Opinnäytetyö (AMK)

Tietojenkäsittely

Sähköisen liiketoiminnan järjestelmät

2012

Karri Koski

TIETOTURVA

– Ilmaiset virustorjuntaohjelmat testissä

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietojenkäsittely | Sähköisen liiketoiminnan järjestelmät

Toukokuu 2012 | 40

Ohjaaja: Minna-Kristiina Paakki

Karri Koski

TIETOTURVA
- ILMAISET VIRUSTORJUNTAOHJELMAT TESTISSÄ

Tämän opinnäytetyön tarkoituksena on tutkia ja testata ilmaisia virustorjuntaohjelmia kahdessa suosituimmassa Windows-käyttöjärjestelmässä, jotka ovat Windows XP ja Windows 7. Molemmat käyttöjärjestelmät valittiin testiin, koska tavoitteena oli selvittää, onko itse käyttöjärjestelmällä käytännön vaikutusta virustorjuntaohjelmien tehokkuuteen tai toimintaan ja minkälainen yhdistelmä mahdollisesti olisi suositeltavin. Valinta kohdistui ilmaisiin virustorjuntaohjelmiin siksi, että myös ilmaisilla virustorjuntaohjelmilla pitäisi pystyä hoitamaan tietokoneen tietoturva täysin kiitettävällä tasolla.

Työssä tarkastellaan asiaa myös tavallisen käyttäjän näkökulmasta, eli esimerkiksi testattavat virustorjuntaohjelmat jätettiin oletusasetuksilleen ja työssä käytettävät virtuaalikoneet luotiin modernin keskivertotietokoneen tehoiseksi. Työssä käytettiin Virtualbox-virtualisointiohjelmistoa.

Työn teoriaosuudessa käydään läpi perustietoja erilaisista haittaohjelmista, keskittyen myös siihen, millaisia eri haittaohjelmien tunnistusmenetelmiä on käytössä. Ennen testausosuutta esitellään neljä testattavaa virustorjuntaohjelmaa ja testausosuudessa käydään läpi testauksen tulokset sekä lopuksi tehdään niistä johtopäätökset.

Testien perusteella lopputuloksena voidaan suositella Windows Xp:ssä käytettäväksi Avast-virustorjuntaohjelmaa ja Windows 7:ssä Avira-virustojuntaohjelmaa. Lopullinen vastuu tietokoneen tietoturvasta on kuitenkin käyttäjällä itsellään.

ASIASANAT:

tietoturva, haittaohjelmat, virustorjuntaohjelmat

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Business Information Technology | e-Business Systems

May 2012 | 40

Instructor: Minna-Kristiina Paakki

Karri Koski

DATA SECURITY
- TESTING OF FREE ANTIVIRUS SOFTWARE

The aim of this thesis was to study and test free antivirus software in two of the most popular Windows operating systems, namely Windows XP and Windows 7. Both of these operating systems were chosen in order to find out what kind of practical influence there is with the operating system to the efficiency or function of the antivirus software. Another focus was to clarify what kind of combination would possibly be the most recommendable. Free antivirus software was chosen to the test, as data security should be kept on excellent level even with free antivirus software.

This thesis deals with the topic from a regular user's point of view, so e.g. the tested antivirus software were left to their default settings and the virtual machines were created with the power of a modern average computer. A virtualization software called Virtualbox was used during the process.

The theory discusses the basics of different malware, also in particular what kind of malware identification methods currently exist. Before the testing part, the four tested antivirus software are introduced and in the testing part the results are reviewed and conclusions are drawn from the test results.

Results implicate recommendation of using Avast antivirus software in Windows Xp and Avira antivirus software in Windows 7. The decisive responsibility of a computer's data security is however, always with the user.

KEYWORDS:

data security, malware, antivirus software

SISÄLTÖ

KUVAT

TAULUKOT

1 JOHDANTO

Monenlaiset haittaohjelmat ja tietoturvariskit uhkaavat tietokoneen käyttäjää tänä päivänä. Ei ole ollenkaan itsestään selvää, että tavallisella käyttäjällä olisi intoa tutkia erilaisia tietokoneensa suojausmahdollisuuksia. Ylipäätään tietokoneen tietoturvasta huolehtiminen vaatii jonkin verran tarkkailua ja jatkuvaa ylläpitoa. Tämä opinnäytetyö pyrkii tuomaan tietoa ja apua tähän ongelmaan.

Nykyään monet kaupalliset tietoturvaohjelmistot ovat paisuneet isoiksi ja raskaiksi ohjelmistoiksi, jotka käyttävät runsaasti tietokoneen resursseja eli keskusmuistia ja prosessoritehoa. Tarjolla on kuitenkin ilmaisia virustorjuntaohjelmia, jotka yleensä ovat kevyempiä ja tarjoavat silti hyvät perusominaisuudet tietoturvauhkien torjumiseen.

Päätin tehdä opinnäytetyöni tästä aiheesta, koska olen jo pitkään ollut kiinnostunut tietoturvaan liittyvistä asioista. Halusin tarkemmin selvittää käytännön vaikutuksia ja eroja käyttöjärjestelmien sekä ilmaisten virustorjuntaohjelmien välillä.

2 HAITTAOHJELMAT

Haittaohjelma on ohjelma (skripti tai koodia), joka on suunniteltu häiritsemään tietokoneen toimintaa erilaisilla tavoilla. Termiä voidaan käyttää myös ylipäätään haitallisesta toiminnasta tietokonetta kohtaan.

Haittaohjelmiksi voidaan luokitella tietokonevirukset, madot, troijalaiset, vakoiluohjelmat, mainosohjelmat tai rootkitit.

Nykypäivänä haittaohjelmat tuntuvat keskittyvän pääasiassa erilaisten yksityisten tietojen hankkimiseen tai varastamiseen ja tätä kautta saavutettavan mahdollisen rahallisen hyödyn maksimoimiseksi rikollisten tai jonkin muun tahon toimesta. Verkkorikollisuus on lisääntynyt yleisesti ottaen sitä mukaa, kun tietokoneiden määrä ja merkitys on lisääntynyt ihmisten arjessa. Erityisesti yritysten täytyy olla entistä valppaampia mahdollisten tietoturvariskien varalta.

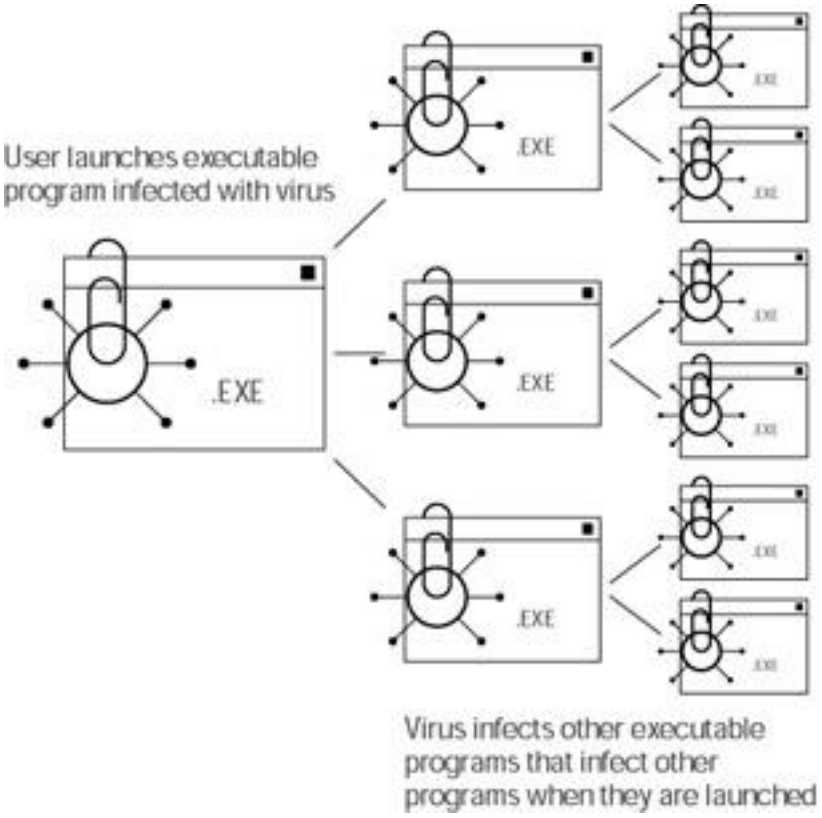
On todettu, että nykyään julkaistaan jo enemmän haitallista koodia sisältäviä ohjelmia kuin laillisia, hyödyllisiä ohjelmia. Tämä luo melkeinpä loputonta taistelua haittaohjelmien tuottajille ja virustorjuntaohjelmien kehittäjille, jotka yrittävät pysyä koko ajan nopealla tahdilla uusiutuvien haittaohjelmien perässä. Nykyisellä haittaohjelmien leviämistahdilla osa kaikista maailman tietokoneista (jotka ovat verkossa) on jatkuvasti saastuneena. On myös laskettu, että noin joka 14. lataus internetistä sisältäisi haitallista koodia. (Malware 2012.)

2.1 Tietokonevirukset

Tietokonevirus on ohjelma, joka voi levitä tietokoneesta toiseen joko verkon tai ulkoisten tallennusvälineiden kautta. Yleensä termiä virus käytetään kaikenlaisista haittaohjelmista, mutta termiä ei pidä sekoittaa näihin, koska tietokonevirus on teknisesti omanlaisensa haittaohjelma. Käytännössä tietokonevirukset tekevät luvattomia muutoksia tietokoneessa ja yleensä juuri tietokonevirukset ovat sellaisia, jotka eivät kiinnitä käyttäjän huomiota millään

tavalla. Tosin tietyt tietokonevirukset eivät varsinaisesti välttämättä edes tee muuta kuin levittävät itseään.

Levittääkseen itsensä tietokoneviruksen täytyy saada lupa suorittaa koodia ja kirjoittaa muistiin. Tämän takia monet tietokonevirukset on liitetty suoritettaviin tiedostoihin, jotka taas voivat olla osana hyödyllisiä ohjelmia. Täten kun käyttäjä suorittaa saastuneen ohjelman myös tietokonevirus suoritetaan samanaikaisesti (Kuva 1).



Kuva 1. Tietokoneviruksen leviäminen. (Internet Insecurity 2011a.)

Tietokonevirukset voidaan jakaa kahteen luokkaan niiden käyttäytymisen perusteella, kun ne suoritetaan: suoraan toimivat virukset ja muistinvaraiset virukset.

2.1.1 Suoraan toimivat virukset

Suoraan toimivat virukset etsivät välittömästi muita saastutettavia kohteita, saastuttavat nämä kohteet ja tämän jälkeen siirtävät kontrollinsa saastutetulle ohjelmistolle. Suoraan toimivat virukset sisältävät haku-moduulin sekä replikaatio-moduulin. Haku-moduuli on vastuussa uusien saastutettavien kohteiden löytämisestä. Haku-moduuli kutsuu replikaatio-moduulia suorittamaan saastuttamisen jokaiselle löytämälleen saastutettavalle kohteelle.

