ESET Glossary

Käyttöopas

Napsauta tätä jos haluat nähdä tämän asiakirjan online-version

Digital Security
Progress. Protected.

ESET Glossary -tuotteen on kehittynyt ESET, spol. s r.o.

Lisätietoja on osoitteessa https://www.eset.com.

Tekninen tuki: https://support.eset.com

REV. 12.4.2024

ESET-sanasto: Johdanto

ESET-sanasto sisältää kattavan kuvauksen nykyisistä uhkista ja ESET-tekniikoista, jotka suojaavat sinua niiltä.

Aiheet on jaettu seuraaviin kappaleihin:

- Tunnistukset – Muun muassa tietokonevirukset, madot, troijalaiset ja mahdollisesti ei-toivotut sovellukset.
- Etähyökkäykset – Uhat, jotka ovat peräisin paikallisista verkoista tai Internetistä.
- Sähköpostiuhat – Muun muassa tietojenkalastelu ja muut huijaukset.
- ESET-tekniikka – ESET-tietoturvaratkaisuissa käytettävissä olevat tuoteominaisuudet

Mainosohjelmat

Mainosohjelmat tarkoittavat mainoksin tuettuja ohjelmistoja. Mainoksia näyttävät ohjelmat kuuluvat tähän luokkaan. Mainosohjelmat avaavat usein automaattisesti mainoksia sisältäviä ponnahdusikkunoita Internet-selaimeen tai muuttavat selaimen aloitussivun. Ilmaisohjelmat sisältävät usein mainosohjelmia, jotka auttavat kehittäjiä kattamaan laatimiensa, useimmiten hyödyllisien, ohjelmistojen kehityskustannukset.

Mainosohjelmat eivät sinänsä ole vaarallisia, mutta niistä aiheutuu vaivaa käyttäjilleen. Ohjelmat ovat vaarallisia, jos niihin sisältyy vakoiluohjelmien kaltaisia seurantatoimintoja.

Jos käytät ilmaisohjelmistoja, seuraa asennusohjelman toimintaa tarkasti. Asennusohjelma ilmoittaa hyvin todennäköisesti, jos ylimääräinen mainosohjelma asennetaan. Usein mainosohjelman asentaminen voidaan peruuttaa.

Joitakin ohjelmia ei voi asentaa ilman mainosohjelmaa, tai se rajoittaa ohjelman toimintaa. Tämä tarkoittaa, että mainosohjelmat käyttävät usein järjestelmää "laillisesti", koska käyttäjä on sallinut ohjelmien toiminnan. Tässä tapauksessa on parempi pelata varman päälle. Jos tarkistus löytää tietokoneesta mainosohjelmatiedoston, se kannattaa poistaa haitallisen koodin varalta.

Bottiverkko

Botti eli web-robotti on on automaattinen haittaohjelma, joka tarkistaa estettyjä Internet-osoitteita ja tartuttaa haavoittuvaisia tietokoneita. Tämän ansiosta hakkerit pystyvät ottamaan haltuunsa useita tietokoneita samanaikaisesti ja muuttamaan ne boteiksi (tunnetaan myös zombeina). Hakkerit tartuttavat yleensä bottien avulla suuren määrän tietokoneita, jotka muodostavat sitten verkon tai bottiverkon. Kun bottiverkko on tietokoneessasi, sen kautta voidaan jakaa palvelunestohyökkäyksiä (DDoS; distributed denial of service). Välityspalvelinta käyttäen voidaan myös suorittaa automaattisia tehtäviä Internetin välityksellä ilman, että tiedät asiasta. Esimerkkejä tästä ovat roskapostin lähettäminen, virukset ja henkilökohtaisten ja yksityisten tietojen, kuten pankkitunnusten tai luottokorttinumeroiden, varastaminen.

Väärä hälytys (FP, false positive)

Realistisesti ajateltuna 100-prosenttista tunnistustarkkuutta ei voida taata. Myös puhtaiden kohteiden virheellinen luokittelu haittaohjelmiksi on aina mahdollista.

Väärä hälytys tarkoittaa puhdasta tiedostoa/sovellusta, joka luokitellaan virheellisesti haittaohjelmaksi tai mahdollisesti ei-toivotuksi sovellukseksi.

