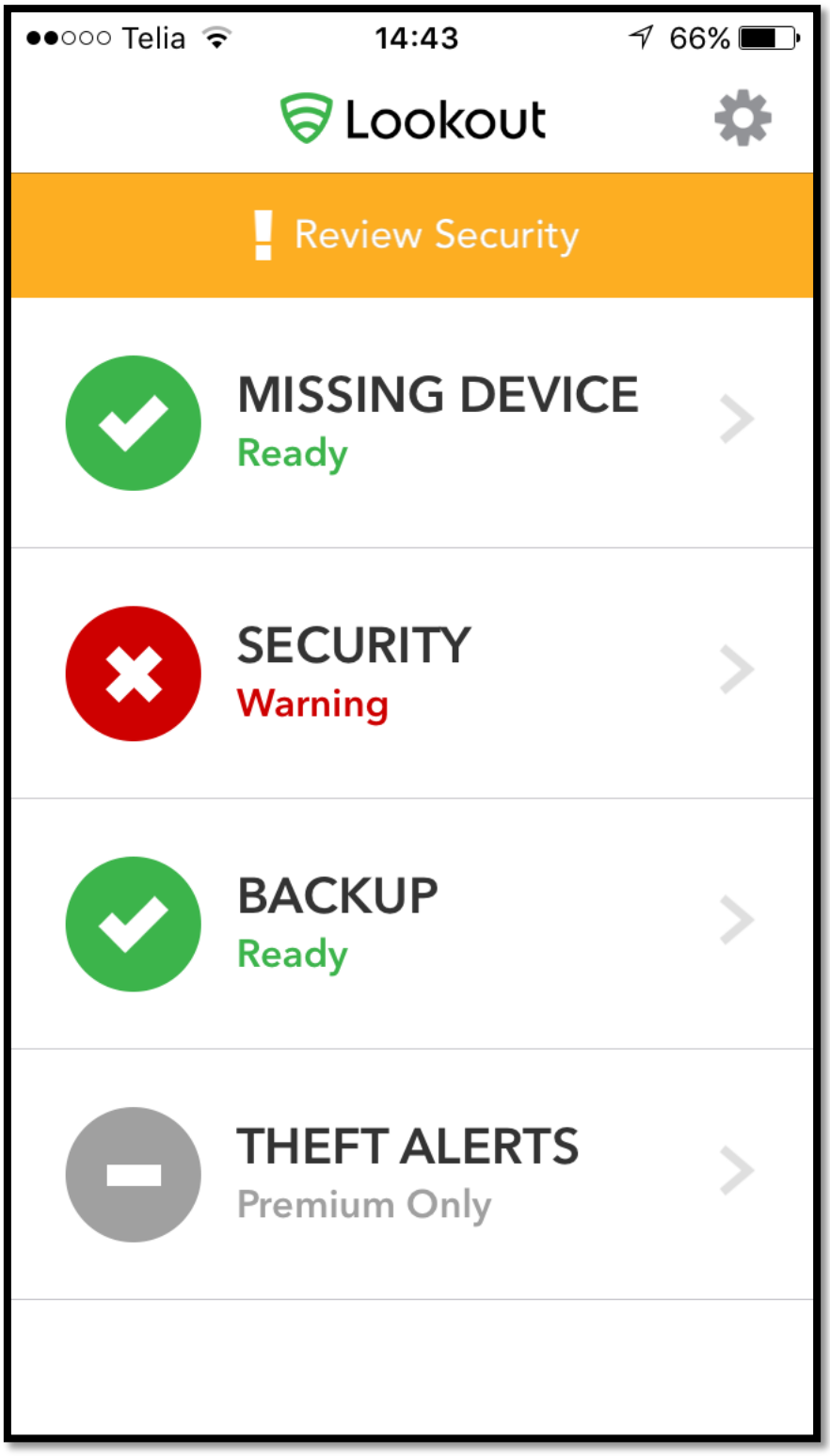
Nõuded telefonile

Koduleht: https://www.lookout.com

Telefoni operatsioonisüsteem: iOS 8.0 või hilisem (CompatibiltyB, 2016).

Paigaldamine

Asun otsima *App Store*, kuhu otsingusse sisestan *lookout mobile security*. Esmalt *get* ning seejärel *install.* Enne kui telefon saab paigaldamist alustada on vaja veel sisestada *Apple ID* salasõna. Esimesel käivitusel tuleb läbida huvitav küsitlus, mille läbi tutvustatakse viirusetõrje erinevaid funktsioone. Peale seda tuleb registreerida kasutaja, milleks sisestame e-postiaadressi koos salasõnaga ning nõustume kasutajatingimustega ja privaatsuspoliitikaga, millega tuleks kindlasti enne nõustumist tutvuda. Viirusetõrje on välimuselt selline (Joonis 24).



Joonis 24. Lookout

Kasutajaliides

Alustame viirusetõrje nime kõrvalt ülevalt paremalt, kus asub mutrike. Tema all asuvad viirusetõrje kõik seaded. Sealt saame lülitada sisse või välja viirusetõrje kõiki funktsioone. Samuti saame veelkord lugeda nii kasutajatingimusi kui ka privaatsuspoliitikat. Lisaks saame abi otsida probleemide korral ning lugeda lähemalt antud viirusetõrje kohta.

Viirusetõrje jaguneb neljaks, millest esimene kannab nime *Missing Device*. Antud funktsiooni jaoks registreerisimegi kasutaja. Telefoni kadumisel on võimalik arvutist määrata asukohta, käivitada alarm või saata telefonile sõnum. Sõnumi eesmärgiks on telefoni leidjaga kontakti loomine.

Teine funktsioon nimega *Security*, mis jälgib, et telefon kasutaks viimast operatsioonisüsteemi. Samuti kontrollitakse telefonis olevaid rakendusi. Antud telefoni puhul kuvab viirusetõrje hoiatuse, kuna värskendus operatsioonisüsteemile on väljas.

Kolmanda funktsiooni nimi on *Backup*, mille abil saame telefoni salvestatud kontaktidest luua varukoopia. Varukoopiat saame näha arvutist, sisenedes tootja kodulehel varem registreeritud kasutajaga. Tasulise versiooni puhul saame ka piltidest luua varukoopia.

Viimast funktsiooni autor kasutada ei saa, kuna selleks peame soetama tasulise versiooni antud viirusetõrjest. Et tasulist kasutada kuu aega, tuleb tasuda £2.29 (u. €2.6) (Joonis 25).

Eripärad

Telefoni kontrollib operatsioonisüsteemi uuendusi ja rakendusi telefonis. Telefon uuendab asukoha infot, jälgides telefoni akut. Seda selleks, et kasutaja saaks vaadata arvutist viimast asukohta enne kui aku täiesti tühjaks sai. Lisaks saame luua varukoopia oma kontaktidest. Tegu on tasuta viirusetõrjega, mida saab rohkemate funktsioonide kasutamiseks uuendada tasuliseks. Ühildub *Apple Watch*-ga.

Eksperiment

Test ebaõnnestus kuna viirusetõrje ei reageerinud failidele üldse.

4.3 F-Secure SAFE

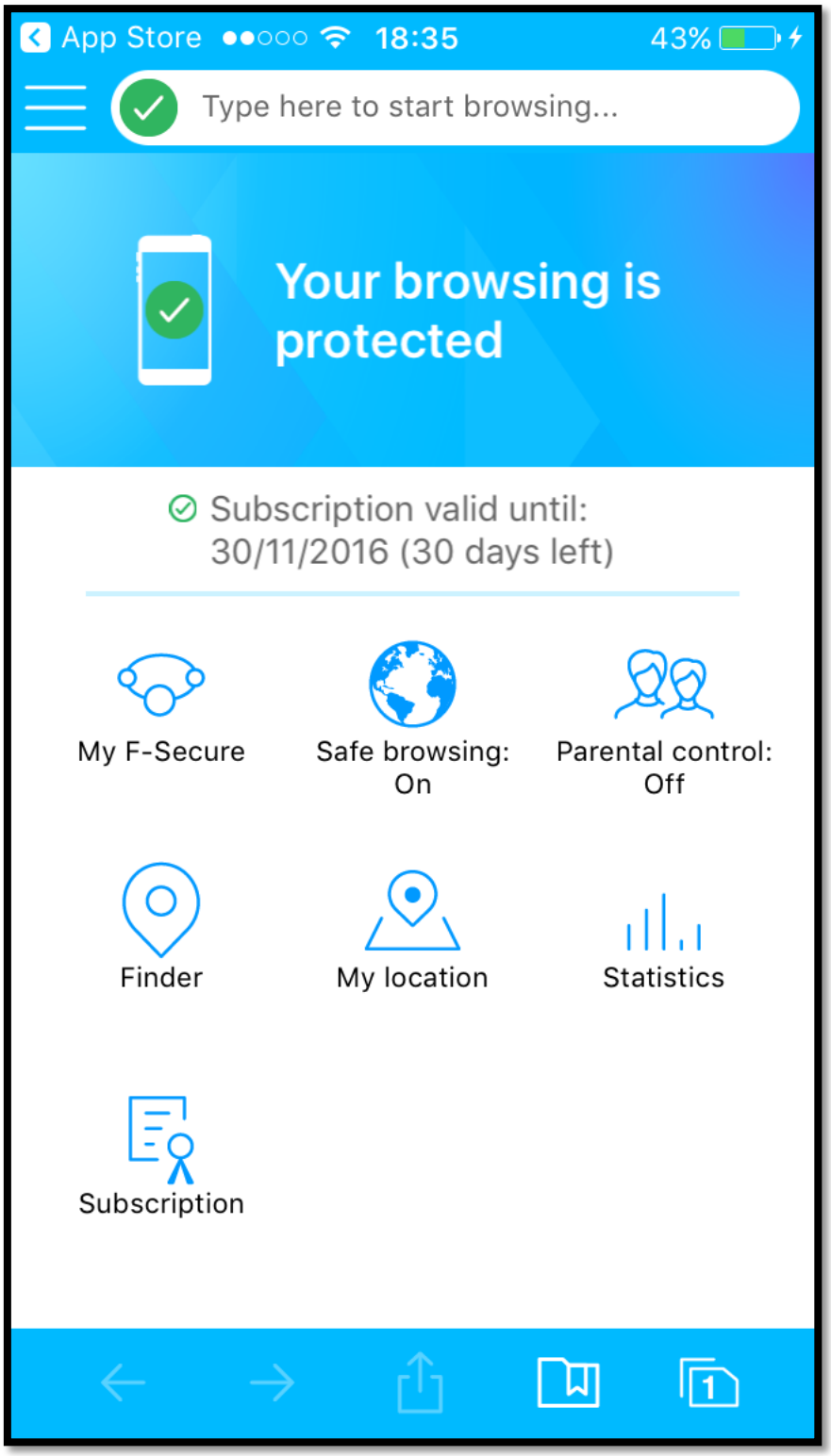
Nõuded telefonile

Koduleht: https://www.f-secure.com

Telefoni operatsioonisüsteem: iOS 8.0 või hilisem (CompatibiltyC, 2016).

Paigaldamine

App Store otsingusse kirjutan *f-secure safe*. Vajutan *get* ja *install* ehk paigalda. Jääb veel sisestada *Apple ID* kasutaja salasõna. Esimesel käivitusel tuleks lugeda läbi ja seejärel nõustuda lõppkasutaja litsentsilepinguga kui ka privaatsuspoliitikaga. Lisaks soovib tootja kasutaja nõusolekul koguda anonüümset infot viirusetõrje töö kohta, et arendada antud toodet edasi. Seejärel tuleb registreerida kasutaja. Selleks on vaja kas sisestada eesnimi, perekonnanimi, e-postiaadress ning salasõna või võib ka kasutada *facebooki* kontot. Järgmiseks peame oma seadmele nime panema. Viirusetõrje avakuva näeb välja selline (Joonis 25).



Joonis 25. F-Secure SAFE

Kasutajaliides

Alustan viirusetõrje tutvustust ülevalt vasakust nurgast, kus asuvad kolm kriipsu üksteise all. Sinna vajutades avaneb menüü vasakult, kust saame muuta vanemate kontrolli ja asukoha määramise seadeid. Lisaks näeme ära kui kaua antud prooviversioon kehtib veel ning vajadusel saame uuendada tasuliseks. Aastane litsents maksab €49.90. Veel saame lugeda antud toote kohta ja kohandada funktsioone. Kriipsude kõrvalt saame läbi viirusetõrje internetis erinevaid veebilehti külastada ja kuvatakse, kas antud veebileht on turvaline või mitte.

Alla liikudes kohtame seitset funktsiooni. Esimene neist kannab nime *My F-Secure*, mis suunab mind registreeritud kasutajaga tootja kodulehele. Saan määrata telefoni asukohta ja käivitada alarmi funktsiooniga *Finder* ja muuta seadme nime. Samu tegevusi saan ka sooritada arvutist sisse logides.

Järgmine funktsioon kannab nime *Safe browsing*. Seadete all määrame veebilehitsejale otsingumootorid, saame sisse lülitada privaatse sirvimise ning tühjendada veebilehitseja vahemälu.

Esimese rea viimane funktsioon nimega *Parental control* ehk vanemate kontroll. Antud funktsiooni sisse lülitamisel saame seada ajalise limiidi interneti kasutamiseks. Lisaks saame määrata, millist sisu blokeerida veebilehitsejas ning seada salasõna neile seadetele. Kes salasõna ei tea, ei saa vanemate kontrolli ka välja lülitada.

Neljandast funktsioonist *Finder* sai juba natukene räägitud. Eelnevale on lisada vaid see, et oma asukohta saab jagada teistega läbi sõnumi või e-postiaadressi.

Viies funktsioon *My location* kuvab telefoni asukoha kaardil. Asukohta on võimalik jagada, saates oma asukoha aadressi sõnumiga või e-posti kirjana.

Kuuendaks funktsiooniks on *Statistics*, mis kuvab mitu veebilehekülge on siiani külastatud ning mitu neist on blokeeritud.

Viimane funktsioon *Subscription*, kus näeme kaua kasutatav prooviversioon veel kehtib. Samuti näeme loetelu funktsioonidest, mis prooviversiooniga kaasnevad. Vajadusel saab kasutaja soetada tasulise versiooni (Joonis 25).

Eripärad

Kohe mainiks ära, et viirusetõrjet saavad paigaldada inimesed, kes on vähemalt 17 eluaastat vanad ehk kui kasutaja *App Store* konto vanuseks pole 17 täis, viirusetõrjet paigaldada ei saa. Kasutaja peab registreerima, et kadumise korral telefoni asukohta määrata või käivitada alarmi. Vanemate kontrolli ja asukoha jagamine sõnumi või e-posti teel. Võimalik internetis erinevaid veebilehti külastada läbi viirusetõrje.

Eksperiment

Läbi viirusetõrje veebilehitseja üritades allalaadida antud faile, reageeris esimesele ja kolmandale. Kui nüüd kasutada telefoni veebilehitsejat, milleks on *Safari*, siis polnud probleeme kõikide failide allalaadimisega ega avamisega.