2.1.2 Muistinvaraiset virukset

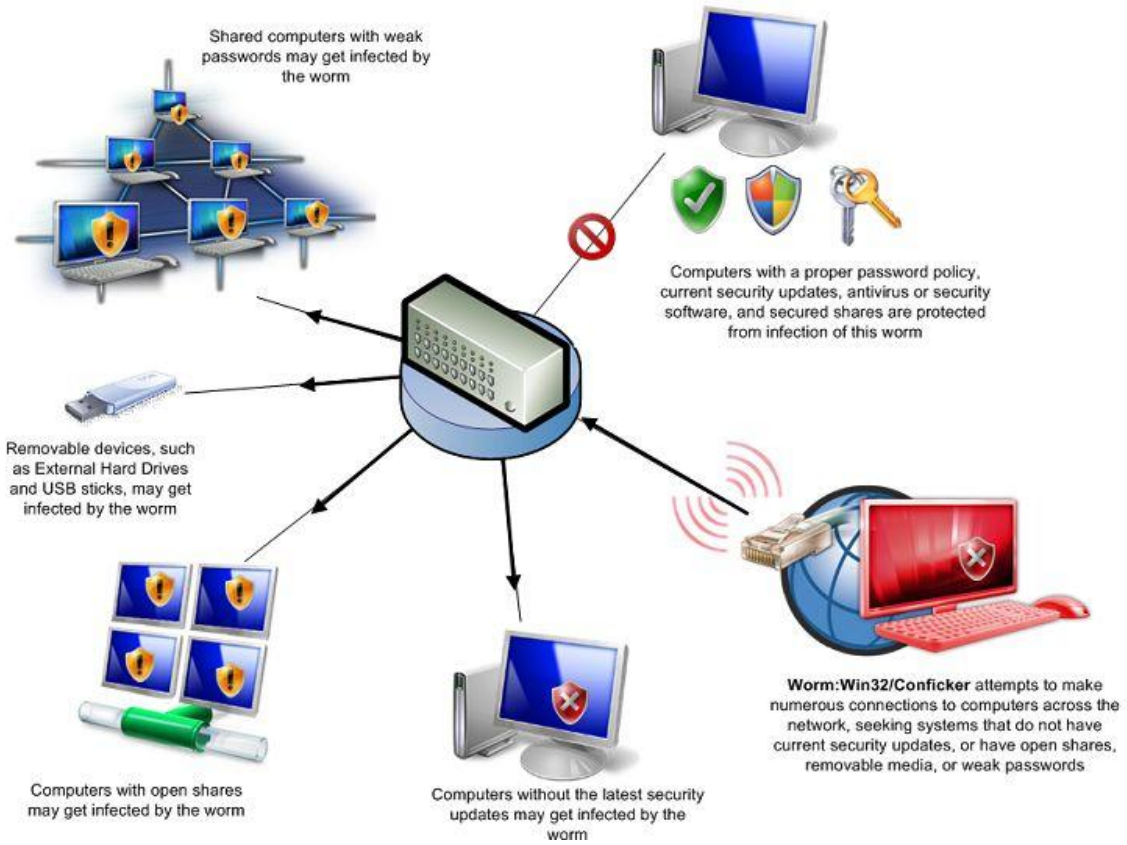
Muistinvaraiset virukset eivät etsi saastutettavia kohteita käynnistyessään. Muistinvarainen virus ei myöskään sisällä haku-moduulia vaan tämän sijasta tällainen virus lataa replikaatio-moduulinsa muistiin ja siirtää kontrollin käyttöjärjestelmälle. Täten replikaatio-moduuli suoritetaan joka kerta, kun käyttöjärjestelmää kutsutaan tekemään jokin tietty operaatio. Tällöin virus pysyy aktiivisena taustalla ja saastuttaa kohteita sitä mukaa, kun tiedostoja suoritetaan tai käytetään ohjelmien tai käyttöjärjestelmän toimesta.

Muistinvaraiset virukset voidaan vielä jakaa kahteen pienempään luokkaan: nopeat saastuttajat ja hitaat saastuttajat. Nopeat saastuttajat pyrkivät saastuttamaan mahdollisimman paljon tiedostoja ja perustuvat nopeaan leviämiseen. Tästä yksi erityinen esimerkki on, jos esimerkiksi käytössä oleva virustorjuntaohjelma ei havaitse virusta muistista ja lähdetään suorittamaan virusten skannaus. Tässä tapauksessa virus voi tavallaan hyödyntää itse virustorjuntaohjelmaa, kun se käy läpi tiedostoja, mutta samalla virus myös saastuttaa kaikki skannatut tiedostot. Tämän tyypin virukset ovat toisaalta helpommin tunnistettavissa, koska monien tiedostojen saastuttaminen yleensä hidastaa tietokonetta tai aiheuttaa muuten epäilyttäviä toimia, jotka virustorjuntaohjelma voi havaita. Hitaat saastuttajat ovat taas nimenomaan suunniteltu leviämään harvemmin ja välttämään niiden havaitsemista, rajoittamalla itse viruksen toimintaa. Esimerkiksi jotkin tämän tyyppiset virukset

saastuttavat tiedostoja ainoastaan silloin kun niitä kopioidaan. (Computer virus 2012.)

2.2 Madot

Mato on itseänsä aktiivisesti ja automaattisesti kopioiva haittaohjelma, joka käyttää verkkoja leviämiseen. Madot skannaavat verkkoja ja hyödyntävät haavoittuvia kohteita levitäkseen (Kuva 2). Toisin kuin tietokonevirus, mato ei vaadi käyttäjältä mitään toimia eikä sen tarvitse liittää itseään olemassa olevaan ohjelmaan. Tämän takia madot leviävät todella nopeasti. Vaikka mato olisikin tehty pelkästään leviämiseen, eikä varsinaisesti haitalliseen toimintaan, niin kuitenkin madot aiheuttavat harmia ainakin vähintään verkkoon käyttämällä kaistaa turhaan.

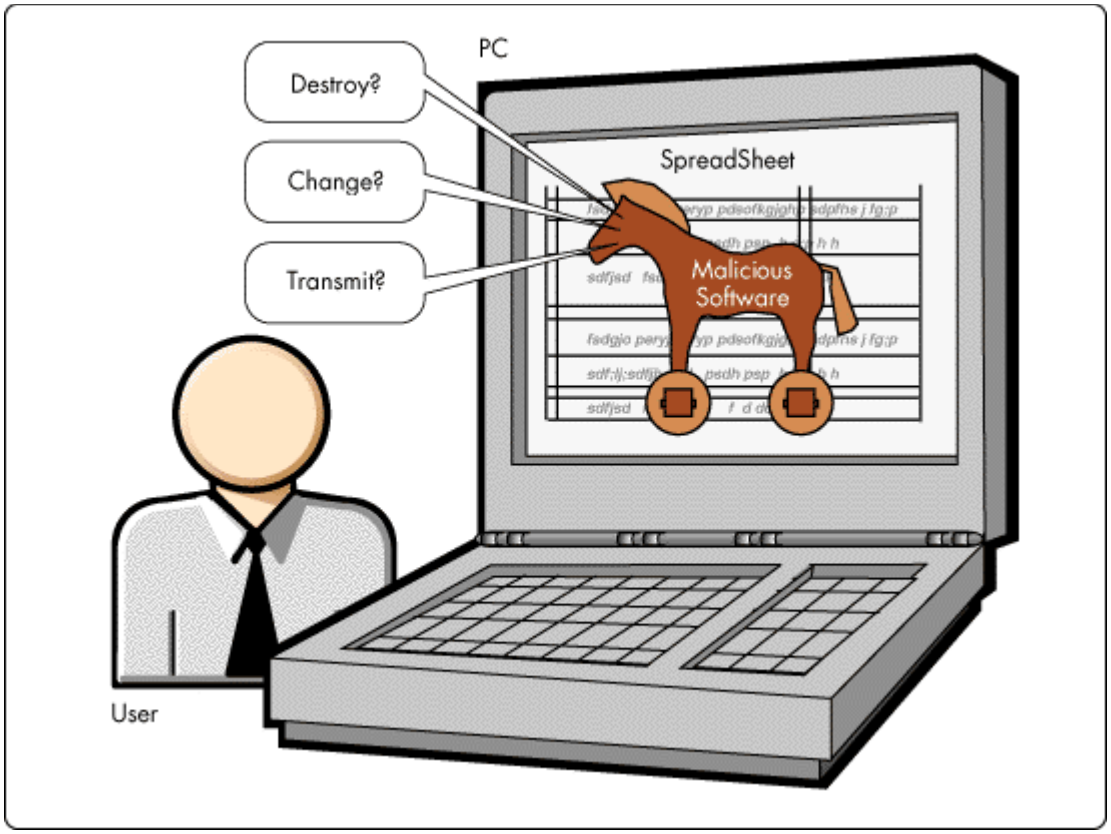


Kuva 2. Madon leviäminen. (Internet Insecurity 2011b.)

Madot sisältävät tietosisällön, joka on koodi, jota käytetään tiedonsiirtoon. Tätä koodia madot hyödyntävät ja perinteisesti madot voivat esimerkiksi poistaa tai salata tiedostoja saastuttamassaan tietokoneessa. Yleensä madot myös asentavat saastuneeseen tietokoneeseen ”takaoven”, jonka kautta madon tekijä voi hallita tai käyttää hyödykseen saastunutta tietokonetta. Täten mato luo ns. zombitietokoneen. Yhdessä nämä lukuisat zombitietokoneet, luovat bottiverkon, jota voidaan hyödyntää esimerkiksi roskapostin lähettämiseen. (Computer worm 2012.)

2.3 Troijalaiset

Troijalainen on haittaohjelma, joka käytännössä esittää olevansa jotain muuta kuin se todellisuudessa on. Siis mikä tahansa tavalliseltakin näyttävä ohjelma, joka houkuttelee käyttäjän asentamaan sen, mutta sisältää kuitenkin haitallista koodia (Kuva 3).



Kuva 3. Troijalainen. (Trojan Horse Software 2006.)

Troijalaiset eivät yritä saastuttaa muita tiedostoja, kuten tietokonevirukset. Troijalaiset eivät myöskään pyri levittämään itseään muihin tietokoneisiin kuten madot. Vaikka troijalaiset eivät pyrikään leviämään, ne voivat silti olla aivan yhtä tuhoisia. Yksi yleisin troijalainen on esimerkiksi ohjelma, joka esittää olevansa virustentorjuntaohjelma, mutta itse asiassa kerääkin koneelle lisää muita haittaohjelmia. Troijalaiset myös leviävät matojen avulla ja näin ollen niiden vaikutus tavallaan tuplaantuu.

Troijalaiset voivat matojen tapaan myös sallia etähallinnan saastuneeseen tietokoneeseen. Tällöin konetta voidaan hyödyntää esimerkiksi bottiverkoissa. Koneelta voidaan myös varastaa yksityisiä tietoja (salasanoja, pankkitietoja) tai ylipäätään seurata käyttäjän toimia tietokoneella. Tämän kaltaiset troijalaiset siis vaativat jonkin ulkopuolisen henkilön toimia. Tämä ulkopuolinen henkilö voi periaatteessa olla kuka tahansa. Tarpeeksi osaava henkilö voi skannata verkkoja löytääkseen troijalaisen saastuttaman tietokoneen ja tätä kautta päästä siihen käsiksi.

Bottiverkkojen ja osittain aggressiivisesta verkkomainonnasta (rikkoo käyttäjien yksityisyyttä) johtuen troijalaisten määrä on koko ajan lisääntynyt ja ne ovatkin yksi yleisin haittaohjelmamuoto. (Trojan horse 2012.)

2.4 Vakoiluohjelmat

Vakoiluohjelma on haittaohjelma, joka kerää tietoa käyttäjästä hänen tietämättään. Näitä tietoja ovat esimerkiksi erilaiset henkilökohtaiset tiedot, kuten käyttäjätunnukset ja salasanat sekä tiedot internetin käytöstä. Pelkän tiedon keräämisen lisäksi vakoiluohjelma voi myös asentaa muita ylimääräisiä ohjelmia tai muokata etenkin tietokoneen tietoturvaan liittyviä asetuksia ja tätä kautta avata väyliä muille haittaohjelmille. Kuten useimmat haittaohjelmat, myös vakoiluohjelma voi aiheuttaa turhaa prosessorin, kiintolevyn tai verkon käyttöä sekä vakausongelmia. Vakoiluohjelmat eivät yleensä pyri virusten tai matojen tapaan leviämään, vaan pikemminkin iskevät jo valmiiksi saastuneisiin

tietokoneisiin. Juuri tästä syystä, koneen toiminta alkaa hidastua tai jumiutua, koska haitallisten prosessien määrä on niin suuri.

Tyypillisesti vakoiluohjelma on piilossa käyttäjältä ja voi olla vaikea havaita sekä se myös asentuu käyttäjän tietämättä, joko harhauttamalla käyttäjää tai haavoittuvuuksien kautta. Vakoiluohjelma voi myös asentua koneelle jonkin hyödyllisen ohjelman mukana ja jopa hyvinkin tunnetuilta virallisilta ohjelmistoalan toimijoilta. Jotkin vakoiluohjelmat jopa poistavat toisia vakoiluohjelmia, siinä toivossa, ettei käyttäjä havaitse vakoiluohjelmaa, koska yleensä vasta monien vakoiluohjelmien yhteisvaikutus herättää käyttäjän huomion.