Pakkaaja

Pakkaaja on itsestään purkautuva suorituksenaikainen ohjelmatiedosto, joka kerää useita erilaisia haittaohjelmia yhteen pakettiin.

Yleisimpiä pakkaajia ovat UPX, PE_Compact, PKLite ja ASPack. Sama haittaohjelma saatetaan havaita eri tavalla, jos se on pakattu eri pakkaajalla. Pakkaajat voivat myös muuntaa "allekirjoituksiaan" ajan mittaan, mikä vaikeuttaa haittaohjelmien havaitsemista ja poistamista.

Mahdollisesti vaaralliset sovellukset

On useita laillisia ohjelmia, jotka yksinkertaistavat verkkoon liitettyjen tietokoneiden hallintaa. Niitä voidaan kuitenkin väärissä käsissä käyttää vihamielisiin tarkoituksiin. ESET voi tunnistaa tällaiset sovellukset.

Tietyt kaupalliset, lailliset ohjelmistot luokitellaan **mahdollisesti vaarallisiksi sovelluksiksi**. Tällaisia ohjelmistoja ovat muun muassa etäkäyttötyökalut, salasanojen murtamiseen käytettävät sovellukset sekä näppäinpainallukset tallentavat sovellukset.

Jos havaitset, että järjestelmässä toimii mahdollisesti vaarallinen sovellus (etkä ole asentanut sitä), ota yhteyttä verkonvalvojaan tai poista sovellus.

Mahdollisesti ei-toivotut sovellukset

Mahdollisesti ei-toivotut sovellukset (ns. Grayware-ohjelmistot) on laaja ryhmä. Siihen kuuluvat ohjelmistot, jotka poikkeavat muun tyyppisistä haittaohjelmista (kuten viruksista tai troijalaisista) siten, että niiden tarkoitus ei ole yksiselitteisesti olla haitallinen. Nämä ohjelmistot saattavat kuitenkin asentaa tarpeettomia lisäohjelmia, muuttaa digitaalisen laitteen toimintaa tai suorittaa toimia, joita käyttäjä ei ole hyväksynyt tai joita hän ei odota.

Grayware-ohjelmiksi voidaan katsoa esimerkiksi mainostusohjelmistot, latauspaketit, erinäiset selaintyökalurivit, harhaanjohtavasti toimivat ohjelmistot, pakettiohjelmistot, seurantaohjelmistot, välityspalvelinohjelmistot (Internetin jako-ohjelmistot), kryptovaluuttojen louhintaohjelmat, rekisteripuhdistajat (vain Windows-käyttöjärjestelmissä) ja muut haitallisuuden rajoja hipovat ohjelmistot tai ohjelmistot, joissa käytetään lainvastaisia tai epäeettisiä käytäntöjä (vaikka ohjelmistot vaikuttavat muuten asiallisilta) ja joita käyttäjä saattaisi pitää ei-toivottuina, jos hän olisi tietoinen siitä, mitä asennettu ohjelmisto tekee.

Mahdollisesti ei-toivottu sovellus voi olla myös itsessään laillinen (mahdollisesti myös kaupallisesti myytävä) ohjelmisto, jota hyökkääjä voi väärinkäyttää. ESET-ohjelmiston käyttäjä voi ottaa tällaisten sovellusten tunnistuksen käyttöön tai poistaa sen käytöstä.

On tilanteita, joissa käyttäjän mielestä mahdollisesti ei-toivotun sovelluksen edut ovat suuremmat kuin riskit. Tästä syystä ESET määrittää kyseiset sovellukset pienemmän riskin luokkaan verrattuna muunlaisiin haittaohjelmiin, kuten troijalaisiin tai matoihin.

- Varoitus – Löytyi mahdollisesti ei-toivottu sovellus
- Asetukset

- Ohjelmakääreet
- Rekisteripuhdistajat
- Mahdollisesti ei-toivottu sisältö

Yksityiskohtaiset ohjeet
Jos haluat tarkistaa ja poistaa mahdollisesti ei-toivotut sovellukset (PUA) ESETin kotikäyttöön tarkoitetuista Windows-tuotteista, tutustu ESET-tietopankin artikkeliin.