4.4 360 Security

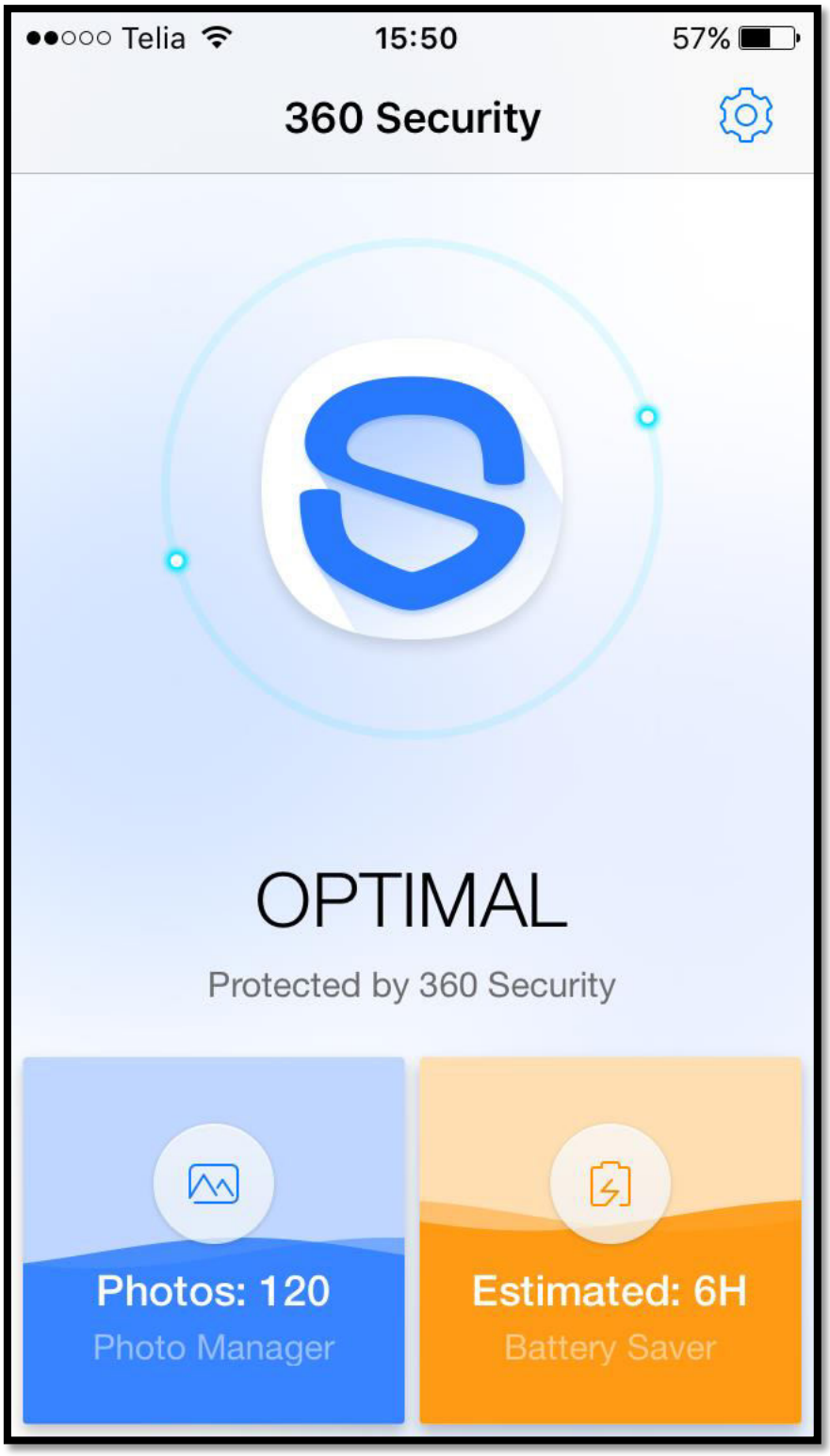
Nõuded telefonile

Koduleht: https://www.360totalsecurity.com

Telefoni operatsioonisüsteem: iOS 7.0 või hilisem (CompatibiltyD, 2016).

Paigaldamine

Avades *App Store* kirjutame otsingusse *360 security*. Vajutame *get* ja *install*. Veel *Apple ID* kasutaja salasõna. Esimesel käivitusel viirusetõrje soovib ligipääsu piltidele. Peale paigaldamist näeb viirusetõrje välja selline (Joonis 26).



Joonis 26. 360 Security

Kasutajaliides

Alustame ülevalt paremast nurgast, kus asub mutter, mille all peidavad ennast viirusetõrje seaded. Sealt saame näiteks sisse lülitada seade, et viirusetõrje annab teada kui telefoni aku täis on laetud või viirusetõrje ei anna endast märku öötundidel (23:00 kuni kella 8:00). Lisaks saame ka hinnata antud viirusetõrjet või anda tagasisidet tootjale. Viirusetõrje kohta näeme tema versiooni ja saame tutvuda nii privaatsuspoliitikaga kui ka lõppkasutaja litsentsilepinguga. Keelt saame ka muuta ning valikuid on 34 kuhu eesti keel ei kuulu.

Liigume edasi alla, kus asuvad kaks kastikest. Esimene neist on *Photo Manager*, kus viirusetõrje vaatab telefonis olevad pildid üle ning jaotab nad ära. Näiteks kui palju on ekraanist tehtud pilte või palju on korduvaid pilte. Korduvate piltide puhul soovib viirusetõrje nad eemaldada, jättes alles ühe pildi.

Teine kast kannab nime *Battery Saver* ning sealt näeme kaua telefoni aku veel kestab. Peale vajutades kuvatakse täpsem informatsioon protsentides. Lisaks näeme kui kaua on telefoniga võimalik näiteks mängida, vaadata filme või kuulata muusikat (Joonis 26).

Eripärad

Tasuta viirusetõrje. Üllatavalt suur keelte valik. Viirusetõrje kontrollib pilte ja vajadusel eemaldab korduvad. Samuti näeme aku kestvust erinevate tegevuste puhul.

Eksperiment

Test ebaõnnestus. Kõiki failid sain allalaadida ja avada.

5. Analüüs

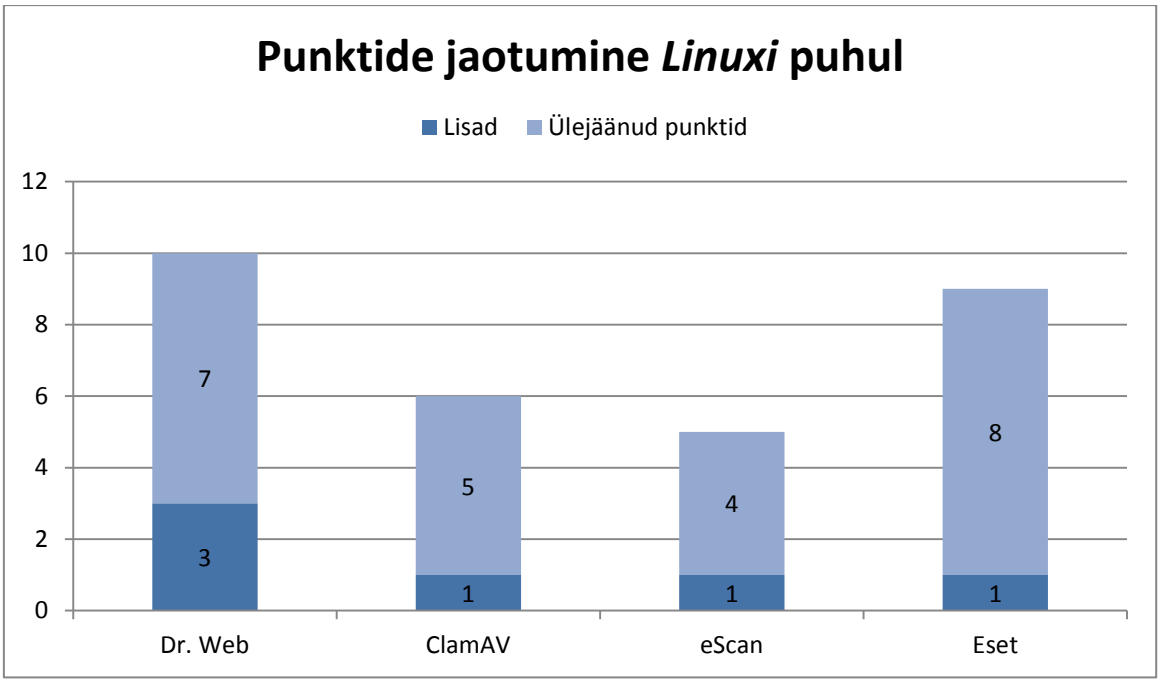
Siinkohal saab lugeda autori poolset kokkuvõtet testimistest iga operatsioonisüsteemi kohta ning näha punktitabelit, mis sai kokku pandud funktsioonide põhjal (Tabelid 1-4) ning nende jaotust lisade ja muude punktide osas (Joonised 27-30). Põhjalikumaid tabeleid saab vaadata lisades, mis asuvad töö lõpus (Tabelid 5-8).

5.1 Linux Mint 18

Tabel 1. Linuxi viirusetõrjete punktid

Viirusetõrje	Dr.Web	ClamAV	eScan	Eset
Punktid	10 punkti	6 punkti	5 punkti	9 punkti

Katses osales neli viirusetõrjet, millest üks tasuta ja ülejäänud tasulised. Kõige rohkem jäid silma autorile samuti kaks kõige rohkem punkte teeninud viirusetõrjet. Samas olid nii eset kui dr.Web ka kõige kallimad tasulistest. Tasulistest valmistas kerge pettumuse eScan, millega tekkisid esimesed probleemid juba paigaldamisel. Autorina isiklikult nõustun moodustunud punktidega, kuna nii clamAV-l kui ka eScan juures olid omad omad murekohad. ClamAV suurimaks murekohaks oli küsimus, kas viirusetõrje on ikka uuendatud. Tasuline eScan ei olnud nii võimekas võrreldes dr.Webi või esetiga. Nii eset kui ka dr.Web eristusid selgelt neist neljast (Tabel 1). Aga see on ainult autori arvamus ning lõpliku otsuse teeb iga kasutaja iseseisvalt. Punktide jaotumist lisade ja ülejäänud punktide vahel saab näha järgnevalt (Joonis 27).



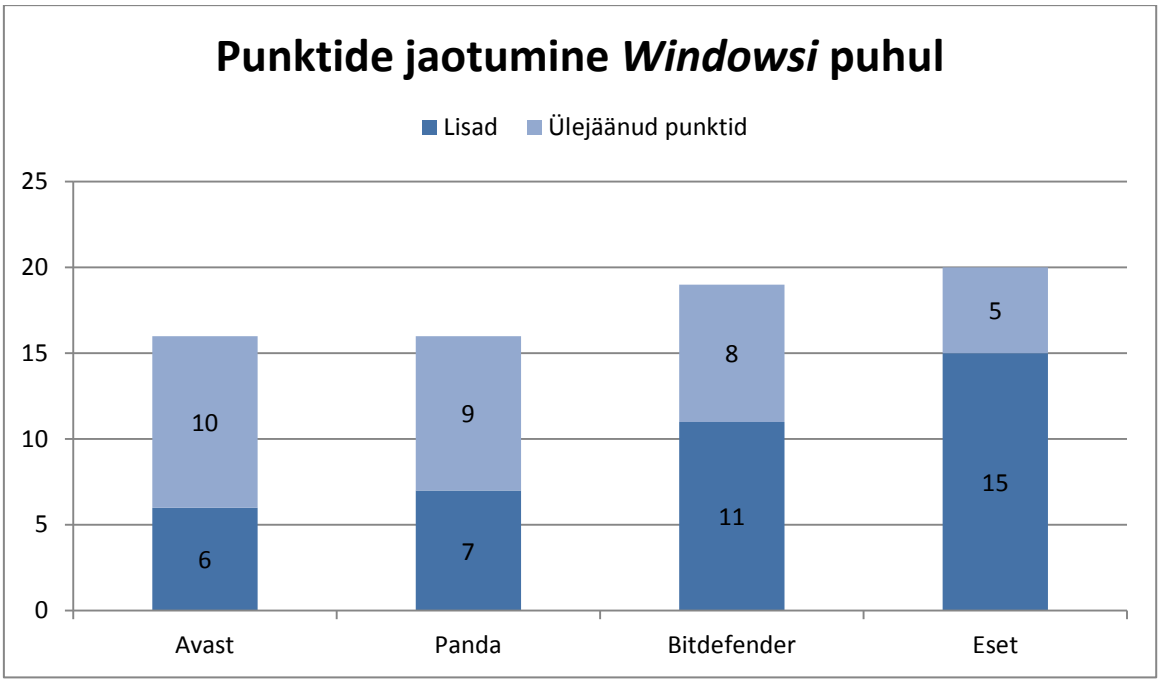
Joonis 27. Punktide jaotus operatsioonisüsteemi Linux Mint 18 puhul

5.2 Windows 10

Tabel 2. Windowsi funktsioonide punktid

Viirusetõrje	Avast	Panda	Bitdefender	Eset
Punktid	16 punkti	16 punkti	19 punkti	20 punkti

Testitud sai neli erinevat viirusetõrjet, millest kaks esimest olid tasuta ning kaks viimast tasulised. Nagu oodata oli, sisaldasid tasulised versioonid mõnevõrra rohkem funktsioone, mis kergitas eriti viirusetõrje eset positsiooni. Kui nüüd võrrelda ainult tasuta viirusetõrjeid, siis avast ja panda olid võrdsed punktitabeli järgi, aga autor eelistaks pigem avasti. Peamiseks põhjuseks on protsessori hõivamine kontrollide ajal, milles avast selgelt parem oli. Tasulistest viirustõrjetest jäi autori arvates peale bitdefender, kuigi punktitabel väidab vastupidist. Eset paistab silma paljude lisadega, aga ilma lisadeta jääks ta alla nii bitdefenderile kui ka tasuta viirusetõrjetele. Kokkuvõttes pean parimaks avasti viirusetõrjet, teisel kohal oleks bitdefender napi paremusega panda ees, kes jääb kolmandaks. Eseti jätaks esikolmikust välja just rohkete lisade tõttu. Erinevad lisad on kasulikud, aga kui neid on liiga palju, siis viirusetõrje põhilised omadused kannatavad (Tabel 2). Punktide jaotumist saab täpsemalt näha siin (Joonis 28).