Vakoiluohjelmat ovat sitkeitä haittaohjelmia. Käyttöjärjestelmän rekisteri sisältää useita lohkoja, joissa tiettyjen avainarvojen muuttamisella saadaan ohjelmat käynnistymään automaattisesti käyttöjärjestelmän käynnistyessä. Tätä rakennetta vakoiluohjelmat hyödyntävät, kiertääkseen itse vakoiluohjelman poistamista. Tyypillisesti vakoiluohjelma linkittää itsensä jokaiseen käynnistyksen sallivaan lohkoon rekisterissä. Kun vakoiluohjelma on käynnissä, se tarkastaa säännöllisesti, jos jokin näistä linkeistä poistetaan. Jos näin tapahtuu, vakoiluohjelma palauttaa tämän linkin automaattisesti. Tämä varmistaa sen, että vakoiluohjelma edelleen käynnistyy käyttöjärjestelmän yhteydessä, vaikka jotkin tai jopa suurin osa näistä linkeistä poistettaisiinkin. (Spyware 2012.)

2.5 Mainosohjelmat

Mainosohjelma toimii yhteistyössä vakoiluohjelmien kanssa ja yleensä ne asentuvat näiden mukana. Molemmat ohjelmat hyödyntävät toisiaan siten, että vakoiluohjelma kerää tietoa käyttäjistä ja luo näille profiileja, joita taas mainosohjelmat käyttävät. Tämän profiilin perusteella mainosohjelma automaattisesti näyttää esimerkiksi ponnahdusikkunoita säännöllisin väliajoin tai tietyn tyyppisiä mainosbannereita sivustoilla. Mainosohjelmat ovat luonteeltaan ärsyttäviä, koska yleensä nämä mainokset käyttävät animaatioita tai muita

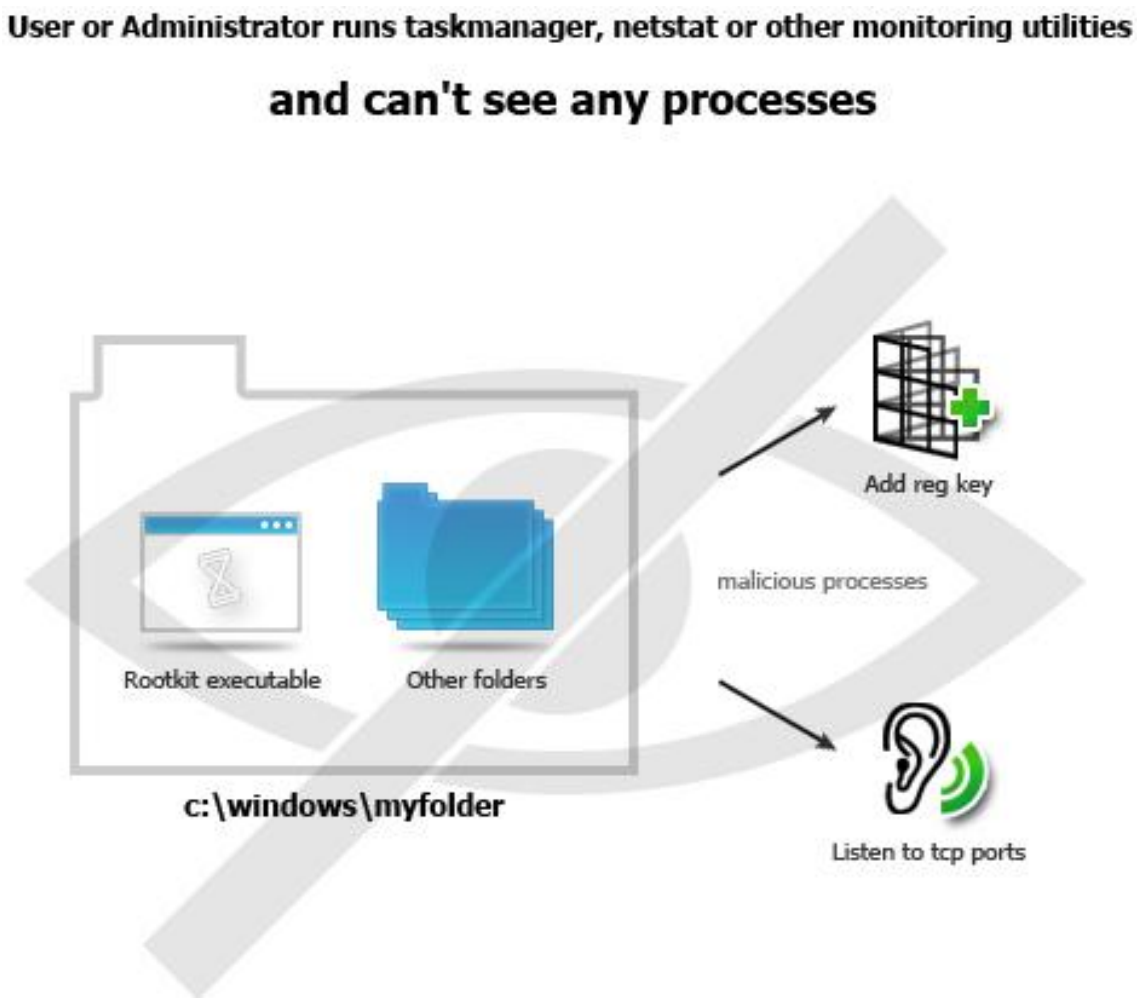
vilkkuvia elementtejä, jotka häiritsevät käyttäjää. Sinänsä itse mainosohjelma on tavallaan harmiton, mutta mainosohjelman vaikutusten ilmaantuessa, voi olettaa, että koneella on myös muita haittaohjelmia.

Mainosohjelmat ovat yleisesti myös kaupallisia ja tässä tapauksessa ne on yleensä integroitu jonkin ohjelmiston mukaan. Mainosohjelmat pyrkivät haalimaan tuottoa tekijälleen ja tämä summa kertyy näytettyjen mainosten määrän perusteella. Tästä syystä jotkin ohjelmistojen kehittäjät käyttävät hyödykseen mainosohjelmia kattaakseen esimerkiksi ohjelmiston kehittämisen kuluja ja joissakin tapauksissa tämä voi antaa mahdollisuuden tarjota ohjelmisto ilmaiseksi tai pienempään hintaan. Näissä tapauksissa mainosohjelma myös usein asentuu erillisenä komponenttina, ja jatkaa toimintaansa vaikka itse ohjelmisto ei olisi edes käynnissä tai vaikka se poistettaisiinkin. Tästä syystä mainosten ilmaantuminen voi jatkua, ennen kuin itse mainosohjelman komponentti poistetaan kunnolla. (Adware 2012.)

2.6 Rootkitit

Rootkit on yksi edistyneimpiä haittaohjelmia ja se on suunniteltu piiloutumaan erittäin hyvin. Tyypillisesti rootkit asentuu automatisoidusti hyödyntämällä haavoittuvuuksia tai troijalaisen mukana tai hyökkääjän toimesta, joka pääsee suoraan fyysisesti käsiksi järjestelmään. Avain-asia rootkitin toiminnassa on admin-tason oikeudet järjestelmään, tämän tason täysillä oikeuksilla rootkitin avulla on mahdollista hallita tai muokata järjestelmää.

Rootkit muokkaa itse käyttöjärjestelmää siten, että se on täysin piilossa käyttäjältä, sen prosessi ei siis näy järjestelmän prosessilistauksissa ja sen konfiguraatiodata on piilotettu eikä sen tiedostoja myöskään lueta (Kuva 4). Rootkit käyttää myös aktiivisia kierto- tai hämäystoimia salatakseen olemassaolonsa käyttöjärjestelmältä. Rootkit tekee tämän muokkaamalla käyttöjärjestelmän ydinosien toimintoja, ajureita tai kernelin moduuleja. Ei ole myöskään harvinaista, että rootkit kytkee pois päältä käyttöjärjestelmän tapahtumalokin havaitsemisensa estämiseksi.



Kuva 4. Rootkit. (AVS Firewall 2012.)

Rootkitin luonteen takia sitä voidaan käyttää perinteisiin haitallisiin tarkoituksiin muiden haittaohjelmien tapaan. Toisaalta ne tarjoavat myös hyödyllisiä toimintoja ja niitä voidaan tarkoituksella käyttää esimerkiksi huijauksen estona erilaisissa verkkopeleissä, tehostamassa emulointiohjelmistoja tai varkaudenesto suojana kannettavissa.

Rootkitin havaitseminen on vaikeaa, koska se toimii samalla turvatasolla käyttöjärjestelmän kanssa ja täten pystyy myös torjumaan tai kumoamaan sellaisen ohjelman, jonka tarkoitus on havaita rootkit. Hankaluus tulee myös siitä, että osa rootkiteistä pesiytyy niin syvälle käyttöjärjestelmään (kernel-tason rootkit), että ei voida luottaa enää niihin toimintoihin, jotka pyrkivät havaitsemaan muutoksia järjestelmässä. Tässä tilanteessa myöskään

toimintojen kuten tiedostojen listauksen tai prosessien listauksen, ei voida luottaa toimivan oletetusti. Toisin sanoen mihinkään järjestelmän osaan ei voida luottaa. Rootkittejä etsivä ohjelma on tehokas ainoastaan silloin, kun rootkitissä on jokin virhe sen piiloutumisessa tai rootkit toimii alemman tason oikeuksilla kuin havaitseva ohjelma. Rootkitin poistaminen voi olla hankalaa tai miltei jopa mahdotonta, riippuen siitä minkä tyyppinen rootkit on kyseessä. Etenkin kernel-tason rootkiteissä, kiintolevyn tyhjennys on yleensä ainoa varma tapa poistaa rootkit. Firmware-tyyppiset rootkitit voivat vaatia jopa laitteiston korvaamista tai erityisvälineitä. (Rootkit 2012.)

3 HAITTAOHJELMIEN TUNNISTUSMENETELMÄT

Virustorjuntaohjelmat käyttävät muutamaa erilaista menetelmää tunnistaakseen haittaohjelmia ja tyypillisesti yksittäinen virustorjuntaohjelma käyttää näitä molempia.

Pääasiassa nämä tunnistusmenetelmät ovat signatuureihin perustuva havaitseminen sekä heuristinen analyysi (epäilyttävään käytökseen perustuva valvonta).

3.1 Signatuureihin perustuva havaitseminen

Signatuureihin perustuva havaitseminen on yleisin haittaohjelmien tunnistamiseen käytetty menetelmä. Signatuuri on ikään kuin näyte tai kaava haittaohjelman koodista. Joka kerta kun tiedostoja skannataan, virustorjuntaohjelma käy läpi signatuurilistan ja vertaa sitä skannattavaan tiedostoon. Jos tiedostosta havaitaan haitallista koodia signatuurilistan perusteella, tiedosto merkataan ja tämän jälkeen voidaan suorittaa tarvittavat toimenpiteet saastuneelle tiedostolle. Tätä menetelmää kuitenkin rajoittaa hieman se, että se perustuu jo valmiiksi tunnistettujen haittaohjelmien löytämiseen. Täten se ei ole tehokas uusia tunnistamattomia haittaohjelmia vastaan.

Koska uusia haittaohjelmia luodaan runsaasti joka päivä, tämä menetelmä tarvitsee usein päivityksiä. Tästä syystä virustorjuntaohjelmien kehittäjät yleensä myös sallivat käyttäjien lähettävän uusia haittaohjelmia tai niiden muunnoksia analysoitavaksi, edistääkseen ja nopeuttaakseen näiden tunnistamista ja tätä kautta päivitystahtia.

Haittaohjelmien tekijät pyrkivät jatkuvasti olemaan askeleen edellä ja muokkaavat haittaohjelmiaan esimerkiksi kryptaamalla koodia, jotta

haittaohjelmaa ei enää havaittaisi signatuurin perusteella. Tämä on yksi syy, minkä takia tarvitaan myös muita tunnistusmenetelmiä.

3.2 Heuristinen analyysi

Tietokonetieteessä heuristiikka on tekniikka, joka on suunniteltu ratkaisemaan jokin ongelma, vaikka ratkaisua ei voitaisikaan todistaa täysin virheettömäksi, mutta joka kuitenkin yleensä tuottaa hyvän lopputuloksen tai yksinkertaistaa varsinaista ongelmaa. Heuristiikan avulla voidaan saavuttaa hyötyjä myös haittaohjelmien tunnistamisessa. Suurin osa vähänkään kehittyneemmistä virustorjuntaohjelmistoista käyttää heuristiikkaa haittaohjelmien tunnistamiseen.