Varoitus – Löytyi mahdollisesti ei-toivottu sovellus

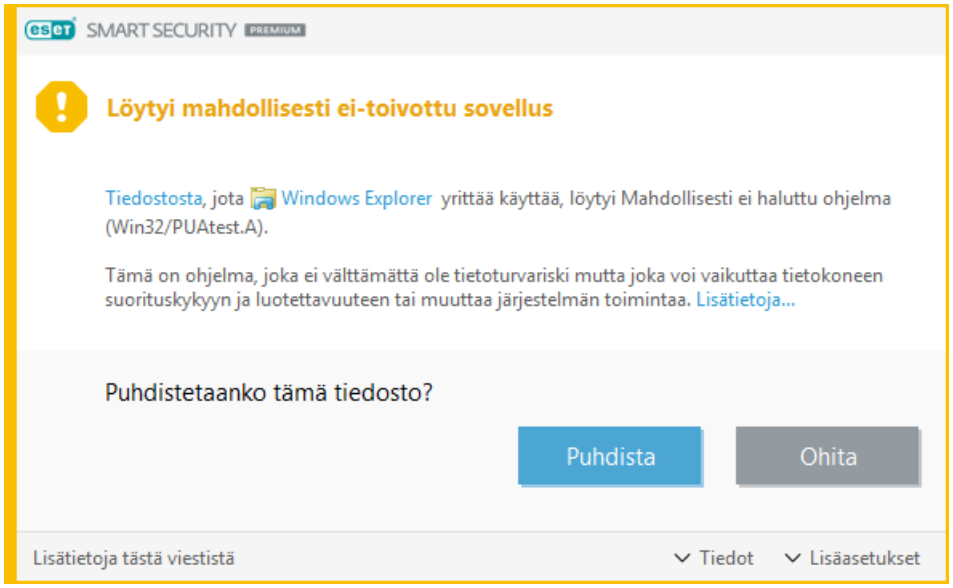
Kun mahdollisesti ei-toivottu sovellus havaitaan, voit päättää, mikä toimenpide suoritetaan:

1.**Puhdista/katkaise**: Tällä asetuksella lopetetaan toimenpide ja torjutaan mahdollisesti ei-toivotun sovelluksen pääsy järjestelmääsi.
Näet **Katkaise yhteys** -vaihtoehdon mahdollisesti ei-toivottujen sovellusten ilmoituksille verkkosivustolta ladattaessa ja **Puhdista**-vaihtoehdon levyllä olevien tiedostojen kohdalla.

2.**Ohita**: Tällä vaihtoehdolla sallitaan mahdollisesti ei-toivotun sovelluksen pääsy järjestelmääsi.