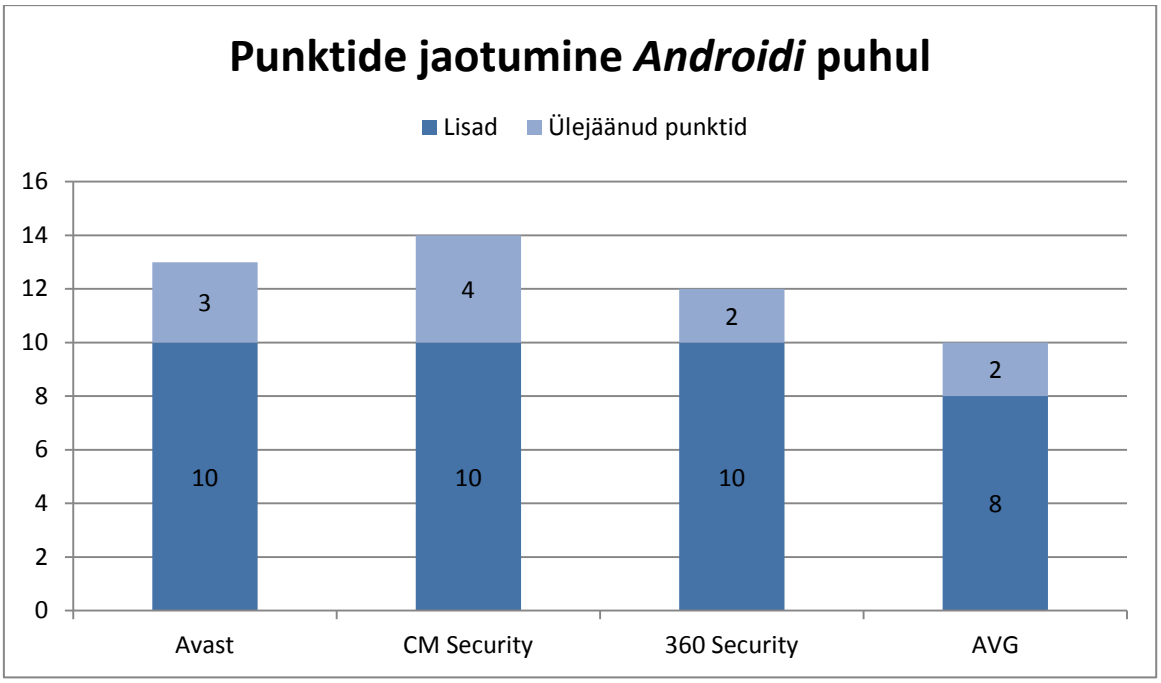
Joonis 28. Punktide jaotus operatsioonisüsteemi Windows 10 puhul

5.3 Android 6.0.1 Marshmallow

Tabel 3. Androidi funktsioonide võrdlus

Viirusetõrje	Avast	CM Security	360 Security	AVG
Punktid	13 punkti	14 punkti	12 punkti	10 punkti

Katsetatud sai läbi neli erineva tootja populaarset viirusetõrjet. Kõiki põhifunktsioone omasid kolm esimest, avg tasuta versiooni mitte. Avg puhul olid nii *AppLock* ehk rakenduste lukk ja *Vault*, kus oli võimalik pilte koodiga kaitsta, tasulise viirusetõrje osad. Kõige rohkem jäi mulle kui autorile silma mingil põhjusel avast, mis punktitabeli põhjal on samuti eesrinnas. Tundus olevat kõige rohkemate funktsioonidega ja koguaeg nähtaval kohal. Samas palju ei jäänud alla ei cm security kui ka 360 security. Samuti suutsid ainult avast ja avg leida allalaaditud viirusetesti failid ja nii cm security kui ka 360 security puhul esines probleeme. Cm security puhul ei olnud võimalik kasutajat registreerida, mille abil oleks kasutaja saanud arvutist näiteks telefoni positsioneerida. 360 security puhul ei saanud autor kolme funktsiooni kasutada kuna puudus toetus või lihtsalt ei käivitunud funktsioon. Kui nüüd medaleid jagada, siis kuld läheks minu poolt viirusetõrjele avast, teise koha annaksin pigem cm security-le ning kolmandaks jätaks 360 security. Väga napilt jääb avg tasuta versioon esimestele alla (Tabel 3). Täpsemalt saab punktide jaotumist näha siin (Joonis 29).



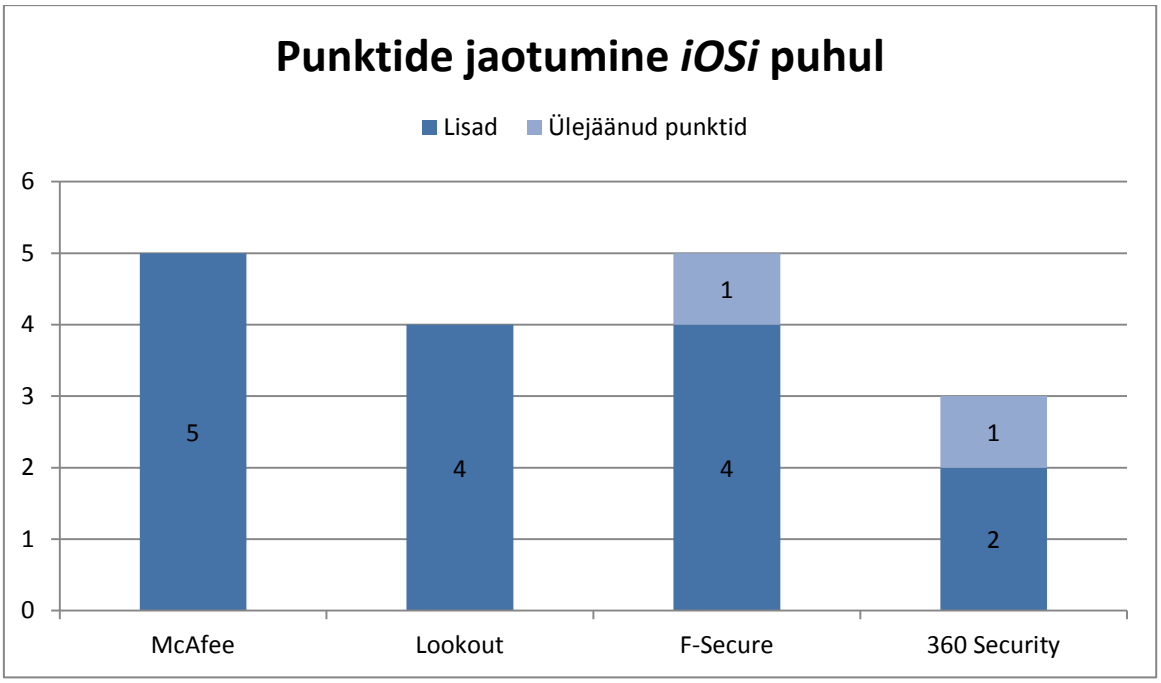
Joonis 29. Punktide jaotumine operatsioonisüsteemi Android 6.0.1 puhul

5.4 iOS 10.0.2

Tabel 4. iOS funktsioonide võrdlus

Viirusetõrje	McAfee	Lookout	F-Secure	360 Security
Punktid	5 punkti	4 punkti	5 punkti	3 punkti

Taaskord võib öelda, et sai võrreldud tasulist f-secure tasuta versioonidega ning tasuta versioonid ei jäänud kaugele. Kui veel arvestada f-secure aastase litsentsi hinda, siis isiklikult kasutaksin pigem tasuta viirusetõrjet. Tasuta viirusetõrjetest meeldisid nii lookout kui ka mcafee. Selgelt viimaseks autori silmis jäi 360 security, millel puudusid põhilised funktsioonid ja lisadega ei saanud viirusetõrje samuti hiilata. Võimalik on lookouti puhul tasuliseks uuendada, aga hind on pea kaks korda odavam kui f-secure puhul. Kokkuvõttes f-secure omas küll uusi ja huvitavaid funktsioone, aga autorina proovikson tasuta viirusetõrjet. Kas siis lookout või mcafee. Kumba neist eelistada sõltub rohkem sellest, mida kasutaja enda telefoni otsib. Järgmisena prooviksin pigem f-secure. Viimaseks valikuks oleks 360 security (Tabel 4). Lähemalt saab punktide jaotumisega tutvuda siin (Joonis 30).



Joonis 30. Punktide jaotumine operatsioonisüsteemi iOS 10.0.2 puhul

Kokkuvõte

Käesoleva bakalaureusetöö eesmärgiks oli tutvustada erinevate operatsioonisüsteemide viirusetõrjeid. Ühtlasi näidata erinevust tasuta ja tasulise toote vahel. Tänu antud bakalaureusetööle muutus kasutajatele viirusetõrje valik vastavalt kasutatavale operatsioonisüsteemile lihtsamaks. Samuti oskavad kasutajad edaspidi muuta oma turvakäitumist, mis aitab tõsta kasutajate teadlikkust internetis valitsevate ohtude eest.

Muidugi oleks mugavam kasutada ühte viirusetõrjet igas operatsioonisüsteemis aga peale bakalaureusetöö käigus läbitud testimisi saab järeldada, et parem ja kindlam valik oleks igas süsteemis omada just sellele operatsioonisüsteemile ehitatud toodet. Viirusetõrje juures on pigem oluline toote efektiivsus. Et kasutatav toode oleks võimeline avastama ja eemaldama pahavara seadmest. Samuti ei tasu kunagi vaadata viirusetõrjete hinnanumbrit, kuna peaaegu alati ei ühti antud toote hind tema efektiivsusega. Sellest saab järeldada ainult üht, et alati pole kalleim viirusetõrje parim ja odavaim automaatselt kehveim. Parim viirusetõrje on see, mis teeb oma tööd hästi ja hind, mida kasutaja tema eest maksab korvab tema väärtuse turvatundes, mida ta kasutajale loob. Lisaks peaks kasutaja olema võimeline muutma enda tegutsemist veebis selliselt, et tekiks võimalikult väike võimalus kuskilt endale pahavara saada. Selleks ei tule lugeda raamatut läbi, vaid piisab kümnekonnast näpunäitest. Koos viirusetõrje paigaldamise ja soovituste järgimisega aidatakse kaasa turvalisele keskkonna tekkele kasutatavas seadmes.

Erinevaid viirusetõrjeid on palju ja antud bakalaureusetöö jaoks pidi autor langetama raskeid otsuseid, valides testitavaid tooteid. Põhiliseks eesmärgiks ei olnud tõsta esile valitud viirusetõrjeprogramme vaid eelkõige näidata kasutajatele mida tasulised ja tasuta viirusetõrjed endas sisaldavad. Kui kasutaja otsustab valida viirusetõrje, mida autor ei testinud siis sellisel juhul on kasutajal võimalus võrrelda oma valikut bakalaureusetöös testitud programmiga. Seeläbi leiab kasutaja endale ja oma seadmetele selle kõige õigema viirusetõrje.

Summary

Title: Comparative analysis of antiviruses.

The aim of this Bachelor thesis is to introduce different antiviruses for different operating systems(Windows, Linux, Android and iOS). Author is using both free and paid versions of antiviruses. Also, talking about other security measurements besides antivirus and sharing some security tips for users.

To achieve this goal the author has chosen four antivirus programs for every operating system. The selection of antiviruses was made according to articles and downloading environments. Firstly, readers find explanations about different types of viruses and other concepts which were used during the thesis. Antivirus testing begins with introduction of requirements for computer or mobile phone. Next phase describes the download process and ends with listing of the main specs and tools for antivirus. Under experiments you can see how quickly antivirus scans files, how much it is effecting processor and is the antivirus capable of finding and then removing viruses. For Windows and Linux the author created dual-boot operating system and then tried to clean one operating system from inside another. The next analysis chapter contains the points tables with author comments. More detailed tables and eicar test results can be found under extras where you can also find statistics about malware and useful recommendations for users.

The purpose of this Bachelor thesis was achieved. Author goal was to introduce different antiviruses, which will help users to choose the best antivirus for their device because there are so many to choose from. Another purpose was to increase users knowledge about threats they can meet using their computer or mobile phone. That is why author is sharing some recommendations which decreases the chance of getting any kind of malware into your device.

In conclusion, every user should be looking and then installing an antivirus software into their computer or mobile phone. The most important thing about antivirus is how efficient it is because everyone make mistakes and it does not matter how big they are but how quickly you learn from them.

Kasutatud kirjandus

ADalma, H. (2016). *Can 2016 be the beginning of a new spam era?* Loetud aadressil http://www.2-spyware.com/news/post9238.html

Alias. (2012). *Pingviini viki*. Loetud 20. oktoober 2016 aadressil https://viki.pingviin.org/Alias

Anti-Malware Testfile. (kuupäev puudub). Loetud aadressil http://www.eicar.org/86-0-Intended-use.html

Armendariz, T. (2016). *Is Google Play Safe?* Loetud aadressil https://www.lifewire.com/is-google-play-safe-153675

Arvutikaitse ABC. (kuupäev puudub). Loetud aadressil http://www.arvutikaitse.ee/arvutikaitse-algtoed/

Avoid 10 fatal mistakes in Linux Mint and Ubuntu. (kuupäev puudub). Loetud aadressil https://sites.google.com/site/easylinuxtipsproject/fatalmistakes

AV-TEST. (2016). Loetud aadressil https://www.av-test.org/en/statistics/malware/

BDalma, H. (2016). *Murettekitav statistika: enamus pahatahtlikke spämmkirju kannavad ransomware-viirust*. Loetud aadressil http://viirused.ee/murettekitav-statistika-enamus-pahatahtlikke-spammkirju-kannavad-ransomware-viirust/

Best Free Online Backup. (2016). Loetud aadressil http://www.techsupportalert.com/content/best-free-online-backup-sites.htm

Can I set Firefox to always use Private Browsing. (kuupäev puudub). Loetud aadressil https://support.mozilla.org/en-US/kb/private-browsing-use-firefox-without-history

CompatibiltyA. (2016). Loetud aadressil https://itunes.apple.com/us/app/mcafee-mobile-security-vault/id724596345?mt=8

CompatibiltyB. (2016). Loetud aadressil https://itunes.apple.com/us/app/lookout-security-backup-missing/id434893913?mt=8

CompatibiltyC. (2016). Loetud aadressil https://itunes.apple.com/us/app/f-secure-safe/id572847748?mt=8

CompatibiltyD. (2016). Loetud aadressil https://itunes.apple.com/us/app/360-security/id1042556580?mt=8

Distributsioon. (2010). *Pingviini viki*. Loetud 20. oktoober 2016 aadressil https://viki.pingviin.org/Distributsioon

Dr.Web anti-virus for Linux. (2016). Loetud aadressil https://download.drweb.com/linux/?lng=en

Dreifeldt, T. (2015). *Tasuta viirusetõrjete võrdlus Microsoft Windows 8.1 näitel* (seminaritöö). Loetud aadressil http://www.cs.tlu.ee/teemaderegister/

ESET NOD32 Antivirus 4 for Linux Desktop FAQ. (2016). Loetud aadressil http://support.eset.com/kb2722/

Fisher, T. (2016). *6 Free Online Backup Plans*. Loetud aadressil https://www.lifewire.com/free-online-backup-plans-2625187

Forrest, C. (2016). *The state of mobile device security: Android vs. iOS*. Loetud aadressil http://www.zdnet.com/article/the-state-of-mobile-device-security-android-vs-ios/

Hallum, C. (2015). *Windows 10 Security Innovations at RSA: Device Guard, Windows Hello and Microsoft Passport*. Loetud aadressil https://blogs.windows.com/business/2015/04/21/windows-10-security-innovations-at-rsa-device-guard-windows-hello-and-microsoft-passport/#08UAFlPP22RSQPcZ.97

Hoffman, C. (2013). *Why Windows Has More Viruses than Mac and Linux*. Loetud aadressil http://www.howtogeek.com/141944/htg-explains-why-windows-has-the-most-viruses/

How do I Download and Install ESET NOD32 Antivirus 4 for Linux Desktop. (2016). Loetud aadressil http://support.eset.com/kb2653/?locale=en_US

How to configure UFW. (2016). Loetud aadressil https://www.reddit.com/r/linuxmint/comments/4e7wd9/how_to_set_up_a_firewall_ufw/