Heuristisella analyysillä pyritään havaitsemaan uusia ja tuntemattomia haittaohjelmia sekä jo olemassa olevien haittaohjelmien muunnelmia. Heuristinen analyysi toimii hieman samankaltaisesti kuin signatuureihin perustuva havaitseminen, mutta tunnistaa yleensä yhden tietyn haittaohjelman sijaan kokonaisia ”haittaohjelmaperheitä” yhden geneerisen signatuurin avulla. Koska haittaohjelmat muuntautuvat ja luovat erilaisia versioita itsestään, on tällainen laajempi signatuuri tarpeellinen. Yhden yleisen signatuurin luonti on mahdollista, koska yleensä haittaohjelmaperheestä löytyy jokin sama ominaisuus, jonka kaikki haittaohjelmat kyseisessä perheessä jakavat. Tätä kautta on myös mahdollista tunnistaa haittaohjelmia entistä nopeammin.

Useimmat virustorjuntaohjelmat toteuttavat heuristisen analyysin suorittamalla epäilyttävän ohjelman tai skriptin omassa virtuaaliympäristössään. Tällä tavalla mahdollisesti haitallinen koodi sekä sen suorittamat operaatiot saadaan analysoitua ja jos siinä havaitaan esimerkiksi monistumista tai tiedostojen päällekirjoitusta, niin tämä kyseinen tiedosto merkitään mahdollisesti haitalliseksi ja käyttäjää hälytetään.

Toinen heuristisen analyysin toimintatapa on ”purkaa” epäilyttävä tiedosto ja analysoida sen lähdekoodia. Tätä lähdekoodia verrataan jo tunnettujen haittaohjelmien lähdekoodiin. Jos tietty prosentti analysoidusta lähdekoodista

vastaa jonkin tunnetun haittaohjelman lähdekoodia, niin tiedosto merkataan mahdollisesti haitalliseksi ja käyttäjää hälytetään.

Vaikka heuristisella analyysillä on mahdollista havaita useita tuntemattomia haittaohjelmia, sen tehokkuus on suhteellisen matala tarkkuuden ja väärien hälytysten takia. Tämä johtuu haittaohjelmien jatkuvasta muuntautumisesta ja kehittymisestä. Koska myös heuristinen analyysi perustuu pitkälti jo tunnettujen haittaohjelmien hyödyntämiseen, siltä voi jäädä huomaamatta sellaisia haittaohjelmia, jotka käyttävät täysin uusia toimintatapoja tai koodia. Toisaalta samalla kuitenkin myös heuristinen analyysi kehittyy haittaohjelmien mukana, kun haittaohjelmia havaitaan eri keinoin ja näitä tietoja lisätään heuristisen analyysin käyttöön. Heuristisen analyysin onnistunut hyödyntäminen riippuukin hyvin pitkälti hyvän balanssin löytämiseen väärien ja oikeiden hälytysten välillä, sekä siitä, kuinka aktiivisesti käyttäjää vaaditaan tekemään ratkaisuja hälytysten perusteella. (Antivirus software 2012.)

4 TESTATTAVAT VIRUSTORJUNTAOHJELMAT

Valitsin testattavaksi valikoiman ilmaisversioita tämän hetken suosituimmista virustorjuntaohjelmista. Yleensä ilmaisissa virustorjuntaohjelmissa tarkoituksena on se, että ne toimivat tietoturvayritysten ”sisäänheittotuotteina”, eli käyttäjää houkutellaan ostamaan samasta ohjelmistosta sen kaupallinen versio kattavammilla tai parannetuilla ominaisuuksilla. Yleensä ilmaisversio sisältää pelkän virustorjunnan. Kaupallisella versiolla tämän lisäksi voi saada esimerkiksi softapalomuuria ja roskaposti tai web-sisällön suodatusta sekä varmuuskopiointia.

4.1 Avast! Free Antivirus v7

Avast on tsekkiläisen AVAST Software a.s:n kehittämä ja se on yksi tämän hetken suosituimmista ilmaisista virustorjuntaohjelmista. Se on saanut myös lukuisia eri palkintoja ja tunnustuksia alan tunnetuimmilta testaajilta (esim. VirusBulletin ja AV Comparatives). Kuukauden kokeiluajan jälkeen Avast vaatii rekisteröitymisen, jonka voi tehdä ilmaiseksi. Avastista on yksi asennuspaketti, joka tukee 32-bittisiä ja 64-bittisiä käyttöjärjestelmiä Windows Xp Sp2:sta eteenpäin. Avastin mukaan sillä on yli 150 miljoonaa käyttäjää. Ensimmäinen virallinen versio ohjelmasta on julkaistu vuonna 2001.

Avastin ilmaisversio sisältää kattavasti toimintoja haittaohjelmien torjuntaan, eikä siitä juurikaan puutu mitään tärkeitä ominaisuuksia sen maksullisiin versioihin nähden. Avast vaatii Flash Playerin asennuksen, jos ohjelmasta haluaa tarkastella erilaista tilastotietoa. Maksullisella Pro-versiolla saa esimerkiksi Sandbox-ominaisuuden eli virtuaalitilan, jossa voi täysin turvallisesti esimerkiksi testata ohjelmia tai surffata netissä. Vieläkin kattavammalla Internet Security -versiolla saa edellä mainittujen ominaisuuksien lisäksi vielä softapalomuurin sekä Anti-spam-ominaisuuksia. (Avast 2012.)

4.2 AVG Free Edition v2012

AVG on tsekkiläisen AVG Technologiesin kehittämä ja se on suosituimpien ilmaisten virustorjuntaohjelmien joukossa. Avg ei vaadi rekisteröintejä ja on suoraan käytettävissä asennuksen jälkeen. Avg:sta on erikseen 32-bittinen sekä 64-bittinen versio. Avg:n mukaan sillä on yli 100 miljoonaa käyttäjää. Ensimmäinen virallinen versio ohjelmasta on julkaistu vuonna 1998.

Avg:n ilmaisversio sisältää hyvät perustoiminnot haittaohjelmien torjuntaan. Hyvänä lisänä ilmaisversiossa saa LinkScanner-ominaisuuden, joka skannaa linkkejä etukäteen ja ilmoittaa käyttäjälle, onko niitä turvallista käyttää. Maksullisessa Basic-versiossa mukaan saa esimerkiksi myös Pc Analyzer -ominaisuuden, jolla voi skannata käyttöjärjestelmän rekisteriä tai levyvirheitä sekä eheyttää kiintolevyä. Tämä on ihan kätevä ominaisuus sellaiselle käyttäjälle, joka ei käytä erillisiä siivousohjelmia. Maksullinen versio tarjoaa myös 24/7 puhelintuen. Internet Security -versio sisältää jälleen kaikki edellä mainitut ominaisuudet sekä softapalomuurin ja Anti-spam-suojauksia. Avg asentaa oletuksena oman Security-työkalupalkkinsa selaimeen, jonka kautta voi käyttää erilaisia toimintoja nopeasti. Omasta mielestäni kuitenkaan yhdenkään ohjelman ei pitäisi asentaa minkäänlaisia työkalupalkkeja, olivat ne sitten hyödyllisiä tai eivät, koska käyttäjälle ei yleensä ilmoiteta asiasta. Tarkemmilla asennus vaihtoehdoilla tämänkin saa ruksattua pois, mutta yleensä tavallinen käyttäjä asentaa ohjelmat pika-asennuksella. (Avg 2012.)

4.3 Avira AntiVir Personal – Free Antivirus v12

Avira on saksalaisen Avira Operationsin kehittämä ja on yksi suosituimpia ilmaisia virustorjuntaohjelmia. Avira ei vaadi rekisteröintejä, jotta sitä voidaan käyttää. Avirasta on yksi asennuspaketti, joka tukee 32-bittisiä ja 64-bittisiä käyttöjärjestelmiä Windows Xp Sp3:sta eteenpäin. Aviran mukaan sillä on yli 100 miljoonaa käyttäjää. Ensimmäinen virallinen versio ohjelmasta on julkaistu vuonna 2004.

Avira sisältää kohtalaisen kattavasti ominaisuuksia haittaohjelmien torjuntaan. Erityisenä lisänä ilmaisversiossa on Antiphishing-ominaisuus, joka siis suojaa käyttäjää sivustoilta, jotka suorittavat henkilökohtaisten tietojenkalastelua. Maksullisessa Premium-versiossa saa esimerkiksi täydellisen live-käyttäjätuen sekä sähköpostiskannaukset. Internet Security -versio sisältää edellä mainitut ominaisuudet sekä softapalomuurin, Anti-spam-ominaisuudet, varmuuskopiointi-toiminnon ja parempaa keskitettyä hallintaa/monitorointia. Avirastakin löytyy oma työkalupalkkinsa asennettavaksi, mutta hyvä puoli on se, että Avira ei asenna sitä huomaamatta edes pika-asennuksessa. Yksi ikävä ominaisuus Avira v12:sta kuitenkin löytyy, nimittäin ohjelma näyttää silloin tällöin ponnahdusikkunoita, joita ei saa pois edes maksullista versiota käyttämällä. Tämä on aika harvinaista nykyään ja Avira varmasti menettää tämän takia joitakin maksavia asiakkaitaan. (Avira 2012.)

4.4 Microsoft Security Essentials v4

Microsoft Security Essentials on Microsoftin kehittämä ja on täysin ilmainen eikä vaadi rekisteröintejä, tosin Windowsin Genuine Advantage -tarkistuksen läpäiseminen vaaditaan, jotta ohjelmaa voidaan käyttää. Mse:sta on erikseen 32-bittinen ja 64-bittinen versio Windows Vistalle/7:lle sekä oma versionsa Windows Xp:lle. Microsoftin mukaan sillä on noin 100 miljoonaa käyttäjää. Ensimmäinen virallinen versio ohjelmasta on julkaistu vuonna 2009.

Security Essentials sisältää yksinkertaiset toiminnot virustentorjuntaan eikä mitään muuta, käytännössä se siis aktiivisesti suojaa haittaohjelmilta ja tietenkin sillä voi niitä myös skannata. Security Essentials on täysin suunnattu tavallisille käyttäjille, eikä siitä ole siis maksullisia tai erityisesti yrityksille suunnattuja versioita, kuten monilla muilla tietoturvaohjelmistojen tarjoajilla. (MSE 2012.)

5 TESTAUSOSUUS

Keskityin testaamisessa pääasiassa tietoturvan sekä suorituskykyyn liityvien asioiden testaamiseen, käytettävyyden arviointi ei ollut keskiössä tässä työssä. Pyrin testeissä pääsemään mahdollisimman realistisiin tuloksiin tavallisen käyttäjän kannalta, joten loin virtuaalikoneen mahdollisimman lähelle keskivertoa modernia tietokonetta tehojen puolesta, eli asetin virtuaalikoneelle käyttöön 2 gigatavua keskusmuistia sekä 2 prosessoriydintä. Jätin testattavat virustorjuntaohjelmat oletusasetuksilleen, koska yleensä peruskäyttäjä ei asetuksiin kiinnitä suurempaa huomiota.

Testaamisen alustana käytettiin Virtualbox virtualisointiohjelmaa, jonka avulla voitiin helposti ja turvallisesti suorittaa testit vaikuttamatta isäntäjärjestelmään. Käyttöjärjestelmistä asennettiin täysin puhtaat asennukset ja näihin asennettiin vain tarpeelliset ajurit sekä kulloinkin testattava virustorjuntaohjelma ilman muita ohjelmia. Ennen testauksen aloittamista virustorjuntaohjelmaan ja käyttöjärjestelmään asennettiin viimeisimmät päivitykset, jotta saataisiin mahdollisimman ajantasainen kuva tietoturvan tasosta. Kun käyttöjärjestelmät oli asennettu ja päivitetty, loin Virtualboxin snapshot toiminnolla palautuspisteen alkutilanteesta, jotta jokaiselle testikerralle oli täysin sama alusta suorittaa testit. Suoritin kaikki testit toukokuussa 2012 kahden päivän aikana, joten tuloksiin tuskin tuli sen kummempaa vaikutusta mahdollisten päivityksien takia.

Kaikissa haittaohjelmien tunnistamiseen liittyvissä tapauksissa testaamiseen käytettiin täysin samaa ennalta ladattua haittaohjelmapakettia, joka sisälsi erityyppisiä haittaohjelmia 3732 kappaletta. Haittaohjelmien torjuntaan liittyvissä tapauksissa testaamiseen käytettiin kymmentä linkkiä, jotka kerättiin malwaredomainlist.com sivustolta. Nämä linkit sisälsivät erityyppisiä ”tuoreita” haittaohjelmia.