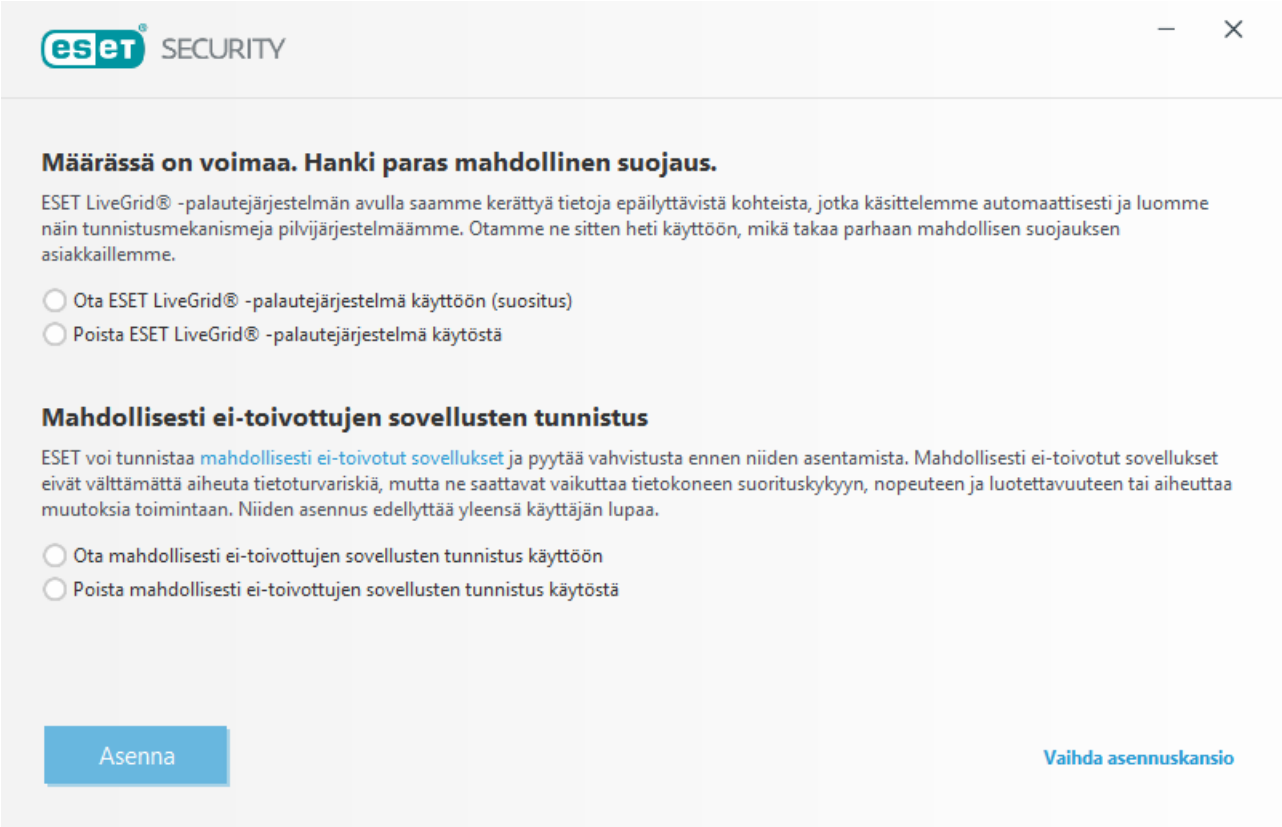
3.**Ohita havaitsemisesta**: Jos haluat sallia sovelluksen käytön koneellasi tulevaisuudessa keskeytyksettä, napsauta **Lisäasetukset** ja valitse sitten vaihtoehdon Ohita havaitsemisesta vieressä oleva **Ohita**-vaihtoehto.

4.**Jätä allekirjoitus pois havaitsemisesta**: Jos haluat sallia kaikkien tiettyä havaittua nimeä (allekirjoitusta) vastaavien tiedostojen suorittamisen tietokoneellasi jatkossa ilman keskeytyksiä (niin nykyisistä tiedostoista kuin verkon latauksistakin), valitse **Lisäasetukset**, valitse **Jätä allekirjoitus pois tunnistuksesta** ja napsauta **Ohita**. Jos tämän jälkeen näyttöön tulee lisää havaintoikkunoita, voit sulkea ne napsauttamalla Ohita (muut ikkunat liittyvät havaintoon, joka tapahtui, ennen kuin jätit allekirjoituksen pois havaitsemisesta).



Asetukset

Kun asennat ESET-tuotettasi, voit päättää, otatko mahdollisesti ei-toivottujen sovellusten havaitsemisen käyttöön alla olevan mukaisesti:



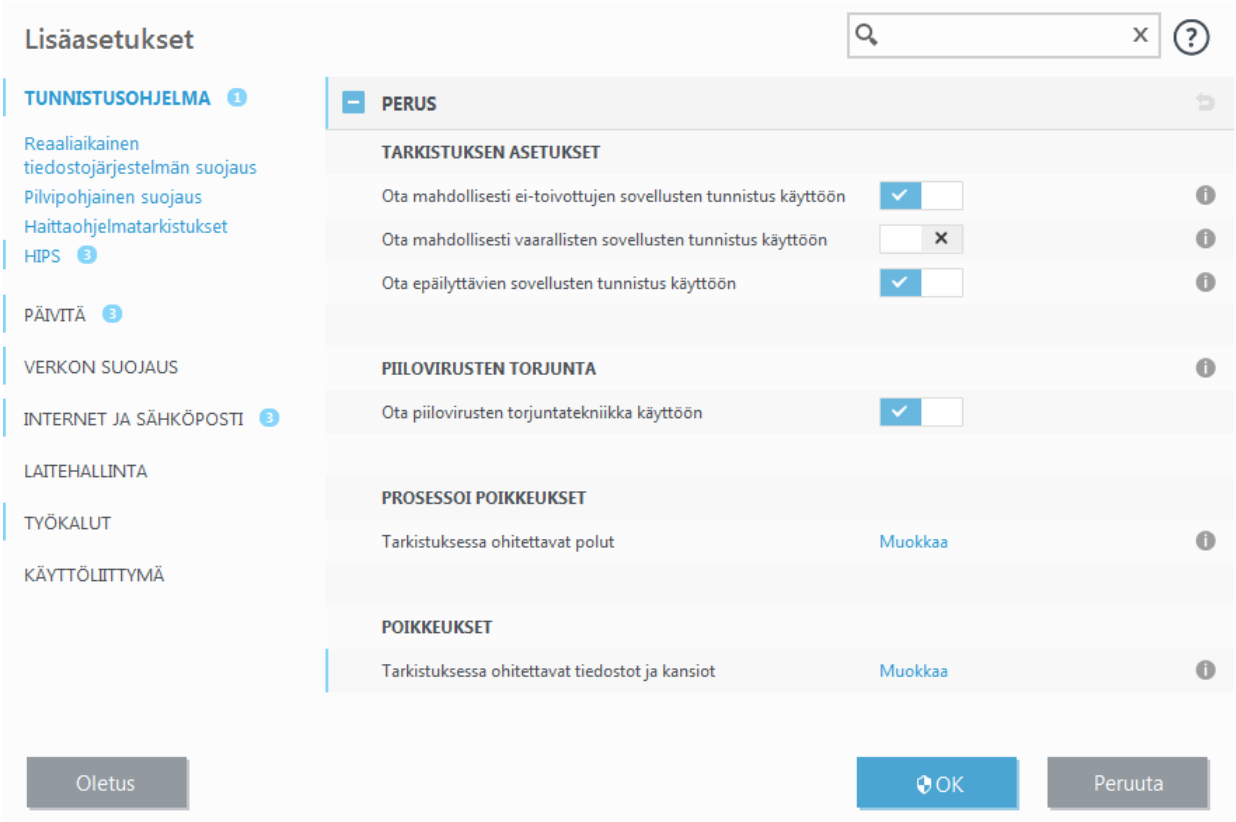
Varoitus
Mahdollisesti ei-toivotut sovellukset voivat asentaa mainoksia ja työkalupalkkeja tai niissä voi olla muita ei-toivottuja ja vaarallisia ohjelmaominaisuuksia.

Voit muokata näitä asetuksia ohjelma-asetuksissasi koska tahansa. Voit ottaa mahdollisesti epätoivottujen, vaarallisten tai epäilyttävien sovellusten havaitsemisen käyttöön tai poistaa sen käytöstä noudattamalla seuraavia ohjeita:

1. Avaa ESET-tuote.

2. Paina **F5**-näppäintä avataksesi **Lisäasetukset**.

3. Napsauta **Tunnistusohjelma**-vaihtoehtoa (aiemmissa versiossa tämä saattoi olla nimeltään **Virustentorjunta** tai **Tietokone**) ja ota käyttöön tai poista käytöstä asetukset **Ota mahdollisesti ei-toivottujen sovellusten havaitseminen käyttöön**, **Ota mahdollisesti vaarallisten sovellusten havaitseminen käyttöön** ja **Ota epäilyttävien sovellusten havaitseminen käyttöön** mielesi mukaan. Vahvista napsauttamalla **OK**.



Yksityiskohtaiset ohjeet

Tarkemmat ohjeet tuotteiden määrittämisestä tunnistamaan tai ohittamaan mahdollisesti ei-toivotut sovellukset on ESET-tietopankin artikkeleissa:

- ESET NOD32 Antivirus / ESET Internet Security / ESET Smart Security Premium
- ESET Cyber Security for macOS / ESET Cyber Security Pro for macOS
- ESET Endpoint Security / ESET Endpoint Antivirus for Windows
- ESET Mobile Security for Android