How to stop automatic freshclam execution. (2016). Loetud aadressil http://askubuntu.com/questions/636851/how-to-stop-automatic-freshclam-execution

I'd like to learn more about PlayOnLinux. (kuupäev puudub). Loetud aadressil https://www.playonlinux.com/en/

Internet Security Threat Report. (2016). Loetud aadressil https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf?aid=elq_&om_sem_kw=elq_16735134&om_ext_cid=biz_email_elq_&elqTrackId=283a3acdb3ff42f4a70ab5a9f236eb71&elqaid=2902&elqat=2

Linux Mint. (2016). Loetud aadressil https://distrowatch.com/table.php?distribution=mint

Linux Security - How Can Your Linux Be Hacked Using Malware, Trojans, Worms, Web Scripts Etc. (2015). Loetud aadressil http://www.linuxandubuntu.com/home/linux-security-how-can-your-linux-be-hacked-using-malware-trojans-worms-web-scripts-etc

Linux Security Review. (2015). Loetud aadressil https://www.av-comparatives.org/wp-content/uploads/2015/05/avc_linux_2015_en.pdf

Linux Signatures. (2015). Loetud aadressil https://www.clamav.net/downloads

Metoodika. (2013). *Vikipeedia*. Loetud 20. oktoober 2016 aadressil https://et.wikipedia.org/wiki/Metoodika

Minimal System Requirements. (kuupäev puudub). Loetud aadressil http://www.bitdefender.com/solutions/antivirus.html

Mis on Windows Hello. (2016). Loetud aadressil https://support.microsoft.com/et-ee/help/17215/windows-10-what-is-hello

Morelli, O. (2016). *Asjaolud, mida kaaluda enne, kui tasud küberkurjategijatele lunaraha.* Loetud aadressil http://viirused.ee/asjaolud-mida-kaaluda-enne-kui-tasud-kuberkurjategijatele-lunaraha/

Murdock, J. (2016). *Apple iOS vs Google Android: Which is the more secure smartphone OS?* Loetud aadressil http://www.ibtimes.co.uk/apple-ios-vs-google-android-which-more-secure-smartphone-os-1547396

Number of Viruses. (2013). Loetud aadressil http://www.cknow.com/cms/vtutor/number-of-viruses.html

Paul, I. (2016). *A beginner's guide to BitLocker, Windows' built-in encryption tool*. Loetud aadressil http://www.pcworld.com/article/2308725/encryption/a-beginners-guide-to-bitlocker-windows-built-in-encryption-tool.html

Questions about Defragging or Antivirus. (2009). Loetud aadressil https://forums.linuxmint.com/viewtopic.php?f=90&t=31723&start=40

Radianti, J., Rich, Eliot., & Gonzalez, J. (2009). *Vulnerability Black Markets: Empirical Evidence and Scenario Simulation.* Loetud aadressil https://www.computer.org/csdl/proceedings/hicss/2009/3450/00/07-02-06.pdf

Security-focused operating systems. (2016). *Wikipedia.* Loetud 28. november aadressil https://en.wikipedia.org/wiki/Security-focused_operating_system

System Requirements for Windows ESET home products. (2016). Loetud aadressil http://support.eset.com/kb358/?viewlocale=en_US

Technical requirements. (kuupäev puudub). Loetud aadressil http://www.pandasecurity.com/homeusers/solutions/free-antivirus/

Testing whether Avast Antivirus protects your computer against malware. (2016). Loetud aadressil https://www.avast.com/faq.php?article=AVKB32

The Best Antivirus Protection of 2016. (2016). Loetud aadressil http://www.pcmag.com/article2/0,2817,2372364,00.asp

The Best Free Antivirus Protection of 2016. (2016). Loetud aadressil http://www.pcmag.com/article2/0,2817,2388652,00.asp

Turkel, D. (2016). *Victims paid more than $24 million to ransomware criminals in 2015 - and that is just the beginning*. Loetud aadressil http://www.businessinsider.com/doj-and-dhs-ransomware-attacks-government-2016-4

Turvaline surfamine. (kuupäev puudub). Loetud aadressil http://abi.rvg.edu.ee/?KKK:Turvaline_surfamine

Ubuntu server - SSH ühendus ja tarkvara repositoorium. (kuupäev puudub). Loetud aadressil http://www.metshein.com/unit/ubuntu-server-ssh-uhendus-ja-tarkvara-repositoorium/

Unable to install Springseed 2 on Ubuntu 15.04. (2015). Loetud aadressil http://askubuntu.com/questions/627420/unable-to-install-springseed-2-on-ubuntu-15-04

Vallaste, H. (2016). *e-teatmik*. Loetud aadressil http://www.vallaste.ee

What are the minimum system requirements for installing and running AVG AntiVirus. (kuupäev puudub). Loetud aadressil https://support.avg.com/SupportArticleView?l=en_US&urlName=AVG-Antivirus-for-Android-download-and-installation

What are the system requirements for Avast 2016. (kuupäev puudub). Loetud aadressil https://www.avast.com/faq.php?article=AVKB44#idt_100

What are the system requirements for Avast Mobile Security. (kuupäev puudub). Loetud aadressil https://www.avast.com/faq.php?article=AVKB66#idt_010

Will Your System Support This Software. (2016). Loetud aadressil http://www.escanav.com/en/linux-antivirus/antivirus-for-linux-desktop.asp#systemsupport

Wine (software). (2016). *Wikipedia.* Loetud 22. oktoober aadressil https://en.wikipedia.org/wiki/Wine_(software)

Wine and Linux Security. (2015). Loetud aadressil http://unix.stackexchange.com/questions/231365/wine-and-linux-security

Lisad

Lisa 1. Viirusetõrjete funktsioonid

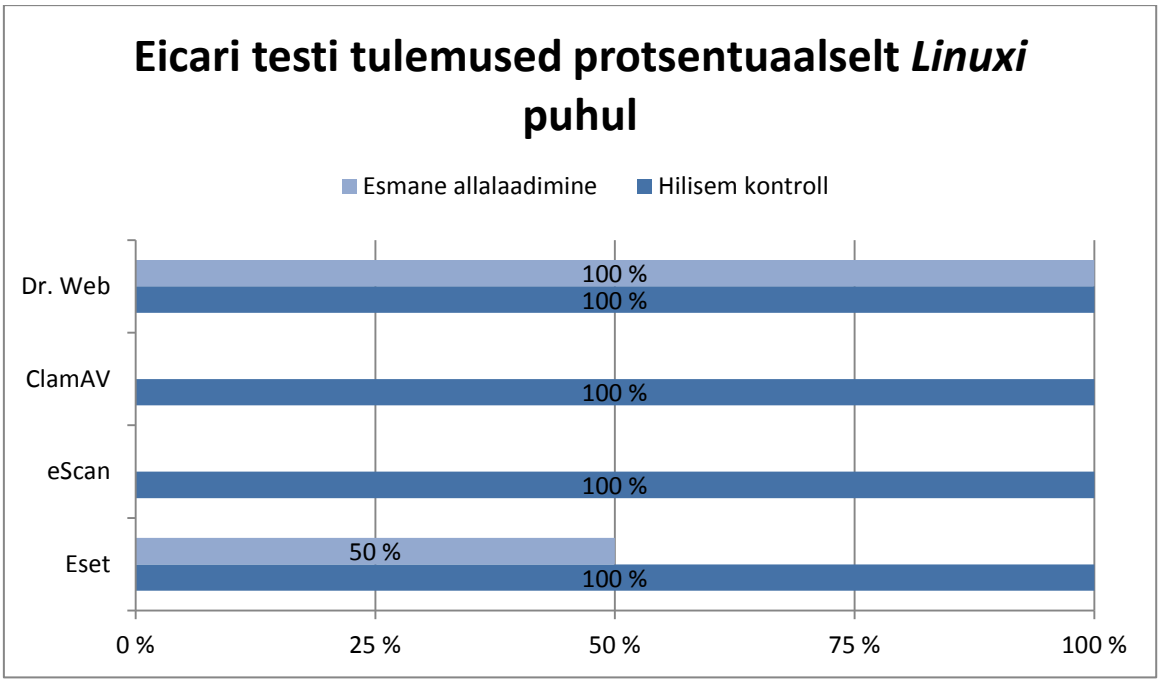
Siinkohal on välja toodud iga testitud operatsioonisüsteemi viirusetõrjete funktsioonide tabelid. Eesmärgiks oli luua punktisüsteem, kus iga funktsiooni parim näitaja saab ühe punkt ning teised nulli. Võrdsete tulemuste korral saavad kõik punkti. Iga lisa annab juurde ühe punkti. Kuna kõike kirjutatut pole võimalik võrrelda, siis lähevad hindamisele ainult need funktsioonid, kus on selgelt parim/parimad välja joonistunud. Selleks lisasin funktsioonidele juurde tärni(*), mis tähistab, et antud funktsioone on võrreldud. Punktiskoore saab vaadata analüüsi all peatükis 5 (Tabelid 1-4) ja kuidas punktid jagunesid (Joonised 27-30). Lisaks eelnevale saab näha antud lisa alt eicari testi tulemusi protsentuaalselt. Kuna eicari test koosnes neljast failist, siis iga fail avastamine või eemaldamine annab vastavalt 25%. Seega kui tuvastati kõik failid on viirusetõrje tabanud 100%. Kui aga näiteks pooled, siis 50%. Koos nimetatud eicari joonistega saab näha ka *Linuxi* ja *Windowsi* viirusetõrjete kontrollitud failide arvu sekundis. Olgu siin ka ära toodud *Windowsi* ja *Linuxi* kontrollitud kausta maht ja failide arv. *Windowsi* puhul oli maht 20.7 GB ja failide arv 119 238. *Linuxi* puhul oli failide arv 290 ja maht 30.2 MB (Joonised 31-36).

Linux Mint 18

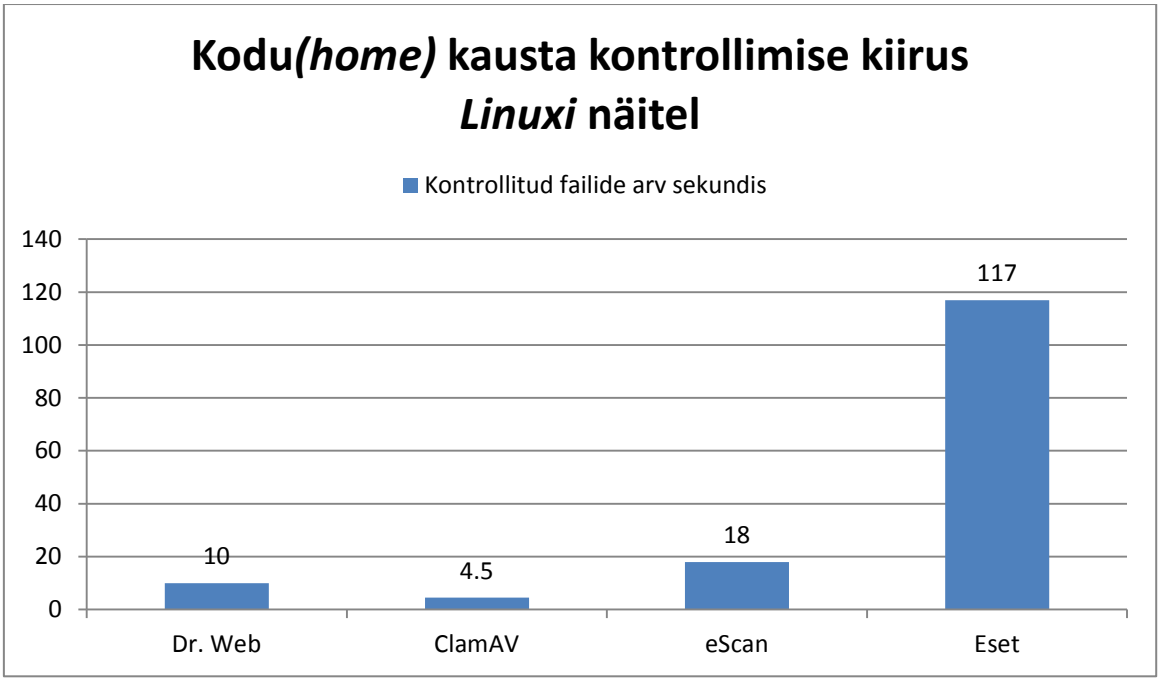
Tabel 5. Linuxi viirusetõrjete funktsioonide võrdlus

Funktsioon/Programm	Dr.Web	ClamAV	eScan	Eset
Toetab millised operatsioonisüsteeme?	GNU/Linux koos kerneli versiooniga 2.6.x või hilisem	Ubuntu, Debian, SuSE, RedHat & Fedora, Fedora & EPEL, Mandriva, Gentoo, Pardus	RHEL 4 ja hilisem(32 & 64 bit), CentOS 5.10 ja hilisem(32 & 64 bit), SLES 10 SP3 ja hilisem(32 & 64 bit), Debian 4.0 ja hilisem(32 & 64 bit), OpenSuSe 10.1 ja hilisem(32 & 64 bit), Fedora 5.0 ja hilisem(32 & 64 bit), Ubuntu 6.06 ja hilisem(32 & 64 bit)	Debian 6.0.7, Fedora 18, Mandriva, Red Hat, SuSE, Ubuntu 12.10 ning kerneli versioon 2.6 või hilisem
Mälu	-	-	1 GB RAM või rohkem	-
Vaba ruumi vajadus kettal?	512 MB	-	1 GB või rohkem	-
Protsessor	-	-	1 GHz või kõrgem	-
Faili allalaadimise asukoht	Viirusetõrje koduleheküljelt	Läbi terminali	Viirusetõrje koduleheküljelt	Viirusetõrje koduleheküljelt

Allalaaditud fail(id)	drweb-11.0.1-av-linux-x86.run	clamav, clamtk, clamav-daemon, clamav-freshclam	escan-antivirus-wks-7.0-18.i386.deb	eset_nod32av_32bit_en_.linux
Paigaldamine	Kasutades terminali või käivitades allalaaditud faili	Kasutades terminali	Kasutades terminali	Käivitasin allalaaditud faili
Sõltuvuste lahendamine*	Automaatne	Automaatne	Ühe sõltvuse pidi manuaalselt paigaldama kasutaja, teistega probleeme ei esinenud	Automaatne
Keelte valik*	9(eesti keelt ei ole)	-	10(eesti keelt ei ole)	20(eesti keelt ei ole)
Käivitamise asukoht	Start menüü - Dr.Web - Dr.Web for Linux	Start menüü - Accessories - ClamTk	Töölaualt või Start menüü - eScan Antivirus - eScan administration	Start menüü - Administration - ESET NOD32 Antivirus
Uuendamine*	Automaatne(vaikimisi iga 30 minuti tagant)	Automaatne(vaikimisi iga tunni tagant, manuaalselt võimalik kasutajal uuendada läbi terminali)	Automaatne(vaikimisi iga tunni tagant kontrollib alates kella 09:30-st)	Automaatne
Kaksikkäivitus	Ei tuvastatud viiruseid	Viirus tuvastati, aga ei suudetud eemaldada	Suudeti leida ja eemaldada mõlemad viirused	Suudeti leida ja eemaldada mõlemad viirused
Protsessorikasutus*	52-60%	53-60%	56-63%	41-60%
Protsessori koormus*	99%	99%	99%	99%
Reaalaja kaitse*	Töötab	Ei tööta	Ei tööta	Töötab
Plaaneeritud kontroll*	Olemas	Olemas	Olemas	Olemas
Kõikide failide kontroll*	Olemas	Olemas	Olemas	Olemas
Kiire failide kontroll*	Olemas	-	-	-
Kindla kausta või faili kontroll*	Olemas	Olemas	Olemas	Olemas
Tasuta või tasuline viirusetõrje?	Tasuline(€26.00 üks aasta üks seade)	Tasuta	Tasuline(€17.60 üks aasta üks seade)	Tasuline(€36.10 üks aasta üks seade)
Lisa(d)*	Link Checker, SpIDer Guard, SpIDer Gate	Faili maine kontroll	Kahtlase faili lähemalt uurimise võimalus	Kahtlase faili lähemalt uurimise võimalus