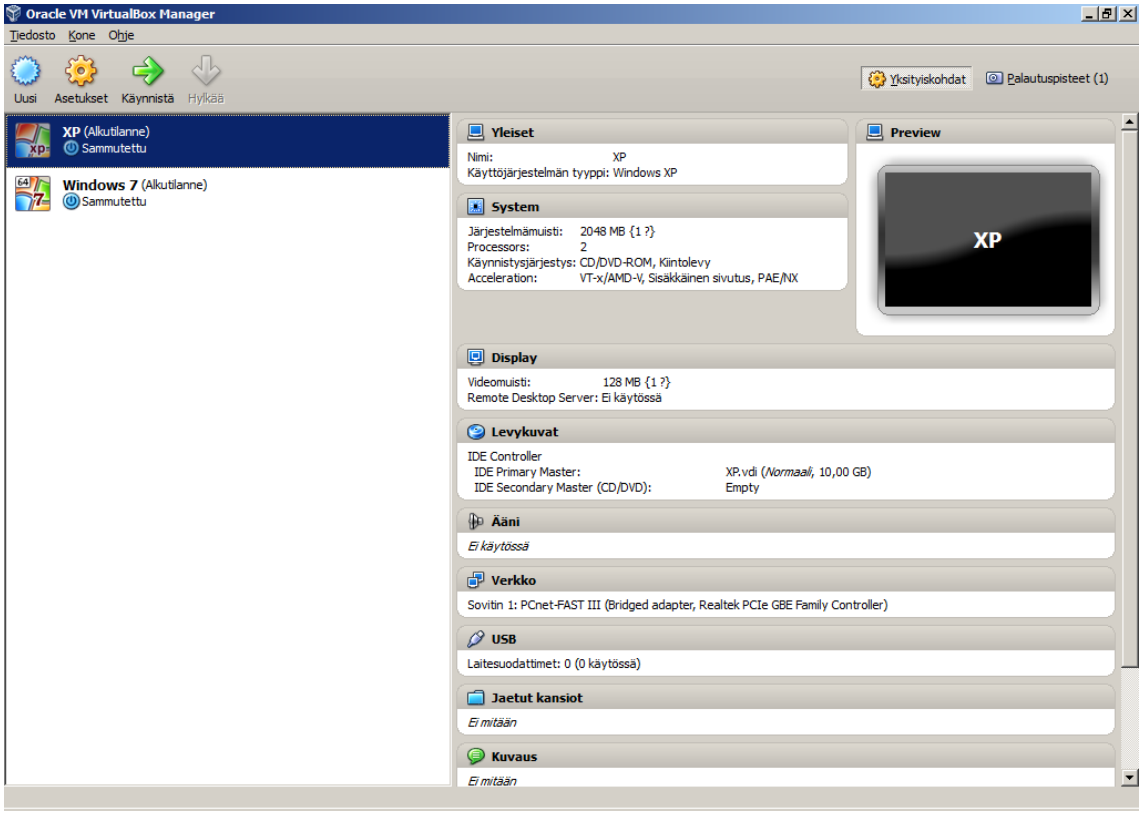
En testannut valmiiksi saastuneen järjestelmän puhdistamista siitä syystä, että oikeastaan ainoa tapa, jolla tietokoneen saa varmasti puhdistettua on kiintolevyn formatointi. Yleisesti virustojuntaohjelmat varmasti eroavat jonkin

verran siinä, kuinka hyvin ne pystyvät puhdistamaan/poistamaan saastuneita tiedostoja, mutta sellaista virustorjuntaohjelmaa ei ole, joka varmasti puhdistaisi saastuneen tietokoneen täydellisesti kaikista haittaohjelmista. Virustorjuntaohjelmien ensisijainen tarkoitus on kuitenkin ennaltaehkäistä mahdollisia tietoturvauhkia.

Muistinkäyttöön liittyvä testi toteutettiin siten, että tietokoneen annettiin olla rauhassa työpöydällä noin kymmenen minuuttia ja tämän jälkeen mitattiin virustorjuntaohjelmaan liittyvien prosessien muistinkäyttö tehtävienhallinnasta. Tietokoneen käynnistymiseen liittyvä testi toteutettiin siten, että tietokone uudelleenkäynnistettiin ja aikaa otettiin siihen asti kunnes prosessorin käyttöaste vakiintui idle-tasolle, eli kun järjestelmän idle prosessi näytti tasaisesti lukua 99.

5.1 Windows XP

Valitsin alustaksi 32-bittisen Windows XP:n, koska se on edelleen suosituimpia käyttöjärjestelmiä maailmassa. Näillä näkymin Windows XP:n muutamaan otteeseen pidennetty tuki päättyy huhtikuussa 2014. Tuon ajankohdan jälkeen XP:tä on vaikea enää suositella käytettäväksi (ainakaan sellaisissa tietokoneissa, jotka ovat yhteydessä verkkoon), koska erilaisia päivityksiä ja korjauksia käyttöjärjestelmään ei enää tehdä ja täten se ei ole enää tietoturvallinen käyttää. Kuvassa 5 nähdään Virtualboxin asetukset Windows XP virtuaalikoneelle.



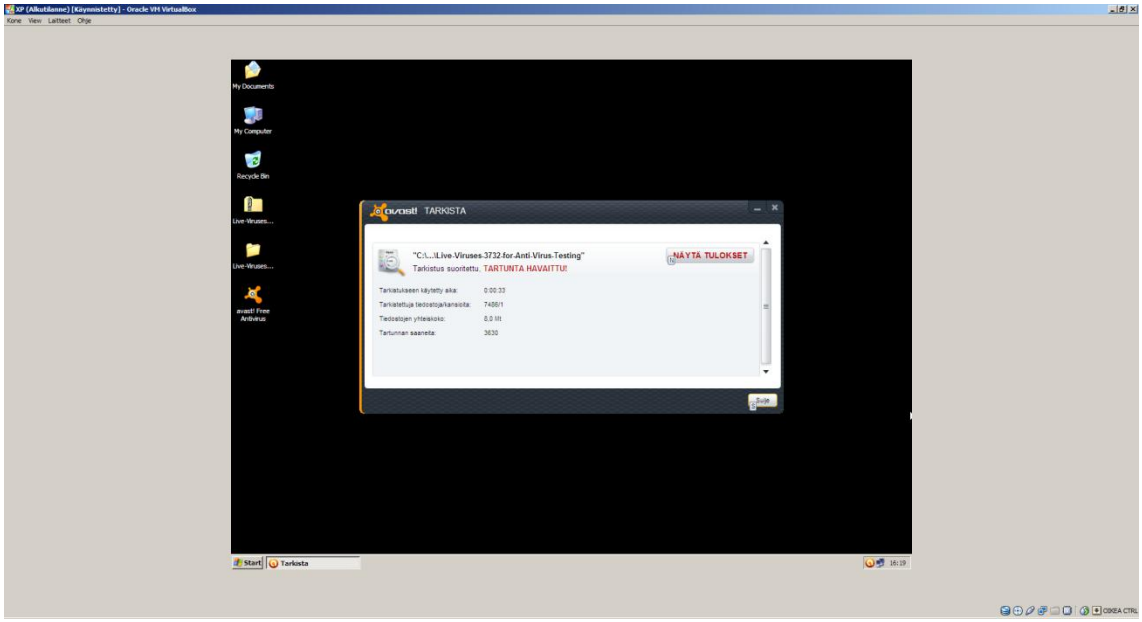
Kuva 5. Windows XP virtuaalikoneen asetukset.

Tämä Windows Xp:n asennus vei tilaa kiintolevyltä noin 1,5 gigatavua.

5.1.1 Avast! Free Antivirus v7

Muistinkäytön osalta Avast on erittäin ”vähäruokainen”. Avast lisää 2 prosessia, jotka kuluttavat yhteensä noin 14 megatavua keskusmuistia. Avast osaa myös pudottaa käyttöliittymän prosessista noin puolet pois, kun ohjelman käyttöliittymä ei ole avoinna työpöydällä ja tällöin muistinkäyttö on yhteensä vain noin 7 megatavua.

Haittaohjelmien tunnistamisessa Avast onnistui havaitsemaan 3630 haittaohjelmaa (Kuva 6). Tunnistamisprosentiksi tulee tällöin noin 97 %. Suoraan tunnistamisen jälkeen Avast onnistui poistamaan kaikki tunnistamansa haittaohjelmat, ilman että niitä tarvitsi ensin siirtää karanteeniin. Avast poisti haittaohjelmat suhteellisen nopeasti, aikaa meni noin 3 minuuttia.



Kuva 6. Windows Xp – Avast – Haittaohjelmien tunnistaminen.

Haittaohjelmien torjumisessa Avast onnistui torjumaan kaikki 10 haitallista linkkiä. Torjumisprosentiksi tulee tällöin 100 %.

Koko järjestelmän skannaukseen aikaa kului 58 sekuntia ja ohjelma käytti skannatessa yhteensä noin 71 megatavua keskusmuistia.

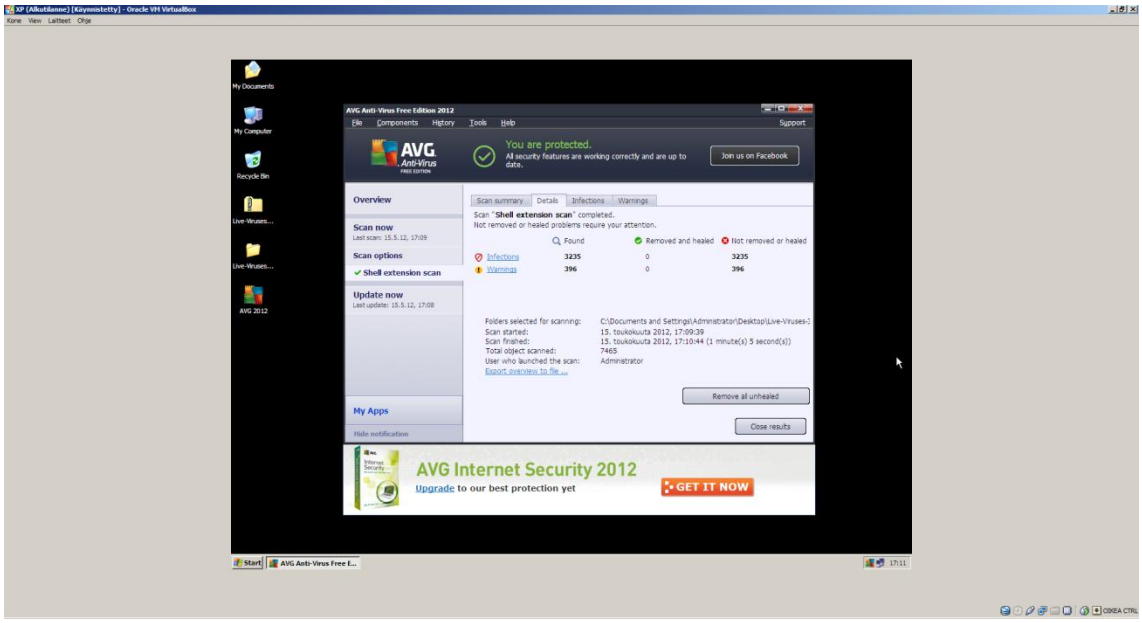
Koneen käynnistäminen Avastin ollessa automaattisesti käynnistyvien ohjelmien listalla kesti noin 37 sekuntia.

5.1.2 AVG Free Edition v2012

Muistinkäytön osalta Avg on kohtalaista tasoa. Avg lisää 10 prosessia, jotka kuluttavat yhteensä noin 56 megatavua keskusmuistia. Avg osaa pudottaa kokonaan pois käyttöliittymän prosessin, kun ohjelman käyttöliittymä ei ole avoinna työpöydällä ja tällöin muistinkäyttö on yhteensä noin 47 megatavua.

Haittaohjelmien tunnistamisessa Avg onnistui havaitsemaan 3631 haittaohjelmaa, tosin se merkitsi näistä 396 kappaletta mahdollisesti haitalliseksi (Kuva 7). Tunnistamisprosentiksi tulee tällöin noin 97 %. Suoraan tunnistamisen jälkeen Avg onnistui siirtämään kaikki haittaohjelmat

karanteeniin, suoraa poistoa ei siis tapahtunut. Avg käytti erittäin runsaasti aikaa haittaohjelmien siirtämiseen karanteeniin, aikaa meni noin 25 minuuttia.



Kuva 7. Windows Xp – Avg – Haittaohjelmien tunnistaminen.