Ohjelmakääreet

Ohjelmakääre on erityinen sovellusmuunnos, jota jotkin verkkotallennustilaverkkosivut käyttävät. Se on kolmannen osapuolen työkalu, joka asentaa ohjelman, jonka halusit ladata, mutta joka lisää muita ohjelmia, kuten työkalupalkkeja ja mainosohjelmistoja. Ylimääräinen ohjelma saattaa myös tehdä muutoksia verkkoselaimesi kotisivuun ja hakuasetuksiin. Verkkotallennustilaverkkosivut eivät myöskään yleensä ilmoita ohjelman myyjälle tai latauksen vastaanottajalle, että muutoksia on tehty. Ne usein myös piilottavat vaihtoehdot, joilla muunnokset voi estää. Näistä syistä ESET luokittelee ohjelmakääreet mahdollisesti ei-toivotuiksi sovelluksiksi. Näin käyttäjillä on mahdollisuus päättää, hyväksyykö latauksen.

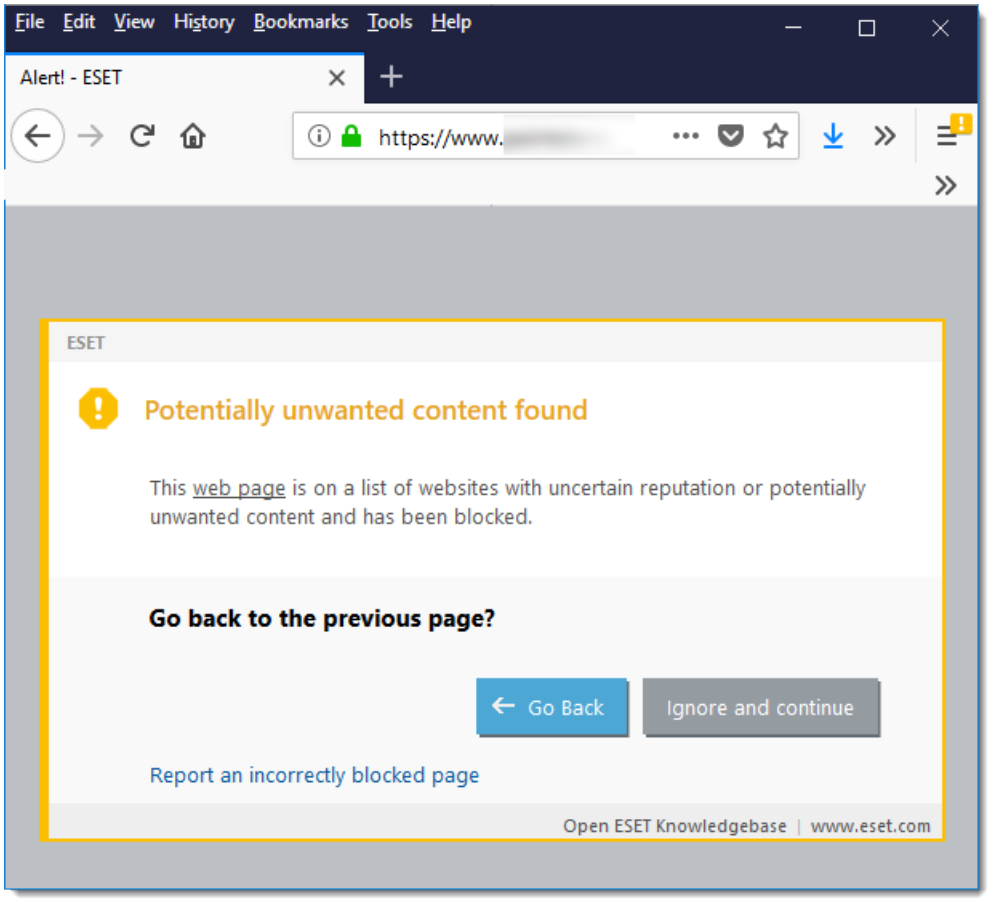
Rekisteripuhdistajat

Rekisteripuhdistajat ovat ohjelmia, jotka saattavat ehdottaa, että Windows-rekisterin tietokannalle on tehtävä huolto- tai puhdistustoimenpiteitä. Rekisteripuhdistajan käyttö voi olla riski tietokonejärjestelmälle. Lisäksi jotkin rekisteripuhdistajat esittävät epäpäteviä, vahvistamattomia tai muutoin perättömiä väitteitä eduistaan ja/tai luovat harhaanjohtavia raportteja tietokonejärjestelmästä ”ilmaisen tarkistuksen” tulosten perusteella. Tällaisten harhaanjohtavien väitteiden ja raporttien tarkoitus on houkutella käyttäjää ostamaan ohjelman täysi versio tai tekemään tilaus siitä, yleensä ilman mahdollisuutta arvioida rekisteripuhdistajaa ennen maksua. Näistä syistä ESET luokittelee tällaiset ohjelmat mahdollisesti ei-toivotuiksi sovelluksiksi ja antaa käyttäjän päättää, sallitaanko