Joonis 31. Eicari testi tulemused protsentuaalselt operatsioonisüsteemi Linux Mint 18 puhul



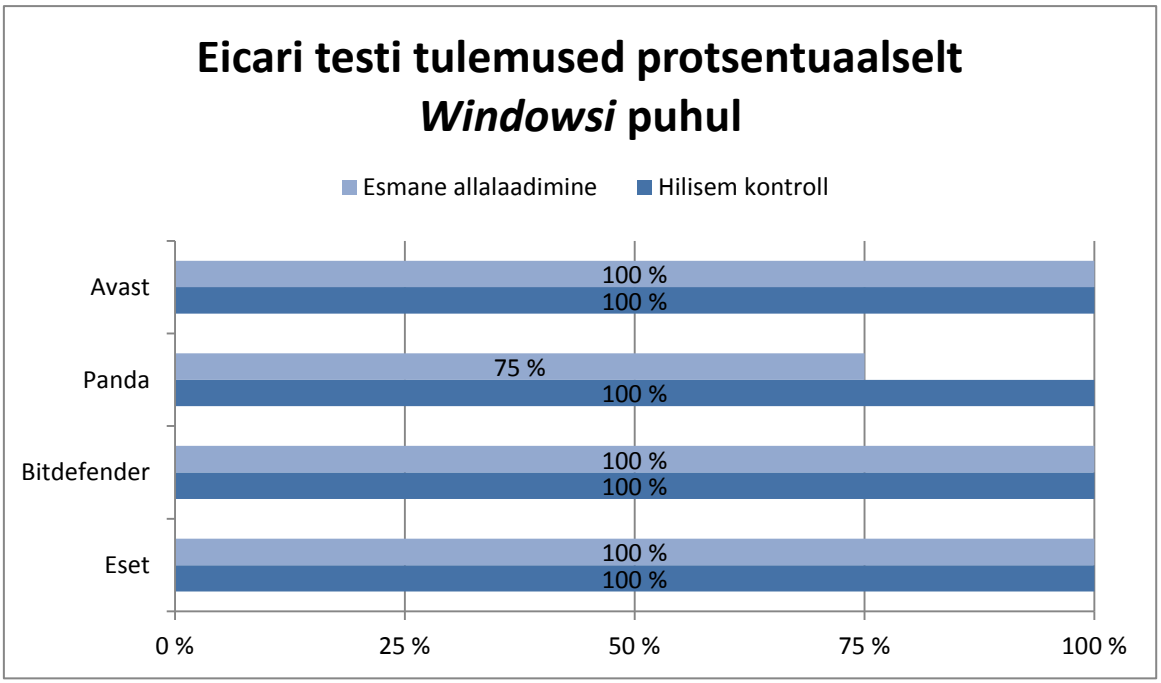
Joonis 32. Kodu(*/home/kasutaja*) kausta kontrollimise kiirus operatsioonisüsteemi Linux Mint 18 puhul

Windows 10

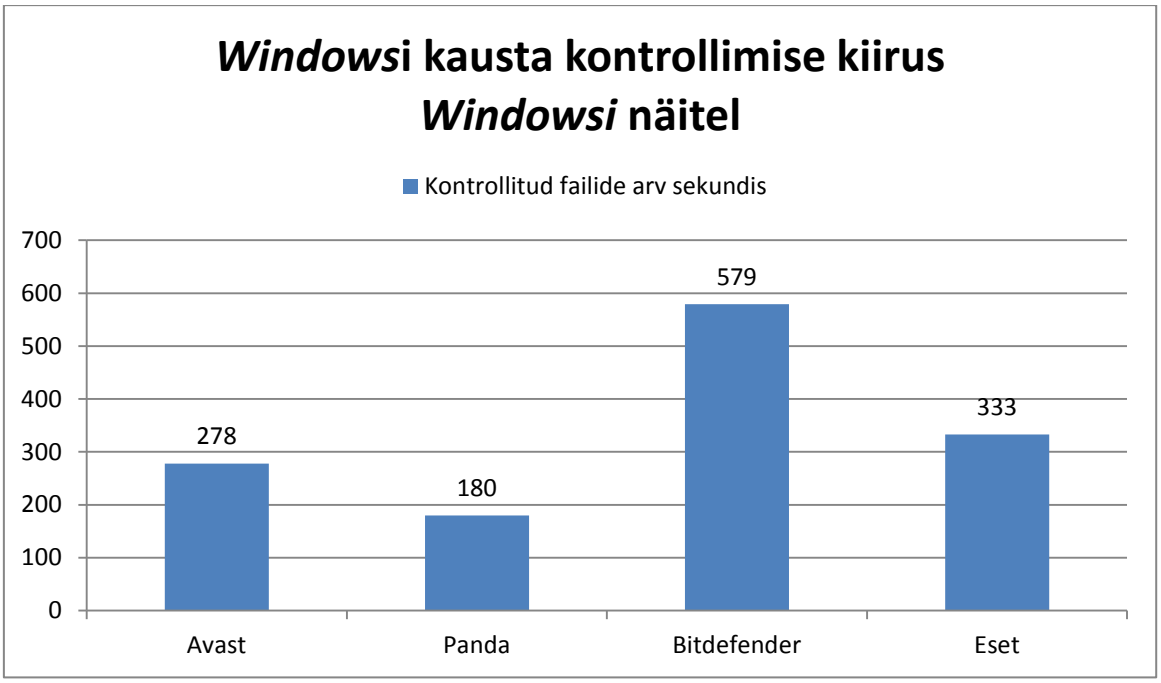
Tabel 6. Windowsi viirusetõrjete funktsioonide võrdlus

Funktsioon/Programm	Avast	Panda	Bitdefender	Eset
Toetab mitut erinevat versiooni?*	6	6	4	5
Mälu*	256 MB RAM	256 MB RAM	1 GB RAM	512 MB RAM(1 GB RAM Vista)
Vaba ruumi vajadus kettal*	2 GB	240 MB	1,5 GB	320 MB
Protsessor	-	300 MHz	1.6 GHz	1 GHz
Veebilehitseja	-	Internet Explorer 6 või uuem, Mozilla Firefox 2 või uuem ja Google Chrome	Internet Explorer 10 või uuem, Mozilla Firefox 30 või uuem ning Google Chrome 34 või uuem	-
Keelte valik*	45 keelt(eesti keel ka)	22 keelt(eesti keelt ei ole)	9(eesti keelt ei ole)	36 keelt(eesti keel ka)
Uuendamine*	Automaatne	Automaatne	Automaatne	Automaatne
Kaksikkäivitus	Ei tuvastatud viiruseid	Ei tuvastatud viiruseid	Ei tuvastatud viiruseid	Ei tuvastatud viiruseid
Protsessorikasutus*	6-16%	43-100%	9-15%	38-56%
Protsessori koormus*	37-54%	85-99%	39-49%	76-99%
Reaalaja kaitse*	Töötab	Töötab	Töötab	Töötab
Tulemüür*	-	-	Olemas	Olemas
Planeeritud kontroll*	Olemas	Olemas	Olemas	Olemas
Kõikide failide kontroll*	Olemas	Olemas	Olemas	-
Kiire failide kontroll*	Olemas	Olemas	Olemas	-
Kindla kausta või faili kontroll*	Olemas	Olemas	Olemas	Olemas
Kasutaja registreerimise vajadus	Kasutaja on vaja registreerida	Kasutajat ei ole vaja registreerida	Kasutaja on vaja registreerida	Kasutaja on vaja registreerida
Lisad*	Smart Scan, Safezone Browser, Rescue Disk, Passwords ning viirusetõrje seadetele saab seada salasõna ja mänguri režiim	Viirusetõrje seadetele salasõna, Safe Web protection, Teadete väljalülitamise režiim, USB Protection, Process Monitor, Rescue Kit, Panda Cloud Cleaner	Erinevad profiilid, Vulnerability scan, Safepay, File Shredder, Rescue Mode, Wi-Fi Security Advisor, Antispam, Wallet, File Encryption, Parentall	ESET Banking & Payment Protection, Password Manager, Secure Data, Home network protection, Removable media scan, Anti-Theft, Parental Control,

			Advisor, Security Widget	Social Media Scanner, faili saata põhjalikku analüüsi, Running processes, failisüsteemi või võrgutegevuse aktiivsuse jälgimine, ESET SysInspector, ESET Sysrescue Live, mängurirežiim ja Webcam protection
Tasuta või tasuline viirusetõrje?	Tasuta	Tasuta	Tasuline(€29.99 1 aasta 1 seade)	Tasuline(€37.74 1 aasta 1 seade)



Joonis 33. Eicari testi tulemused protsentuaalselt operatsioonisüsteemi Windows 10 puhul



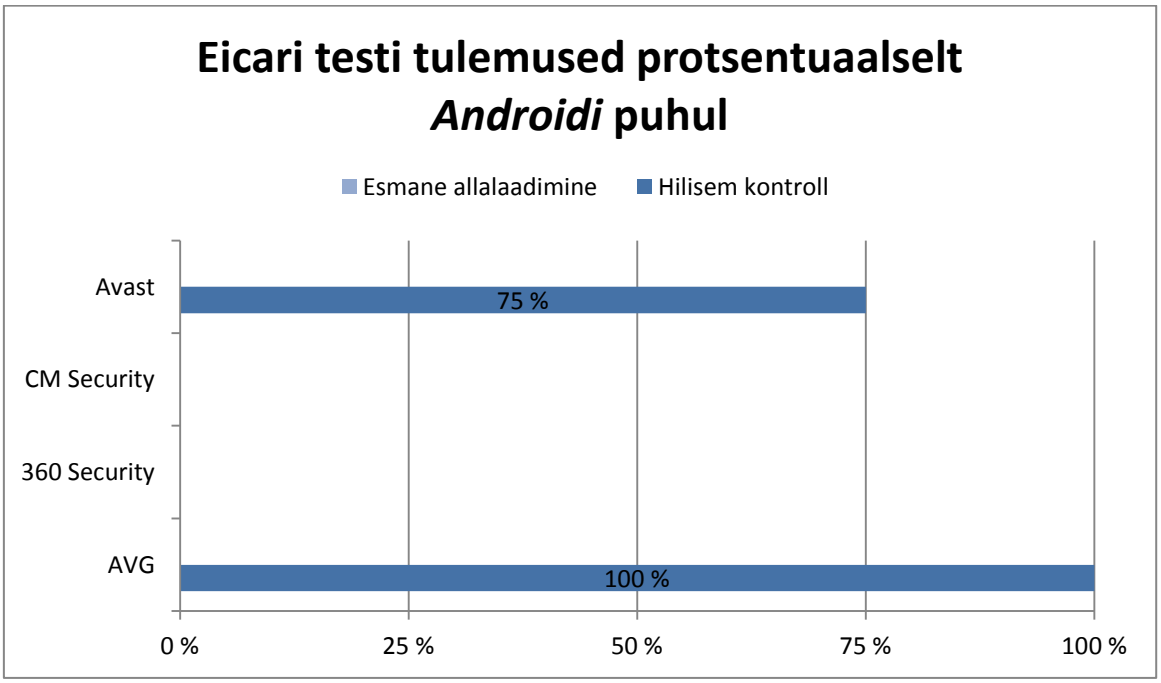
Joonis 34. *Windowsi* kausta kontrollimise kiirus operatsioonisüsteemi MS Windows 10 puhul

Android 6.0.1 Marshmallow

Tabel 7. Androidi viirusetõrjete funktsioonide võrdlus

Funktsioon/Programm	Avast	CM Security	360 Security	AVG
Toetatud Androidi versioonid	Android 4.0.3 või hilisem	-	-	Android 2.2 või hilisem
Kontroll*	Olemas	Olemas	Olemas	Olemas
Nõutav õiguste arv*	6	7	12	14
Kasutaja registreerimise vajadus	Lisa nimega *Anti-Theft* kasutamiseks	Lisa nimega *Find Phone* kasutamiseks	Lisa nimega *Find My Phone* kasutamiseks	Lisa nimega *Anti Theft* kasutamiseks
Planeeritud kontroll*	Olemas	Olemas	-	Olemas
Reaalaja kaitse*	Ei tööta	Ei tööta	Ei tööta	Ei tööta
Keelte valik*	20+	28	34	33
Hinne *Google Play* rakenduses*	4,5/5	4,7/5	4,6/5	4,5/5
Hindajate arv*	4 456 000	20 612 471	14 958 805	5 226 095

Tasuta või tasuline viirusetõrje?	Tasuta	Tasuta(Tasulisele versioonile uuendamiseks tuleb tasuda €0.99 ühe kuu eest(täishind €2.99))	Tasuta	Tasuta(Tasulise versiooni täishind üheks kuuks €2.50 ning aastaks €9.00)
Lisad*	Cleanup & Boost, Battery Saver, Passwords, Wi-Fi Check, App Locker, Call Blocker, Privacy Advisor, Anti-Theft, Wi-Fi Finder, Firewall	AppLock, Safe Browsing, Wi-Fi Security, Battery Saver, Phone Boost, Clean Junk Files, Notification Manager, Caller ID & Blocker, Download Security, Find Phone	Notification Manager, AppLock, Phone Temperature, Game Boost, Space Cleaner, App Manager, Find My Phone, Call & SMS Filter, Data Monitor, Firewall	Anti Theft, Battery Usage, Task Killer, Call Blocker, Secure Search, Data Usage, Storage Usage, Cleaner 2016 - Clean & Boost