Haittaohjelmien torjumisessa Avg onnistui torjumaan kaikki 10 haitallista linkkiä. Torjumisprosentiksi tulee tällöin 100 %.

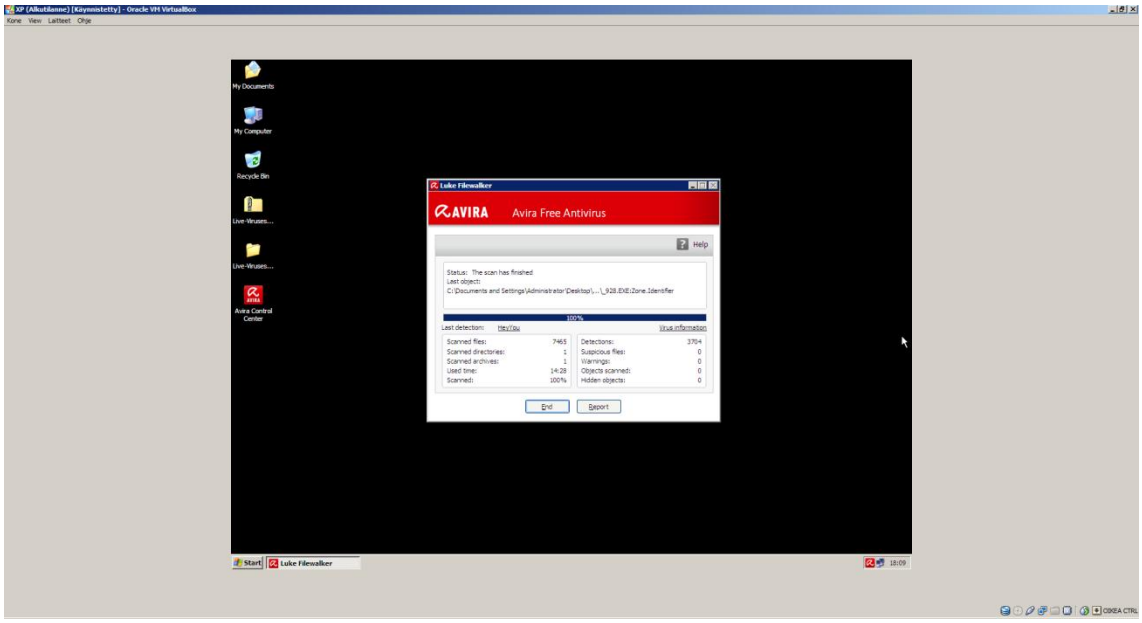
Koko järjestelmän skannaukseen aikaa kului 1min 47 sekuntia ja ohjelma käytti skannatessa yhteensä noin 79 megatavua keskusmuistia.

Koneen käynnistäminen Avg:n ollessa automaattisesti käynnistyvien ohjelmien listalla kesti noin 48 sekuntia.

5.1.3 Avira AntiVir Personal – Free Antivirus v12

Muistinkäytön osalta Avira on säästäväistä tasoa. Avira lisää 5 prosessia, jotka kuluttavat yhteensä noin 26 megatavua keskusmuistia. Avira osaa pudottaa kokonaan pois käyttöliittymän prosessin, kun ohjelman käyttöliittymä ei ole avoinna työpöydällä ja tällöin muistinkäyttö on yhteensä vain noin 10 megatavua.

Haittaohjelmien tunnistamisessa Avira onnistui havaitsemaan 3704 haittaohjelmaa (Kuva 8). Tunnistamisprosentiksi tulee tällöin noin 99 %. Tässä kohtaa voidaan kuitenkin mainita, että Avira käytti ennalta valitun kohteen skannaamiseen reilusti enemmän aikaa kuin muut testissä olleet ohjelmat. Suoraan tunnistamisen jälkeen Avira onnistui poistamaan kaikki tunnistamansa haittaohjelmat, ilman että niitä tarvitsi ensin siirtää karanteeniin. Avira poisti haittaohjelmat nopeasti, aikaa meni noin 2 minuuttia.



Kuva 8. Windows Xp – Avira – Haittaohjelmien tunnstaminen.

Haittaohjelmien torjumisessa Avira onnistui torjumaan 9 haitallista linkkiä. Torjumisprosentiksi tulee tällöin 90 %.

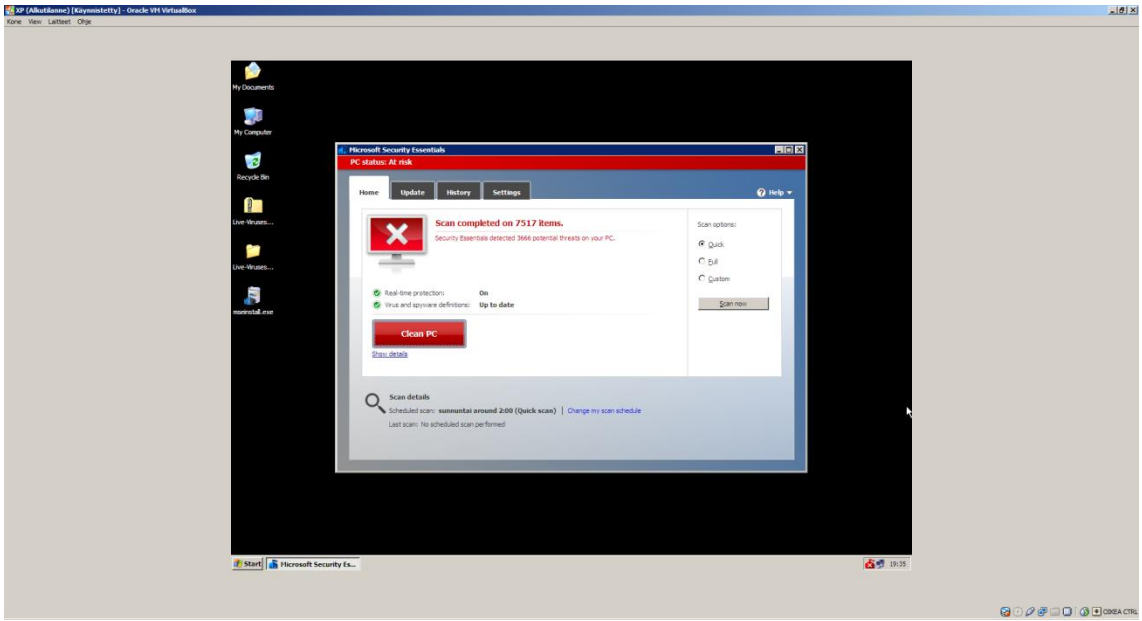
Koko järjestelmän skannaukseen aikaa kului 1min 37 sekuntia ja ohjelma käytti skannatessa yhteensä noin 171 megatavua keskusmuistia.

Koneen käynnistäminen Aviran ollessa automaattisesti käynnistyvien ohjelmien listalla kesti noin 40 sekuntia.

5.1.4 Microsoft Security Essentials v4

Muistinkäytön osalta Mse on kohtalaista tasoa. Mse lisää 2 prosessia, jotka kuluttavat yhteensä noin 53 megatavua keskusmuistia. Mse ei osaa pudottaa pois käyttöliittymän prosessia, kun ohjelman käyttöliittymä ei ole avoinna työpöydällä, joten muistinkäyttö pysyy täysin samana.

Haittaohjelmien tunnistamisessa Mse onnistui havaitsemaan 3666 haittaohjelmaa (Kuva 9). Tunnistamisprosentiksi tulee tällöin noin 98 %. Suoraan tunnistamisen jälkeen Mse yritti oletuksena puhdistaa saastuneita tiedostoja, mutta epäonnistui tässä jokaisen tiedoston kohdalla. Tämän jälkeen Mse onnistui automaattisesti siirtämään karanteeniin kaikki havaitut haittaohjelmat. Mse siirsi haittaohjelmat karanteeniin suhteellisen nopeasti, aikaa meni noin 4 minuuttia.



Kuva 9. Windows Xp – Mse – Haittaohjelmien tunnistaminen.

Haittaohjelmien torjumisessa Mse onnistui torjumaan 7 haitallista linkkiä. Torjumisprosentiksi tulee tällöin 70 %.

Koko järjestelmän skannaukseen aikaa kului 1min 58 sekuntia ja ohjelma käytti skannatessa yhteensä noin 98 megatavua keskusmuistia.

Koneen käynnistäminen Mse:n ollessa automaattisesti käynnistyvien ohjelmien listalla kesti noin 35 sekuntia.

5.1.5 Yhteenveto tuloksista

Taulukossa 1 listataan testin tulokset Windows Xp:n osalta.

Taulukko 1. Windows Xp – Testitulokset.

Windows XP	Tunnistus %	Torjumis %	Muistinkäyttö Mt (UI on/off)	Scan time min.sec	Boot time sec
Avast	97	100	14/7	0.58	37
AVG	97	100	56/47	1.47	48
Avira	99	90	26/10	1.37	40
MSE	98	70	53/53	1.58	35

Haittaohjelmien tunnistamisen ja torjumisen osalta testatut virustorjuntaohjelmat ovat hyvin tasaisia. Ainoa poikkeus on Mse, jonka heuristiikka ei ilmeisesti ole aivan yhtä kehittynyt kuin muissa, koska torjumisprosentti jäi jälkeen muista. Avira saavuttaa erittäin korkean tunnistusprosentin.

Muistinkäytön osalta Avast on selkeästi muita edellä ja Mse sekä Avg kuluttavat reilusti enemmän muistia siihen verrattuna.

Skannausajoissa Avast on jälleen muita selkeästi nopeampi.

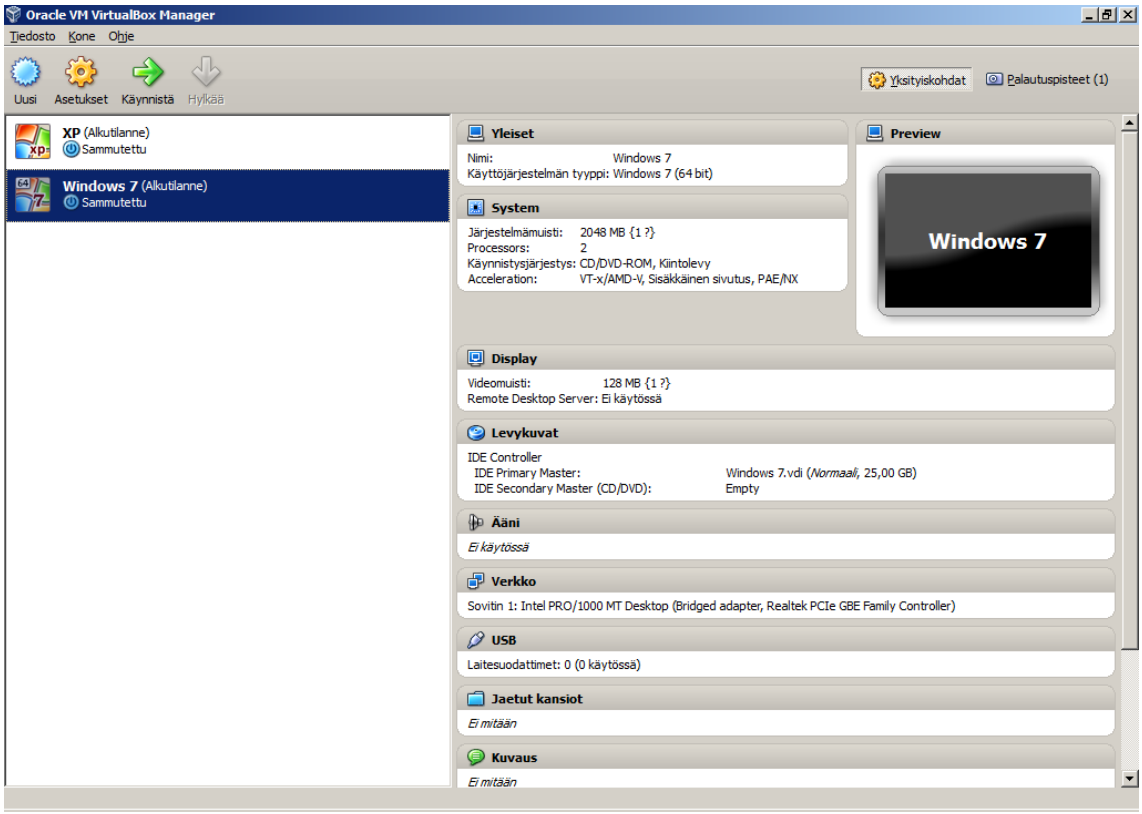
Tietokoneen käynnistämiseen kuluvassa ajassa Mse saa parhaan tuloksen ja Avast pystyy miltein samaan lukemaan.