tai estetäänkö ne.

Mahdollisesti ei-toivottu sisältö

Jos mahdollisesti ei-toivottujen sovellusten tunnistus on käytössä ESET-tuotteessa, sivustot, jotka tunnetaan mahdollisesti ei-toivottujen sovellusten tyrkyttäjinä tai käyttäjien harhauttamisesta tekemään järjestelmää tai selauskokemusta mahdollisesti haittaavia toimia, estetään mahdollisesti haitallisena sisältönä. Jos saat ilmoituksen, että sivusto on luokiteltu mahdollisesti haitalliseksi sisällöksi, voit siirtyä pois estetyltä verkkosivulta valitsemalla **Siirry takaisin** tai antaa sivuston latautua valitsemalla **Ohita ja jatka**.



Lisätietoja tästä aiheesta on tässä ESET-tietopankin artikkelissa.

Kiristysohjelma

Kiristysohjelmat (eli tiedostojen salausohjelmat) on haittaohjelmia, jotka lukitsevat laitteen tai salaavat sen sisällön ja kiristävät käyttäjältä sitten rahaa, jotta sisällön käyttömahdollisuus palautetaan. Tällaisissa haittaohjelmissa voi myös olla sisäinen ajastin ja esiohjelmoitu maksupäivä, johon mennessä uhrin on tehtävä maksu. Jos vaatimuksiin ei suostuta tähän päivään mennessä, hinta kasvaa tai laitteen käyttö estetään.

Kun laite saa tartunnan, tiedostojen salausohjelma saattaa yrittää salata laitteen jaetut asemat. Tästä voi saada sellaisen käsityksen, että haittaohjelma leviäisi verkossa, mutta näin ei ole. Tämä tilanne tapahtuu, kun tiedostopalvelimen jaettu asema salataan mutta itse palvelimella ei ole haittaohjelmatartuntaa (ellei kyseessä ole päätepalvelin).

Kiristysohjelmien laatijat luovat avainparin, joka sisältää julkisen ja yksityisen avaimen, ja lisäävät julkisen avaimen haittaohjelmaan. Itse kiristysohjelma voi olla osa troijalaista tai vaikuttaa tavalliselta tiedostolta tai kuvalta, joka

lähetetään uhrille sähköpostitse, sosiaalisessa verkostossa tai pikaviestipalvelun avulla. Kun haittaohjelma on päässyt tietokoneelle, se luo satunnaisen symmetrisen avaimen ja salaa laitteella olevat tiedot. Haittaohjelman julkista avainta käytetään symmetrisen avaimen salaamiseen. Tämän jälkeen kiristysohjelma vaatii maksua tietojen salauksen purkamiseksi. Maksua vaativassa viestissä, joka näkyy laitteessa, saatetaan varoittaa perättömästi, että järjestelmää on käytetty laittomiin toimiin tai että se sisältää laitonta sisältöä. Kiristysohjelman uhria pyydetään maksamaan vaadittu summa jollakin maksutavalla. Maksutavat perustuvat yleensä hankalasti jäljitettävissä oleviin maksutapoihin, kuten digitaalisiin kryptovaluuttoihin, maksullisiin SMS-viesteihin tai ennalta maksettuihin maksukortteihin. Maksun saamisen jälkeen kiristysohjelman tekijän on määrä käyttää yksityistä avaintaan symmetrisen avaimen ja käyttäjän tietojen salauksen purkamiseen. Tätä ei kuitenkaan taata.