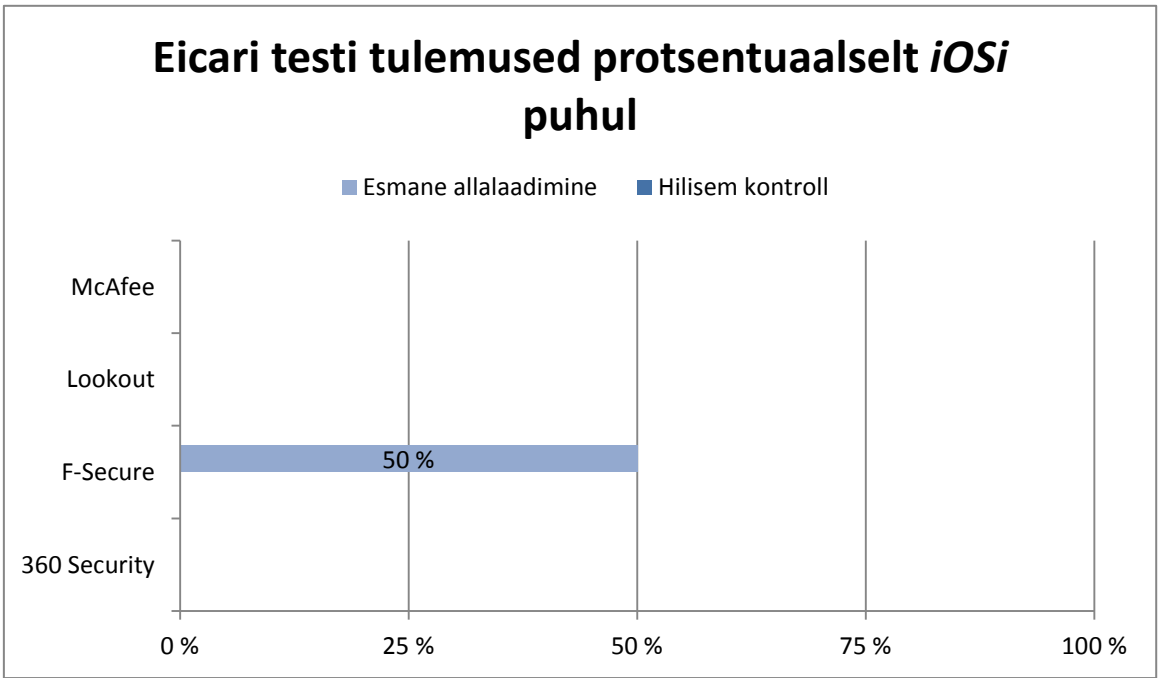


Joonis 35. Eicari testi tulemused protsentuaalselt operatsioonisüsteemi Android 6.0.1 puhul

iOS 10.0.2

Tabel 8. iOS viirusetõrjete funktsioonide võrdlus

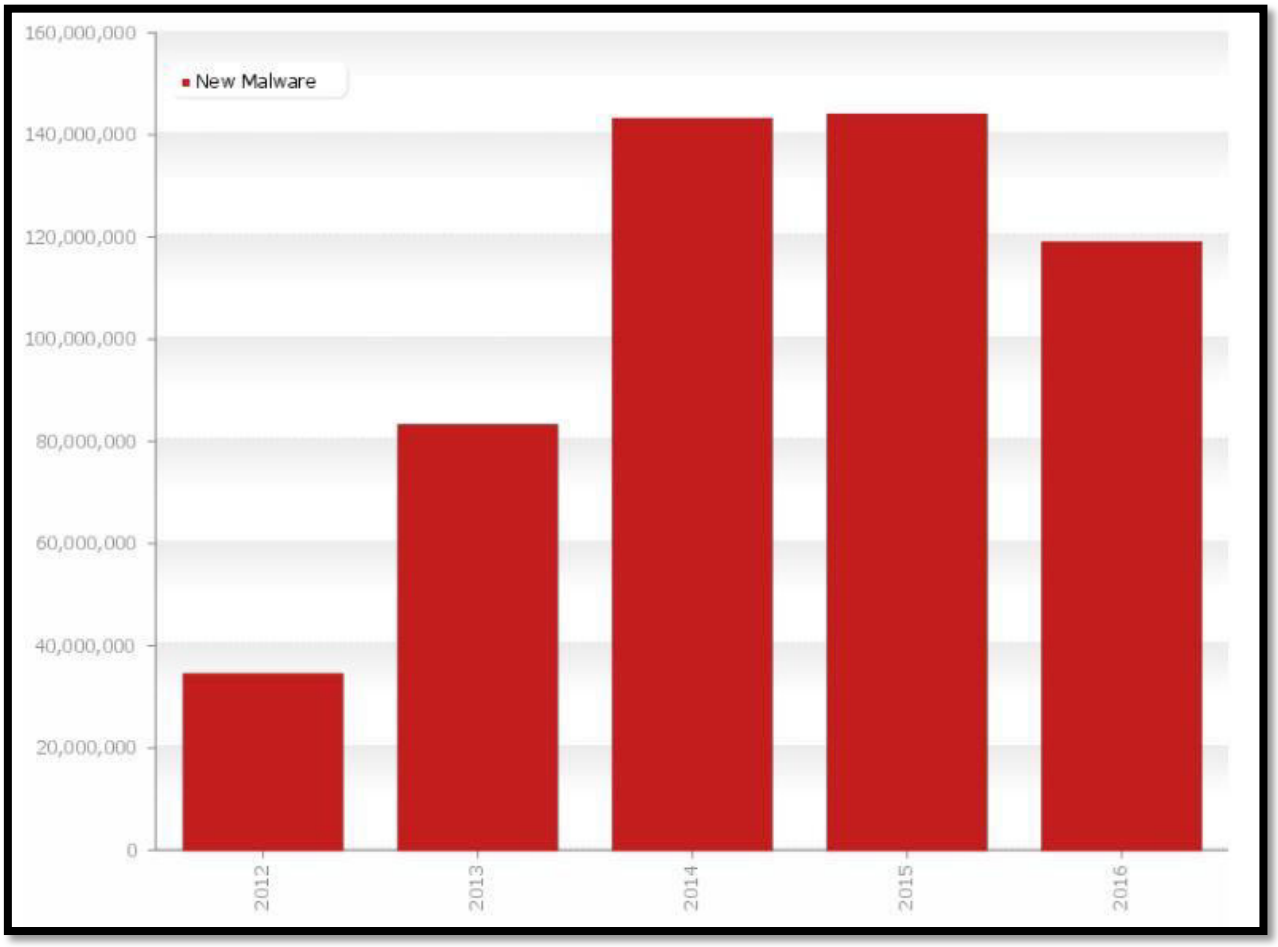
Funktsioon/Programm	McAfee	Lookout	F-Secure	360 Security
Toetatud iOS versioonid	iOS 8.0 või hilisem	iOS 8.0 või hilisem	iOS 8.0 või hilisem	iOS 7.0 või hilisem
Kasutaja loomise vajadus	Vajalik rakenduse *Device Security* kasutamiseks	Vajalik rakenduse *Missing Device* kasutamiseks	Vajalik rakenduse *Finder* kasutamiseks	Kasutajat ei ole vaja registreerida
Keelte valik*	24(eesti keelt ei ole)	8(eesti keelt ei ole)	18(eesti keelt ei ole)	33(eesti keelt ei ole)
Reaalaja kontroll*	Ei tööta	Ei tööta	Läbi viirusetõrje veebilehitseja osaliselt töötab	Ei tööta
Tasuta või tasuline viirusetõrje?	Tasuta	Tasuta, aga rohkemate funktsioonide kasutamiseks on võimalik soetada tasuline kuuks ajaks £2.29 eest	Tasuta saab proovida 30 päeva, aastane litsents maksab €49.90	Tasuta
Lisad*	Apple Watch support, Vault, CaptureCam, Contacts Backup, Device Security	Missing Device, Security, Backup ja Apple Watch support	Safe Browsing, Parental Control, Finder ja My Location	Photo Manager ja Battery Saver



Joonis 36. Eicari testi tulemused protsentuaalselt operatsioonisüsteemi iOS 10.0.2 puhul

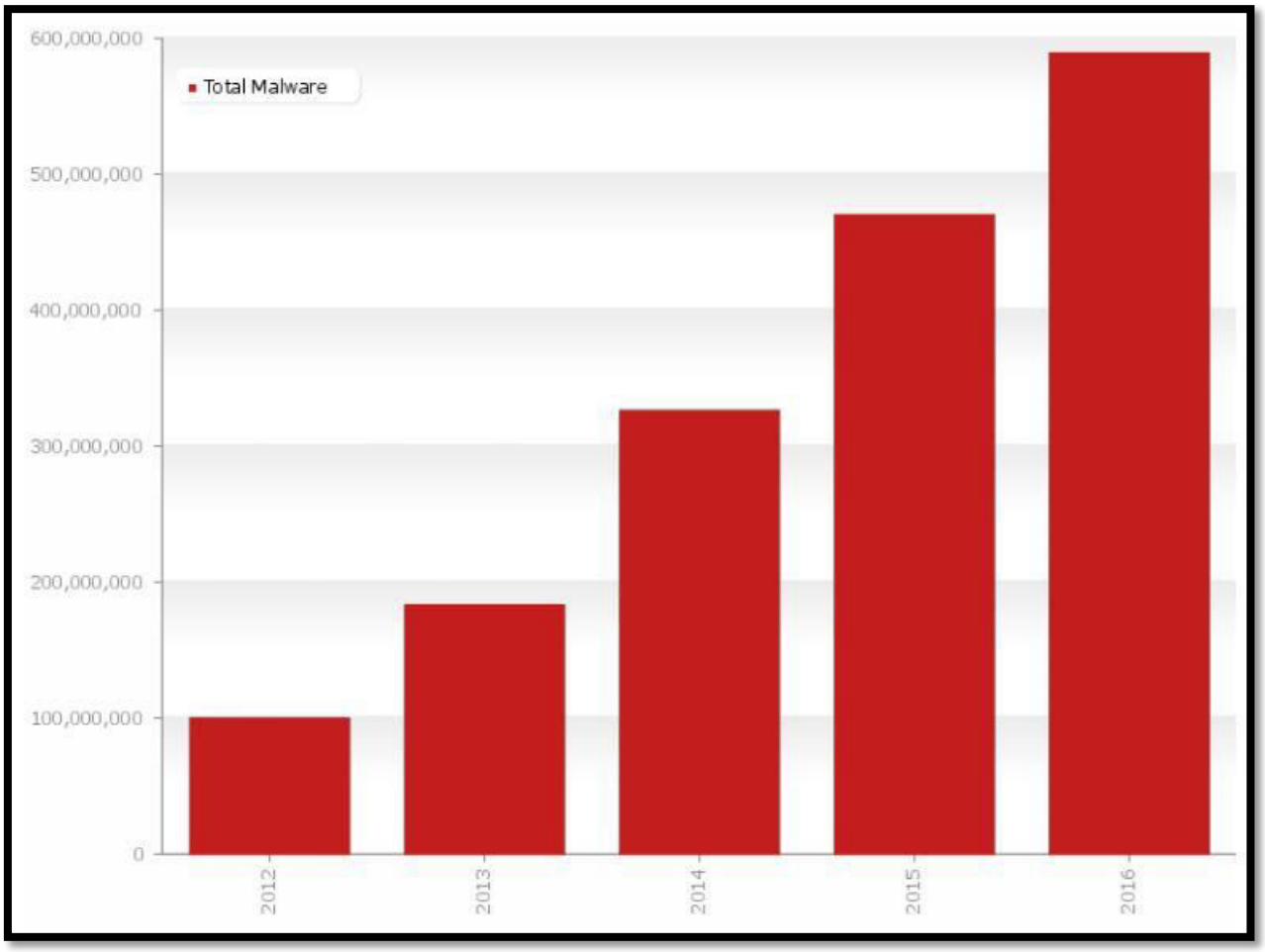
Lisa 2. Pahavara kasv aastate jooksul

Antud lisa sisaldab pilte pahavara statistikast, mis peaks kasutajaid ühe enam motiveerima oma faile ja andmeid kaitsma. Viimase viie aasta lõikes esimest korda on loodud antud aastal uut pahavara vähem kui eelmisel aastal (Joonis 37). Kuigi aasta pole veel lõppenud, jäävad eelmise aasta numbrid selles osas arvatavasti löömata (AV-TEST, 2016).



Joonis 37. Uue pahavara loomine viie aasta lõikes

Kuid kui võtta arvesse kogu pahavara siis eelmise aastaga võrreldes on numbrid kasvanud märkimisväärselt (Joonis 38). Aastast aastasse on olnud stabiilne tõus (AV-TEST, 2016).



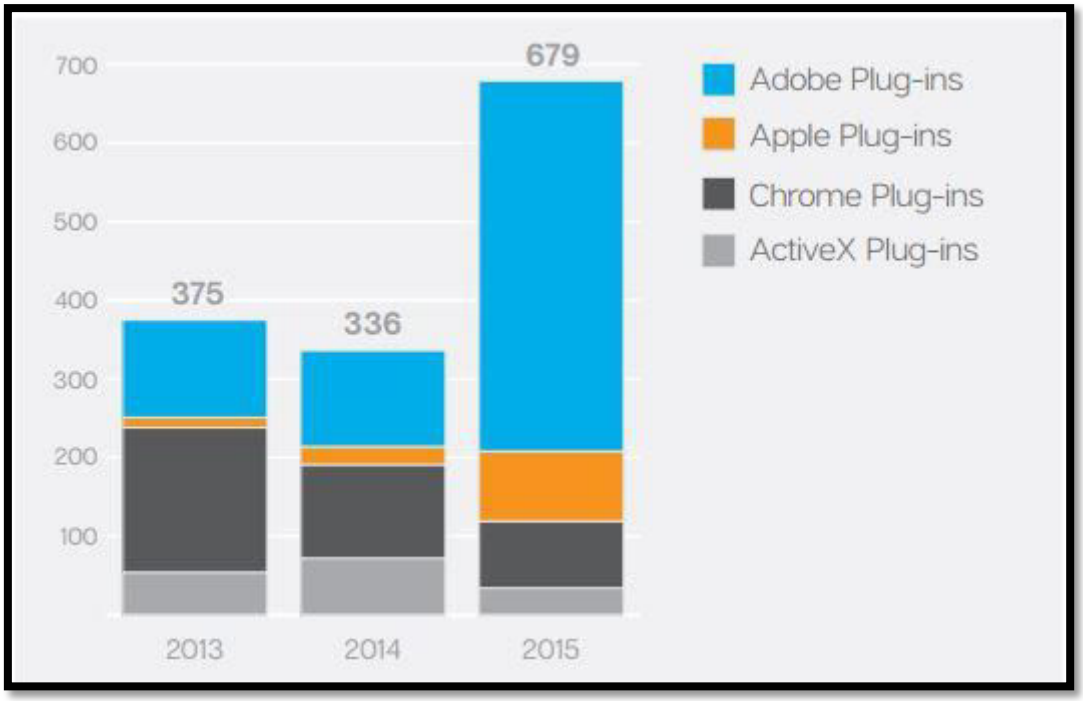
Joonis 38. Kogu pahavara kasv viie aasta jooksul

Seda kõike saab seletada sellega, et järjest rohkem kopeeritakse juba loodud pahavara ja seejärel muudetakse pahavara sisu erinevate levitajate poolt. Selline teguviis otseselt ei tekita juurde uusi viirusi, aga viiruste koguarv kasvab kindlasti. Samuti levib palju sellist pahavara, mis tekitab endast igakord uue versiooni kui käivitub. Seega mida pikemalt on pahavara süsteemis, seda raskem on hiljem pahavara eemaldada (Number of Viruses, 2013).