Näiden tulosten perusteella mielestäni suositeltavin virustorjuntaohjelma Windows Xp:lle olisi Avast. Tietenkin riippuu siitä minkälaisia ominaisuuksia ohjelmassa painottaa, mutta Xp:n käyttäjillä on yleensä keskimäärin vanhempaa laitteistoa käytössään ja tästä syystä arvostan Avastin erittäin

pienen muistinkäytön sekä nopean käynnistymisajan korkealle, jotta virustorjuntaohjelma ei turhaan hidastaisi tietokoneen käyttöä.

5.2 Windows 7

Valitsin toiseksi alustaksi 64-bittisen Windows 7:n, koska Windows 7 on nousemassa XP:n ohi suosituimmaksi käyttöjärjestelmäksi maailmassa ja Windows 7 on myös käyttöjärjestelmän tasolla tietyiltä perusratkaisuiltaan parempi tietoturvan kannalta. Päätin valita 64-bittisen version siitä syystä, että todennäköisesti tulevaisuudessa sen suosio lisääntyy, kun tietokoneiden tehokkuus edelleen kasvaa ja ohjelmistot laajenevat ja kehittyvät. Teoriassa 64-bittisyyden ansiosta käyttöjärjestelmän pitäisi olla myös tietoturvallisempi. Kuvassa 10 nähdään Virtualboxin asetukset Windows 7 virtuaalikoneelle.



Kuva 10. Windows 7 virtuaalikoneen asetukset.

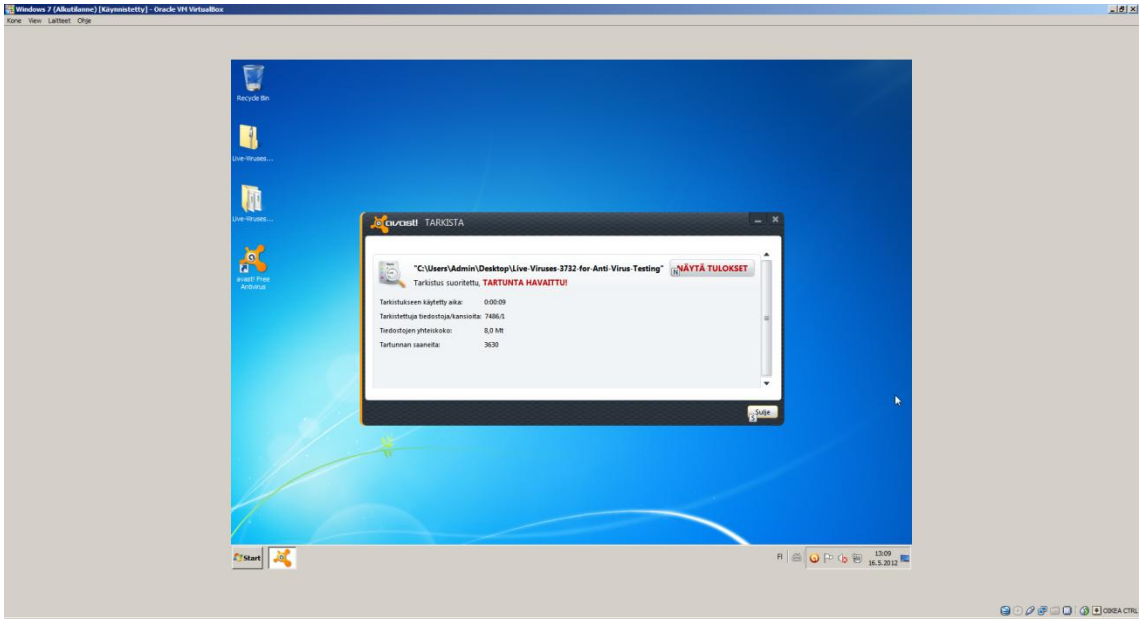
En käyttänyt levyasetuksien osalta Sata controlleria, vaikka se Windows 7:ssä on tuettuna oletuksena, koska tämä todennäköisesti vaikuttaisi ainakin jossain määrin positiivisella tavalla suorituskykyyn liityvien testien tuloksiin ja täten se antaisi ylimääräistä etua. Myöskään kiintolevyn koolla ei tässä tapauksessa ole mitään merkitystä, koska virtuaalinen kiintolevy käyttää vain sen määrän tilaa mitä se tarvitsee ja Virtualbox osaa dynaamisesti kasvattaa sen kapasiteettia jos lisätilalle tulee tarvetta.

Tämä Windows 7:n asennus vei tilaa kiintolevyltä noin 8,5 gigatavua.

5.2.1 Avast! Free Antivirus v7

Muistinkäytön osalta Avast on erittäin ”vähäruokainen”. Avast lisää 2 prosessia, jotka kuluttavat yhteensä noin 9 megatavua keskusmuistia. Avast osaa myös pudottaa käyttöliittymän prosessista suurinpiirtein puolet pois, kun ohjelman käyttöliittymä ei ole avoinna työpöydällä ja tällöin muistinkäyttö on yhteensä vain noin 4 megatavua.

Haittaohjelmien tunnistamisessa Avast onnistui havaitsemaan 3630 haittaohjelmaa (Kuva 11). Tunnistamisprosentiksi tulee tällöin noin 97 %. Suoraan tunnistamisen jälkeen Avast onnistui poistamaan kaikki tunnistamansa haittaohjelmat, ilman että niitä tarvitsi ensin siirtää karanteeniin. Avast poisti haittaohjelmat todella nopeasti, aikaa meni alle minuutti.



Kuva 11. Windows 7 – Avast – Haittaohjelmien tunnistaminen.

Haittaohjelmien torjumisessa Avast onnistui torjumaan kaikki 10 haitallista linkkiä. Torjumisprosentiksi tulee tällöin 100 %.

Koko järjestelmän skannaukseen aikaa kului 2min 54 sekuntia ja ohjelma käytti skannatessa yhteensä vain noin 20 megatavua keskusmuistia.

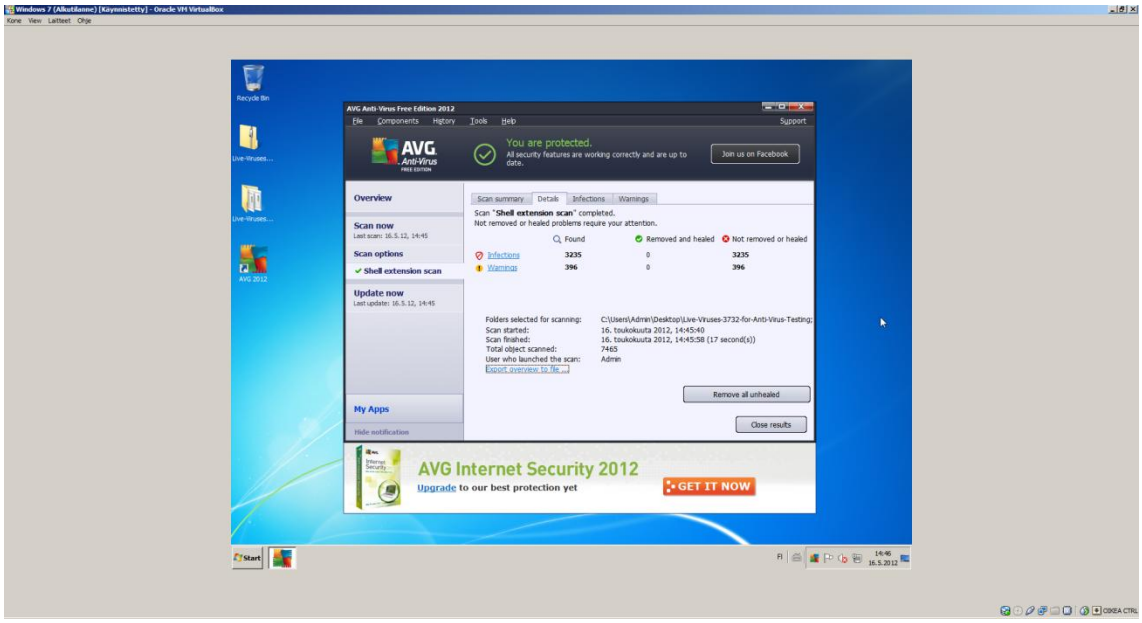
Koneen käynnistäminen Avastin ollessa automaattisesti käynnistyvien ohjelmien listalla kesti vain noin 21 sekuntia.

5.2.2 AVG Free Edition v2012

Muistinkäytön osalta Avg on säästäväistä tasoa. Avg lisää 10 prosessia, jotka kuluttavat yhteensä noin 20 megatavua keskusmuistia. Avg osaa pudottaa kokonaan pois käyttöliittymän prosessin, kun ohjelman käyttöliittymä ei ole avoinna työpöydällä ja tällöin muistinkäyttö on yhteensä noin 15 megatavua.

Haittaohjelmien tunnistamisessa Avg onnistui havaitsemaan 3631 haittaohjelmaa, tosin se merkitsi näistä 396 kappaletta mahdollisesti haitalliseksi (Kuva 12). Tunnistamisprosentiksi tulee tällöin noin 97 %. Suoraan tunnistamisen jälkeen Avg onnistui siirtämään kaikki haittaohjelmat

karanteeniin, suoraa poistoa ei siis tapahtunut. Avg käytti kohtalaisesti aikaa haittaohjelmien siirtämiseen karanteeniin, aikaa meni noin 10 minuuttia.



Kuva 12. Windows 7 – Avg – Haittaohjelmien tunnistaminen.

Haittaohjelmien torjumisessa Avg onnistui torjumaan kaikki 10 haitallista linkkiä. Torjumisprosentiksi tulee tällöin 100 %.

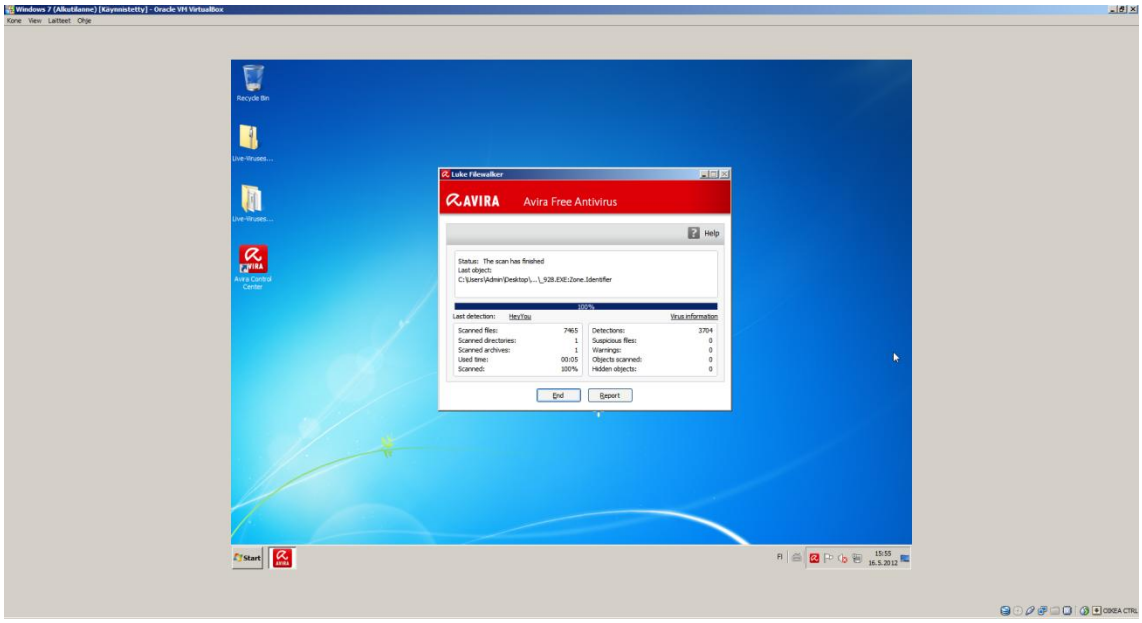
Koko järjestelmän skannaukseen aikaa kului 3min 41 sekuntia ja ohjelma käytti skannatessa yhteensä noin 40 megatavua keskusmuistia.

Koneen käynnistäminen Avgn ollessa automaattisesti käynnistyvien ohjelmien listalla kesti noin 27 sekuntia.

5.2.3 Avira AntiVir Personal – Free Antivirus v12

Muistinkäytön osalta Avira on säästäväistä tasoa. Avira lisää 5 prosessia, jotka kuluttavat yhteensä noin 21 megatavua keskusmuistia. Avira osaa pudottaa kokonaan pois käyttöliittymän prosessin, kun ohjelman käyttöliittymä ei ole avoinna työpöydällä ja tällöin muistinkäyttö on yhteensä vain noin 6 megatavua.

Haittaohjelmien tunnistamisessa Avira onnistui havaitsemaan 3704 haittaohjelmaa (Kuva 13). Tunnistamisprosentiksi tulee tällöin noin 99 %. Suoraan tunnistamisen jälkeen Avira onnistui poistamaan kaikki tunnistamansa haittaohjelmat, ilman että niitä tarvitsi ensin siirtää karanteeniin. Avira poisti haittaohjelmat erittäin nopeasti, aikaa meni noin 30 sekuntia.



Kuva 13. Windows 7 – Avira – Haittaohjelmien tunnistaminen.

Haittaohjelmien torjumisessa Avira onnistui torjumaan 9 haitallista linkkiä. Torjumisprosentiksi tulee tällöin 90 %.

Koko järjestelmän skannaukseen aikaa kului 3min 16 sekuntia ja ohjelma käytti skannatessa yhteensä noin 222 megatavua keskusmuistia.

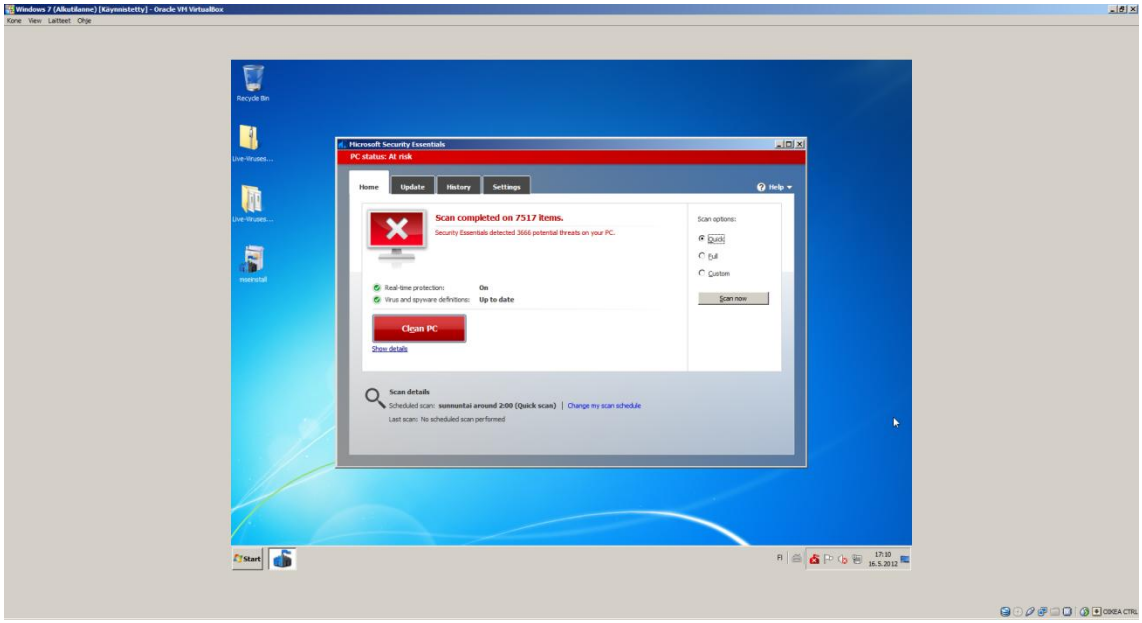
Koneen käynnistäminen Aviran ollessa automaattisesti käynnistyvien ohjelmien listalla kesti noin 24 sekuntia.

5.2.4 Microsoft Security Essentials v4

Muistinkäytön osalta Mse on säästäväistä tasoa. Mse lisää 2 prosessia, jotka kuluttavat yhteensä noin 16 megatavua keskusmuistia. Mse ei osaa pudottaa

pois käyttöliittymän prosessia, kun ohjelman käyttöliittymä ei ole avoinna työpöydällä, joten muistinkäyttö pysyy täysin samana.

Haittaohjelmien tunnistamisessa Mse onnistui havaitsemaan 3666 haittaohjelmaa (Kuva 14). Tunnistamisprosentiksi tulee tällöin noin 98 %. Suoraan tunnistamisen jälkeen Mse yritti oletuksena puhdistaa saastuneita tiedostoja, mutta epäonnistui tässä jokaisen tiedoston kohdalla. Tämän jälkeen Mse onnistui automaattisesti siirtämään karanteeniin kaikki havaitut haittaohjelmat. Mse siirsi haittaohjelmat karanteeniin suhteellisen nopeasti, aikaa meni noin minuutti.



Kuva 14. Windows 7 – Mse – Haittaohjelmien tunnistaminen.

Haittaohjelmien torjumisessa Mse onnistui torjumaan 7 haitallista linkkiä. Torjumisprosentiksi tulee tällöin 70 %.

Koko järjestelmän skannaukseen aikaa kului peräti 35min 15 sekuntia ja ohjelma käytti skannatessa yhteensä noin 33 megatavua keskusmuistia.

Koneen käynnistäminen Mse:n ollessa automaattisesti käynnistyvien ohjelmien listalla kesti noin 21 sekuntia.

5.2.5 Yhteenveto tuloksista

Taulukossa 2 listataan testin tulokset Windows 7:n osalta.

Taulukko 2. Windows 7 – Testitulokset.

Windows 7	Tunnistus %	Torjumis %	Muistinkäyttö Mt (UI on/off)	Scan time min.sec	Boot time min.sec
Avast	97	100	9/4	2.54	21
Avg	97	100	20/15	3.41	27
Avira	99	90	21/6	3.16	24
Mse	98	70	16/16	35.15	21

Haittaohjelmien tunnistamisen ja torjumisen osalta tuloksissa ei ole eroa Xp:hen verrattuna.

Muistinkäytön osalta Avast on edelleen muita edellä, mutta myös muiden ohjelmien muistinkäyttö tippuu matalalle tasolle.

Skannausajoissa Avast pysyy muita nopeampana myös Windows 7:ssä. Mse tekee tässä kohtaa poikkeuksen ja sen skannausaika on erittäin paljon muita pidempi.

Tietokoneen käynnistymiseen kuluvassa ajassa Mse ja Avast tekevät parhaan tuloksen, mutta myös muiden ohjelmien käynnistysajat paranevat.

Näiden tulosten perusteella mielestäni suositeltavin virustorjuntaohjelma Windows 7:lle olisi Avira. Windows 7:n käyttäjillä on yleensä moderni laitteisto käytössään ja tästä syystä esimerkiksi muistinkäyttö ei ole enää ihan niin määräävä ominaisuus kuin Xp:n kohdalla. Avira pärjää jokaisessa testissä tasaisesti erittäin hyvin ja täten kokonaisuutena se vaikuttaa parhaimmalta.

6 JOHTOPÄÄTÖKSET

Tämän työn testitulosten perusteella on selvää, että käyttöjärjestelmät eivät sinänsä vaikuta haittaohjelmien tunnistamiseen tai torjumiseen, koska tulokset olivat täysin samoja molemmissa käyttöjärjestelmissä. Virustorjuntaohjelma tekee siis kaiken työn tältä osin. Käytännössä muutamien prosenttien erot eivät vaikuta järin suurilta, mutta kun miettii puhtaasti lukumääriä, niin parhaiten ja huonoiten tunnistaneen ohjelman välillä on eroa 74 haittaohjelmaa. Tuollaisesta määrästä kuitenkin voi jo yksikin haittaohjelma aiheuttaa paljon harmia tietokoneen käyttäjälle, jos sellainen saastuttaa tietokoneen.

Muistinkäytön osalta sen sijaan havaittiin kautta linjan selkeää laskua Windows 7:ssä, osassa ohjelmia jopa yli puolet pienempiä lukemia verrattuna Xp:n tuloksiin. Tämä johtuu todennäköisesti Windows 7:n reilusti paremmasta muistinhallinnasta verrattuna Xp:n vastaavaan.

Skannausajat olivat kautta linjan suurempia Windows 7:ssä kuin Xp:ssä, mutta tämä johtuu aika pitkälti myös siitä, että Windows 7:n asennus vie reilusti enemmän tilaa kuin Xp:n asennus ja täten virustorjuntaohjelmilla on enemmän tiedostoja skannattavana. Suhteessa skannausajat olivat siis kuitenkin nopeita, koska Windows 7:n asennuksen koko oli yli viisinkertainen Xp:hen nähden.

Tietokoneen käynnistymisajoissa Windows 7:ssä havaittiin selkeää laskua jokaisessa testissä verrattuna Xp:n tuloksiin. Käynnistymisajat olivat noin puolet lyhyempiä jokaisen ohjelman kohdalla. Tämä johtuu Windows 7:n paremmasta tavasta käsitellä käynnistyviä palveluja ja prosesseja bootin yhteydessä.

Näissä testeissä muistinkäyttöön, skannausaikoihin ja käynnistymisaikaan vaikuttaa tietenkin myös käytössä oleva laitteisto sekä hieman myös virtualisointiohjelmiston asetukset. Suhteessa tulokset ovat kuitenkin luotettavia, koska testialusta oli joka kerralla täysin sama.

Lopuksi voidaan kuitenkin todeta, että paras turva edelleen on käyttäjä itse sekä käyttäjän tekemät valinnat ja vasta tämän jälkeen mikä tahansa sellainen

tietoturvaratkaisu, joka käyttää runsaasti erilaisia teknologioita eri tasoilla suojatakseen järjestelmää.

Työn tavoitteena oli selvittää mahdollisia eroja ja vaikutuksia käyttöjärjestelmien ja virustorjuntaohjelmien yhteistoiminnassa. Testeistä saatiin selkeät tulokset, joilla pystyi hyvin vertailemaan, minkälainen yhdistelmä olisi mahdollisesti suositeltavin. Tulevaisuudessa tietoturva ja sen kehittäminen tulee todennäköisesti olemaan entistä tärkeämpää, kun kokoajan enemmän luottamuksellisia tietoja sijaitsee erilaisissa järjestelmissä.

LÄHTEET

Adware 2012. Wikipedia. Viitattu 26.2.2012 http://en.wikipedia.org/wiki/Adware

Antivirus software 2012. Wikipedia. Viitattu 15.4.2012 http://en.wikipedia.org/wiki/Antivirus_software#Identification_methods

Avast 2012. Viitattu 19.4.2012 http://www.avast.com/en-eu/index

Avg 2012. Viitattu 23.4.2012 http://free.avg.com/ww-en/homepage

Avira 2012. Viitattu 30.4.2012 http://www.avira.com/en/index

AVS Firewall 2012. Viitattu 2.3.2012 http://onlinehelp.avs4you.com/images/Firewall/Rootkit.png

Computer virus 2012. Wikipedia. Viitattu 19.1.2012 http://en.wikipedia.org/wiki/Computer_virus

Computer worm 2012. Wikipedia. Viitattu 23.1.2012 http://en.wikipedia.org/wiki/Computer_worm

Internet Insecurity 2011a. Viitattu 19.1.2012 http://insertintelligentname.files.wordpress.com/2011/10/0704.jpg

Internet Insecurity 2011b. Viitattu 23.1.2012 http://insertintelligentname.files.wordpress.com/2011/10/diagram.jpg

Malware 2012. Wikipedia. Viitattu 10.1.2012 http://en.wikipedia.org/wiki/Malware

MSE 2012. Wikipedia. Viitattu 8.5.2012 http://en.wikipedia.org/wiki/Microsoft_Security_Essentials

Rootkit 2012. Wikipedia. Viitattu 2.3.2012 http://en.wikipedia.org/wiki/Rootkit

Spyware 2012. Wikipedia. Viitattu 17.2.2012 http://en.wikipedia.org/wiki/Spyware

Trojan horse 2012. Wikipedia. Viitattu 7.2.2012 http://en.wikipedia.org/wiki/Trojan_horse_(computing)

Trojan horse software 2006. Viitattu 7.2.2012 http://www.linux4windows.com/Articles/digital_trojan_horse_in_business_home_software.gif