Eraldi soovin välja tuua pahavara, milleks on lunavara. Esiteks tooksin välja Ameerika Ühendriikide 2015 aasta näite, mille 2500 juhtumi puhul üle 24 miljoni dollari (üle 22,5 miljoni euro) lunaraha maksti (Turkel, 2016). Sellega seoses saadetakse tänavu järjest rohkem spämmkirju (ADalma, 2016). Mis teeb spämmkirjad eriti ohtlikuks on nende seos lunavaraga. Nimelt enamus kirju sisaldab lunavara, mis krüpteerib arvuti failid ja seejärel nõuab teatud rahasummat nende vabastamiseks (BDalma, 2016). Kuna tegu on äärmiselt ebameeldiva pahavaraga, siis leviku peatamiseks saab kasutaja palju ise ära teha. Esmalt tuleks kasutajal lunaraha maksmisest keelduda ja otsida teisi võimalusi olukorra lahendamiseks. Näiteks kui kasutaja on korrapäraselt faile varundanud, siis on odavam võtta kasutusele varundatud failid.

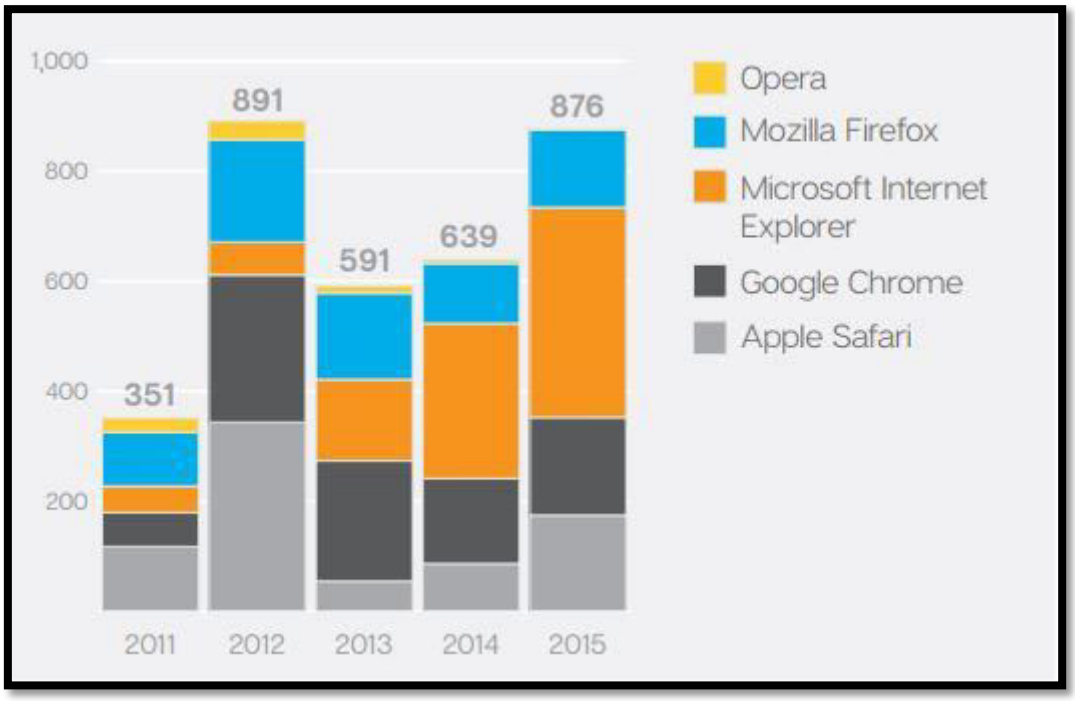
Samuti on võimalus kasutada otsimootorite abi, et leida tasuta dekrüpteerija või küsida spetsialisti käest arvamust antud olukorrale. Kuna nõutud raha maksmine ei garanteeri andmete tagasisaamist, siis tuleks kasutajal otsustada, kas odavam on tasuda lunaraha või kaotada failid. Võimalik on ka olukord, kus kasutaja tasub lunaraha. Talle saadetakse krüpteerija, mis küll krüpteerib failid lahti uuesti, aga võib sisaldada uut pahavara. Kuna kasutaja on tasunud juba korra lunaraha, siis ilmselt teeks ta seda uuesti järgmisel korral (Morelli, 2016).

Veel soovin ära mainida lisad, mille kaudu enim kasutajad rünnatakse (Joonis 39). Nagu näha on viimasel aastal teinud selge kasvu *Adobe*, mille puhul enim probleeme valmistab kasutajatele just *Adobe Flash Player* ehk *Shockwave Flash* (Internet Security Threat Report, 2016).



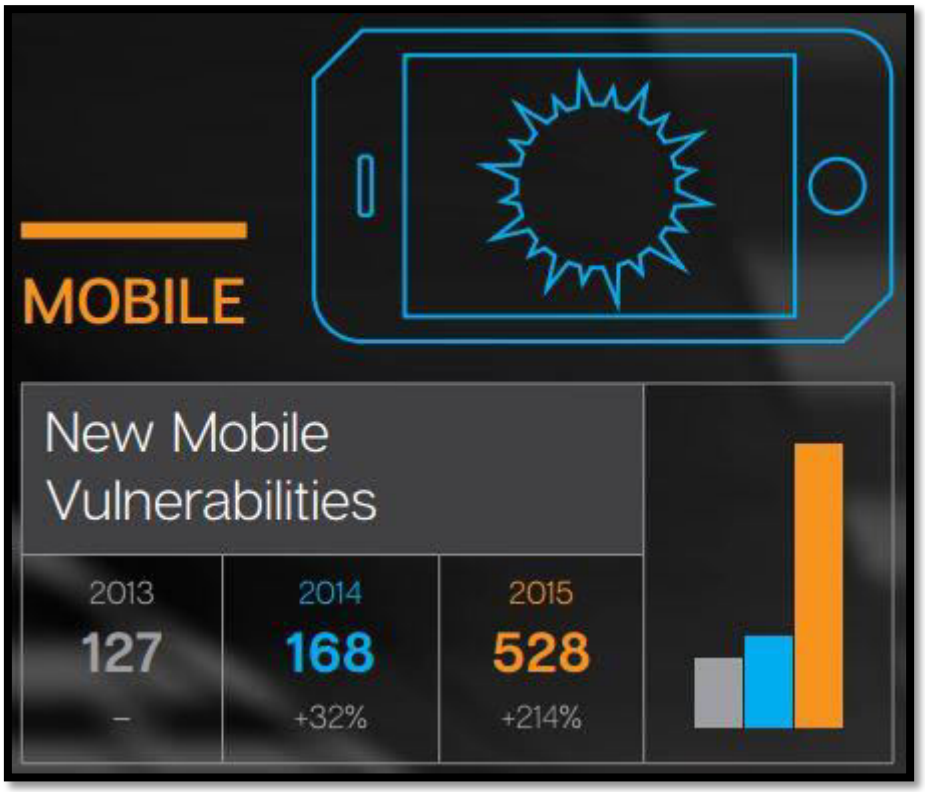
Joonis 39. Lisade haavatavused

Veebibrauseritest on haavatavaim *Microsoft Internet Explorer* (Joonis 40). See ei ole mingi üllatus kuna iga *Windowsi* operatsioonisüsteem sisaldab ühte versiooni *Explorerist*, mida kasutaja ei pruugi kunagi kasutada, aga ometi on ta olemas (Internet Security Threat Report, 2016).



Joonis 40. Veebilehitsejate haavatavus

Et näidata kui tähtis on oma andmeid kaitsta ka telefonis viirusetõrje abil, toon välja mõned näitajaid, mis väärivad tähelepanu. Märkimisevääselt on kasvanud telefonide haavatavuste arv (Joonis 41). Üheks asjaoluks on kindlasti telefonide kasv aastast aastasse (Internet Security Threat Report, 2016).



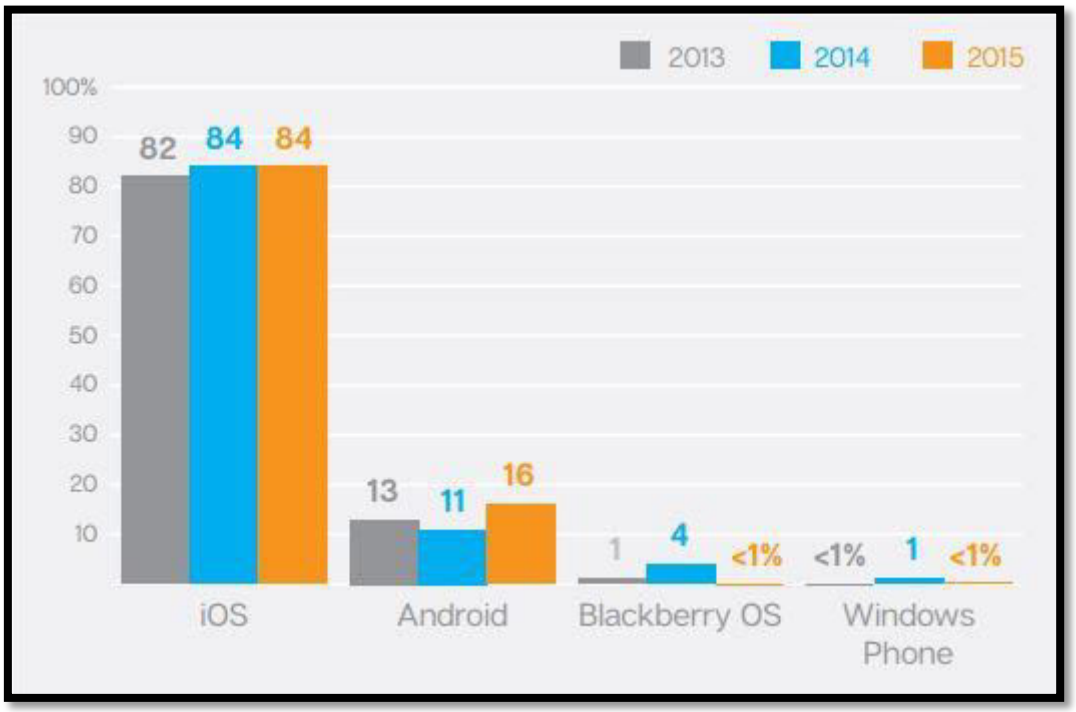
Joonis 41. Telefonide haavatavuste arvu kasv

Järsu tõusu on ka teinud telefonide puhul *Zero-day Vulnerabilities*, mis kujutavad endast tarkvara auku, mille kaudu saab kurjategija siseneda seadmesse (Joonis 42). Tegu on auguga, millest tootja veel ei pruugi teadlik olla. Seetõttu on selliste rünnakute ennetamiseks vajalik omada uusimat tarkvara versiooni oma telefonis (Internet Security Threat Report, 2016).

Joonis 42. *Zero-day Vulnerabilities*

Telefonide operatsioonisüsteemidest on kõige haavatavam *iOSi* kasutavad seadmeid, kuigi *Android* on teinud suurima tõusu viimasel aastal (Joonis 43). *iOSi* haavatavuse kõrge tase on tingitud suurest arvust seadmetest, mis on nii öelda lahti murtud ehk avatud (*jail-break*). Lahti murtud telefonis saavutatakse juurdepääs suuremale kogusele tarkvarale, aga eemaldades kõik

piirangud tootja poolt. Sinna hulka ka kõik selle, mis varem kaitsest telefonis olevaid faile. Seega muutes antud telefoni väga haavatavaks (Internet Security Threat Report, 2016).



Joonis 43. Telefonide operatsioonisüsteemide haavatavused

Samuti on suureks ohumärgiks see, et turvaaukudega kaubeldakse mustal turul enne kui avalikkus teada saab (Radianti, Rich & Gonzalez, 2009).

Lisa 3. Soovitused kasutajale

Käesoleva bakalaureusetöö soovitused on defineeritud autori seminaritöös (Dreifeldt, 2015):

1. Paigaldage arvutisse/telefoni viirusetõrjetarkvara, kasutage ja uuendage seda!

Viirusetõrjesüsteem on teie esimene ja kõige võimekam abimees sissetungijatega võitlemiseks.

2. Kasutage tulemüüri!

Tulemüür on piltlikult öeldes valvur, mis otsustab, millistel rakendustel on õigus teie arvutisse või telefoni siseneda ja millistel mitte.

3. Laadige regulaarselt alla operatsioonisüsteemi ja rakendusprogrammide uuendusi ja täiendusi ning võimalusel automatiseerige see!

Iga tarkvaratootja üritab reeglina seista hea selle eest, et tema toodang oleks kvaliteetne ja töötaks korralikult ning parandada avastatud turvaaugud nii kiiresti kui võimalik. Parandused ja täiendused võib tavaliselt alla laadida tootja kodulehelt ning seda on soovitav teha võimalikult kiiresti, sest kiirus kahandab oluliselt võimalust, et keegi juba avastatud turvaauke teie vastu ära ei kasuta. Kindlasti võimalusel kontrollida tähtsamad programmid üle, kuna enamus operatsioonisüsteeme uuendab programme eraldi ja nii võis mõni tähtis jupike uuendamata jääda.

4. Suhtuge kahtlustavalt e-kirjalisadesse. Ärge kunagi avage tundmatult saatjalt tulnud faile, sõprade saadetud failid aga kontrollige kindlasti viirusetõrjega üle!

Paljud viirused ja muud pahalased maskeerivad end pealtnäha ohututeks tekstidokumentideks või piltideks, veebilink aga võib teid suunata lehekülgedele, kust teie arvutisse või telefoni laaditakse mitmesugust pahavara või kui teie eesti keelt kõnelev sõber hakkab teile ühtäkki võõrkeelseid kirju või kiirsuhtlussõnumeid saatma, paluge tal kontrollida, ega ta arvuti või telefon äkki nakatunud pole.

5. Suhtuge ettevaatusega kõigesse, mida internetist alla laete, kui vähegi võimalik, üritage kontrollida selle päritolu!

Pahatihti laetakse koos tarkvaraga alla ka lisatarkvara, mille olemasolust teile ei teatata ning mis asub teie arvutis või telefonis omatahtsi tegutsema. Samuti ärge võtke tõsiselt ettepanekuid laadida näiteks alla spetsiaalne videovaatamiseprogramm, et ühe konkreetse saidi sisule paremini ligi pääseda, ning kontrollige kõik allalaetavad failid enne käivitamist viirusetõrjega igaks juhuks üle.

6. Tehke varukoopiaid ning hoidke neid arvutist/telefonist eraldi!

Arvutis olevad andmeid võivad kahjustada saada paljude erinevate ohtude tagajärjel. Sama kehtib ka telefonide kohta. Mitte ainult rünnak või viirus, vaid ka tugev voolukõikumine või telefoniliini sisse löönud pikne võivad hävitada kõik teie failid. Kuid kahju pole nii suur kui teete oma andmetest regulaarselt varukoopiaid, nii võite pärast süsteemi taastamist jätkata oma tegemisi samast seisust, mil te viimase varukoopia tegite. Varukoopiaid tuleks mõistagi hoida mitte arvutis endas, vaid soovitavalt eraldi andmekandjal, näiteks plaadil või välisel kõvakettal. Soovitav oleks neid hoida teises ruumis või koguni teises hoones. Veelgi parem oleks omada mitut varukoopiat, mis asuksid üksteisest eraldi.

7. Kasutage tugevaid salasõnu ja ärge jagage kergekäeliselt oma isiku-, kontakt- ega juurdepääsuõigusi!

Salasõnad on mõeldud selleks, et teatud ressurssidele või rakendustele ei saaks ligi need, kellel selleks õigusi pole. Olge üsna kindlad, et sissetungija proovib esimeses järjekorras teie nime, sünnikuupäeva, auto numbrit või märgikombinatsiooni "admin123". Kui kasutate salasõna asemel salafraasi, mille pikkus on 64 ja rohkem sümbolit siis võite ennast tunda juba turvaliselt. Keerukust (suurtäht, number, erisümbol) võib mõningal määral lisada ent see ei ole primaarne. Salafraasi murdmiseks kuluvat aega tasub regulaarselt kontrollida näiteks aadressil https://howsecureismypassword.net/ - tehnika ja tehnoloogia arendes need ajad lühenevad. Selle tulemusena võib salafraasi murdmiseks kuluv aeg olla piisavalt kriitiline, et panna sissetungija oma ettevõtmisest loobuma. Salasõnad, PIN-koodid ja muud ligipääsuandmed on mõeldud selleks, et neid kasutaksite ainult teie, seega ei tohi neid mistahes ettekäändel mitte kellelegi edasi anda, isegi kui neid küsib hea sõber, IT-töötaja või pank. Võimalusel kasutada

mitmeastmelist isikutuvastust - http://2fa.com/ ja näiteks riistvaralist võtit - https://en.wikipedia.org/wiki/Universal_2nd_Factor.

8. Logige end administraatorina sisse ainult siis, kui see on hädavajalik ning seadke vähemalt 16 tähemärgi pikkune salasõna antud kontole - igapäevatöö tegemiseks logige sisse piiratud õigustega kasutajana, kus samuti soovitaks salasõna kasutada. Sedaviisi suudab arvutisse sisseroninud pahalane hoopis väiksemat kahju tekitada. Telefoni puhul vaadake, millisele rakendusele te annate administraatori õigused.

Administraatoril on piiramatu juurdepääs kõigile süsteemi ressurssidele ning õigus paigaldada mistahes programme ja programmilisasid. Pahalane, kelle te adminstraatorina alla tõmbasite, võib saada teie arvutis samad õigused ning teha hoopis rohkem kurja. Mõni pahalane ei suudagi end ilma piisavate õigusteta teie arvutisse sisse seada. Looge endale ja kõigile teistele arvuti kasutajatele piiratud õigustega konto. Administraatorina logige end sisse ainult siis kui teil on vaja paigaldada uusi programme, muuta olemasolevate programmide seadeid või teha vajalikke süsteemitoiminguid. Võimalusel kasutage turvalisemat sisselogimist, näiteks ID-kaardiga või riistvaralise võtmega, näiteks Everykey - https://everykey.com/. Hoidke salasõnu turvaliselt. Üheks võimaluseks on siinkohal toode Mooltipass - https://www.themooltipass.com.

9. Olge ettevaatlik mälupulkade ja teiste andmekandjatega, kontrollige neis sisalduvat kindlasti pärast seda, kui olete neid võõras arvutis/telefonis kasutanud.

Peale andmekandja kasutamist võõras arvutis või telefonis on oht, et sinna peale võis sattuda mõni pahalane, kes hiljem nakatab kõiki arvuteid, kus andmekandjat kasutatakse, seepärast on mõistlik ta läbi kontrollida. Isegi kui tegu on sõbra arvutiga või telefoniga, võib temagi seadmes olla pahalane, kelle olemasolust keegi varem ei teadnud. Juhuslikult leitud mälupulka vaadatakse eraldi arvutis kus ei ole missioonikriitilisi andmeid. USB Dead Drops ei ole hea idee! Lisainfo https://deaddrops.com/.

10. Seal, kus võimalik, kasutage ID-kaarti või ka mobiili ID-ed. Ärge ID-kaarti pärast kasutamist lugejasse unustage!

ID-kaart on üks lihtsamaid ja turvalisemaid võimalusi kaitsta näiteks oma pangakontot kuritarvitamise või dokumentide võltsimise eest.

11. Veebilehitsejas toimetades kasutage privaatset režiimi!

See tähendab seda, et siis ei jäeta tundlikku infot meelde lehitseja poolt - külastatud aadresside ajalugu, sessioonide küpsised, sisestatud vormide infot ning salasõnu. Vaikimisi jätavad kõik veebilehitsejad sellise tundliku info meelde kui neid ei ole teisiti seadistatud. Privaatse režiimi saab kiirelt sisse lülitada: Internet Explorer ja Mozilla Firefox - CTRL+SHIFT+P, Google Chrome ja Opera - CTRL+SHIFT+N. Safari puhul tuleb see käsitsi valida rippmenüüst(*Private browsing*).

12. Kui te ei saa aru või pole kindel, mida arvuti/telefon teie käest tahab, siis lugege veelkord, kui vaja, tõlkige teade, küsige mõnelt tuttavalt asjatundjalt üle või kasutage interneti otsimootoreid!

Paljud tarkvaratootjad ei lisa kahjuks oma operatsioonisüsteemide või rakendusprogrammide keelevalikusse eesti keelt. Seda enam pole põhjust klõpsida avanenud dialoogiboksides nuppe "*Yes*" ja "*Next*" ning loota parimat. Üritage välja selgitada, mida seade teie käest tahab ning kas see, mida ta tahab, on ikka mõistlik.

Grupipoliitika rakendamine aitaks samuti kaasa arvuti kaitsmisele pahavara eest. Kui näiteks ära keelata *MS Windowsi* registri ja käsurea kasutamine koos Juhtpaneeliga. Sel juhul on palju asju juba kinni pandud ja pahavara ei saa ligi. Kahjuks ei ole selline asi võimalik aga ei *MS Windows Basic* ega *Home* versioonidel - seetõttu tuleks valida vähemalt Pro versioon.

Kasutage oma tervet mõistust - ärge registreerige kahtlastesse keskkondadesse; ärge osalege kui tahes ahvatlevates loosimistes; ärge saatke edasi kettkirju; ärge klõpsake kõike, mida teile näidatakse ning ärge jagage oma andmeid kõigile, kes neid küsivad! Samuti ärge logige sisse igale poole, samal ajal olles avalikus võrgus, sest tuletame meelde, et andmed on kõikidele nähtavad sellistes võrkudes. Samuti ei kehti arusaam, et mida rohkem erinevaid viirusetõrjeid,

seda turvalisem arvuti on, sest viirusetõrjed hakkavad üksteist segama ja nende töö kvaliteet langeb koos sellega.

13. Nutiseadmes tuleks internetiühendus (sh Bluetooth) välja lülitada kui seda reaalselt ei kasutata.

See võiks olla reegel ehk siis tavapärane olek, et internet on nutiseadmes väljas ja vaid vajadusel ühendutakse internetti. Internetiühendust võiks välja lülitada ka arvutites kui seda ei kasuta. FBI soovitab ka arvuti välja lülitada kui seda ei kasutata - https://www.fbi.gov/scams-and-safety/on-the-internet kuid piisab ka interneti väljalülitamisest kui on ette näha, et arvutit mõne aja pärast taas kasutatakse. Kui aga võrguühenduste haldamine liialt keerukas on siis on lihtsam seade lihtsalt välja lülitada nagu FBI soovitab. Lennnujaamas ja muudes rahvarohketes kohtades ei ole soovitav kohe nutiseadet sisse lülitada kui see väljas oli. Sisselülitamisel hõigatakse eetrisse ka riistvara MAC-aadress ja küberkurikaelad kes tavaliselt rahvarohketes kohtades eetrit uurivad, saavad selle kätte. Kui nutiseade käima on läinud siis ta loeb oma seadetest, et peab olema varjatud ja siis peidab oma nime Bluetooth võrgus, et teised seadmed ei näeks. Kuid küberkurikael on MAC-aadressi kätte saanud ja selle alusel saab seadet juba rünnata. Siis ei tohiks näiteks sissetulevatele päringutele vastata ja need tuleks katkestada. Kuid leidub ka seadmeid, mis ei küsi nõusolekut ja võtavad vaikimisi Bluetooth ühenduse kaudu tulevad päringud vastu. Võimalusel tuleks testida seda oma seadme puhul ja kui ei ole võimalik seadistada esmalt nõusolekut küsima siis tasub uurida kas tarkvarauuendus parandab olukorda. Kui mitte siis on soovitav seade välja vahetada.

14. Kasutage nuhkimise minimeerimiseks turvalisemaid otsimootoreid, näiteks:

https://www.startpage.com/

https://duckduckgo.com/

https://www.ixquick.com/

http://www.hongkiat.com/blog/private-search-engines/

15. Võimalusel kasutada avalikes võrkudes olles krüpteeritud ühendust.

Näiteks avalikes WiFi võrkudes ja ka mobiilse interneti puhul lisaks VPN-ühendust, mida on võimalik enamus ruuterites tööle sättida. Kaughalduse jaoks kasutada võimalusel krüpteeritud ühendust, näiteks FTP asemel OpenSSH jne. RSA puhul kasutada vähemalt 4096-bit võtmeid või isegi enam (hetkel kuni 16384-bit, tulevikus ehk ka rohkem). Kasutada ka uue põlvkonna krüptograafiat, näiteks RSA asemel elliptilisi algoritme, nt Ed25519 koos kõrge KDF-väärtusega (a=miljon või enam). KDF - https://en.wikipedia.org/wiki/Key_derivation_function ja parameetri a kohta https://linux.die.net/man/1/ssh-keygen.

16. Jälgige regulaarselt turvalisuse maailmas toimuvat.

Turvalisus ei ole seisund vaid protsess, mille eest peab pidevalt hea seisma. Näiteks on välja tulnud kvantarvutid, mis muudavad oluliselt olukorda ka turvalisuse vallas. Seni turvalisena toiminud salasõnad ja krüptograafia võivad olla loetud minutitega murtavad kvantarvutite poolt. Oma salasõna turvalisust tasub regulaarselt kontrollida, näiteks aadressil https://howsecureismypassword.net/. Uus ajastu nõuab uut lähenemist: kvantkrüptograafia - see tuleb varem või hiljem ka rakendada. Väike paranoia on turvalisuse maailmas alati kasulik ja tuleb mõelda 2-3 sammu ette võimalike küberkurikaelte sammudest, kasutades näiteks missioonikriitilistes kohtades maksimaalset krüptot jm turvalisust tõstvaid lahendusi. Ei tasu jääda lootma ühele sammule vaid kasutada tuleb kõiki turvalisuse lahendusi koos. Kui üks lahendus murtakse siis kaitsevad teised.

17. Võimalusel kasutage turvalisemat operatsioonisüsteemi.

Näiteks GNU/Linuxit (nt Ubuntu või selle turvaline sugulane Tails) või mõnda analoogset turvalisemat operatsioonisüsteemi (https://en.wikipedia.org/wiki/Security-focused_operating_system). Linuxile on omane iga tarkvarapaketi ehtsuse kontroll enne allalaadimist, mis väldib muuhulgas ka APT-tüüpi pahavara leviku - http://www.arvutikaitse.ee/apt-jouliselt-ebamaarane-kuber-oht/. Mitte segi ajada Debiani-põhiste Linuxite turvalise paketihaldussüsteemiga APT - https://wiki.debian.org/Apt. Kui on vaja MS Windows'i kasutada siis seda saab teha virtuaalarvutis, näiteks VirtualBox'i abil - https://www.virtualbox.org/. Näiteks Microsoft pakub valmiskujul legaalselt tasuta prooviversioone virtuaalarvuti kujul - https://developer.microsoft.com/en-us/microsoft-

edge/tools/vms/. Lisaks pakutakse tänapäeval ka mitmeid MS Windowsi rakendusi veebipõhiselt kasutada. Nii ei ole oluline, mis operatsioonisüsteem arvutis on. Võimalusel tuleks suletud lähtekoodiga omandusliku tarkvara puhul kasutada veebipõhiseid lahendusi. Näiteks MS Office'i saab asendada tasuta MS OneDrive'iga või selle tasulise versiooni MS Office 365'ga. Samas on olemas alternatiivina ka vabatarkvaraline Open365 - https://github.com/Open365/Open365.

18. Kasutage avatud lähtekoodiga tarkvara ja avatud standardeid ning vältige tootjalukustust.

Avatus tagab võimaluse veenduda tarkvara turvalisuses. Vabatarkvara on üks hea näide turvalisest valikust ja aitab vältida tootjalukustust (*vendor lock-in*).

Tootjalukustuse artiklid:

https://en.wikipedia.org/wiki/Vendor_lock-in

https://viki.pingviin.org/Tootjalukustus

Vabatarkvara kasutamise kasulikkusest on näiteks aru saanud USA valitsus, sh kaitsejõud:

https://sourcecode.cio.gov/ - White House Government-wide Open-Source Software policy

https://code.gov/ - USA valitsuse avatud lähtekoodi varamu, mida peetakse üheks innovatsiooni läbimurdeks.

https://www.whitehouse.gov/blog/2016/03/09/leveraging-american-ingenuity-through-reusable-and-open-source-software - Valge Maja vabatarkvara poliitika

https://pages.18f.gov/open-source-program/ - vabatarkvara kasutamine USA valitsuses

http://dodcio.defense.gov/Portals/0/Documents/FOSS/2009OSS.pdf - aastast 2009 USA valitsuse vabatarkvara memorandum

http://mil-oss.org/ - USA kaitsejõududes vabatarkvara kasutamise grupp, kõik huvilised võivad liituda. Pealkirja "*Resources*" all on mitmeid artikleid jm materjale.

Mõned märksõnad kvantarvutite teemadel

timeline of quantum computing

cateogry: quantum information science

Quantum asymmetry between time and space

Scientists May Have Just Figured Out Why Time Moves Forward, Not Backwards

Bringing time and space together for universal symmetry

Quantum Theory Proves That Time Does Not Exist

Google's Quantum Computer

Scientists Create a 5-atom Quantum Computer That Could Make Today’s Encryption Obsolete

Quantum leap: D-Wave's next quantum computing chip offers a 1,000x speed-up

Scientists have developed a device that can guarantee producing an endless sequence of entangled photons.

First Quantum Photonic Circuit with an Electrically Driven Light Source

Hacking, Cryptography, and the Countdown to Quantum Computing

Quantum computing advances with researchers' control of entanglement

This video game shows why humans are better at quantum physics than supercomputers

New evidence could break the standard view of quantum mechanics

Quantum computers: 10-fold boost in stability achieved

Wits researchers find techniques to improve carbon superlattices for quantum electronic devices

New 3-D wiring technique brings scalable quantum computers closer to reality

Precise quantum cloning: possible pathway to secure communication

A new class of materials could realize quantum computers

Fujitsu eyes architecture to rival quantum computers

Quantum computers can talk to each other via a photon translator

Quantum computers: The world’s first buyers’ guide

Basic quantum computation achieved with silicon for first time

Diamond shows promise for a quantum Internet

Single photon converter – a key component of quantum internet

How can quantum information be stored as long as possible? An important step forward in the development of quantum memories has been achieved by a research team of TU Wien.

Fast track control accelerates switching of quantum bits

UTS opens centre for quantum software development

Quantum computers ditch all the lasers for easier engineering

Further Improvement of Qubit Lifetime for Quantum Computers

US lead in quantum computing 'under siege,' says white house cyber adviser

Quantum Keys Transmitted Over Record-Breaking 404 km

Microsoft is developing its own quantum computer hardware

Google’s DeepMind AI gives robots the ability to dream

Stanford researchers create new special-purpose computer that may someday save us billions

Computer scientists find ‘inexact computing’ can improve answers