> **Lisätietoja kiristysohjelmasuojauksesta**
>
> ESETin tuotteissa käytetään monitahoisia tekniikoita laitteiden suojaamiseen kiristysohjelmia vastaan. ESET-tietopankin artikkelissa on kuvattu parhaat toimintatavat, joilla voit suojata järjestelmääsi kiristysohjelmilta.

Rootkit-ohjelmat

Rootkit-ohjelmat ovat vihamielisiä ohjelmia, jotka myöntävät Internet-hyökkääjille rajattoman järjestelmän käyttöoikeuden ja samalla salaavat niiden olemassaolon. Järjestelmää käytettyään (yleensä järjestelmän heikkoutta hyödyntäen) rootkit-ohjelmat käyttävät käyttöjärjestelmän toimintoja välttääkseen virustentorjuntaohjelmien tunnistuksen: ne piilottavat prosesseja, tiedostoja ja Windowsin rekisteritietoja. Tästä syystä niiden havaitseminen tavallisilla testaustekniikoilla on lähes mahdotonta.

Rootkit-ohjelmia estäviä tunnistamisen tasoja on kaksi:

1. Kun se yrittää käyttää järjestelmää: Se ei ole vielä läsnä ja näin ollen on passiivinen. Useimmat virustentorjuntaohjelmat voivat poistaa rootkit-ohjelmia tällä tasolla (olettaen, että ne tunnistavat kyseisen tiedoston saaneen tartunnan).

2. Kun se on piilotettu tavalliselta testaamiselta: ESET-käyttäjillä on käytössään piilovirusten torjuntatekniikka, joka kykenee myös havaitsemaan ja poistamaan aktiivisia rootkit-ohjelmia.

ROP-hyökkäykset

ROP-hyökkäys (Return-oriented programming) on tavallinen koodin uudelleenkäyttöhyökkäys, jossa hyökkääjä kohdistaa järjestelmään haitallisia hallintatoimia nykyisen koodin kautta. ROP-hyökkäys on kehittynyt versio puskurin ylivuotohyökkäyksestä, jossa ohjelma kirjoittaa tarkoitetun datarakenteen ulkopuoliseen muistiosoitteeseen yleensä kiinteäpituista puskuria käyttämällä.

ROP on haavoittuvuuden hyödyntämistekniikka, jolla voidaan suorittaa koodia kohdejärjestelmässä. Ottamalla kutsupinon haltuunsa hyökkääjä voi ohjata tietokoneella suoritettavien nykyisten luotettujen ohjelmistojen toimintaa ja saada ne tekemään muita kuin toivottuja toimia.

Vakoiluohjelmat

Tämä luokka kattaa kaikki sovellukset, jotka lähettävät yksityisiä tietoja ilman käyttäjän hyväksyntää/tietoa. Vakoiluohjelmat käyttävät seurantatoimintoja lähettämään erilaisia tilastotietoja, kuten vierailtujen sivustojen luettelon, käyttäjän yhteystietoluettelon sähköpostiosoitteet tai tallennettujen näppäilyjen luettelon.

Vakoiluohjelmistojen laatijat väittävät usein, että näitä tekniikoita käytetään ottamaan selvää käyttäjien tarpeista ja kiinnostuksen kohteista, jolloin mainostuksen kohdentaminen paranee. Ongelmana on se, ettei hyödyllisen ja vihamielisen sovelluksen ero ole selkeä eikä kukaan voi olla varma, etteikö haettuja tietoja käytetä väärin. Vakoiluohjelmiston hankkimat tiedot voivat olla turvakoodeja, PIN-numeroita, pankkitilinumeroita ja niin edelleen. Vakoiluohjelmisto liitetään usein ohjelman ilmaisversioon, jotta se loisi liikevaihtoa tai toimisi houkutteena ostaa ohjelmisto. Käyttäjille ilmoitetaan usein vakoiluohjelmiston mukanaolosta asennuksen aikana, jotta hän päivittäisi maksulliseen versioon, jossa vakoiluohjelmistoa ei ole.

Tunnettuja freeware-tuotteita, joissa on vakoiluohjelmistoa, ovat vertaisverkkosovellukset. Spyfalcon tai Spy Sheriff (ja useat muut) kuuluvat erityiseen vakoiluohjelmaluokkaan – ne vaikuttavat olevan vakoiluohjelmiston torjuntaohjelmia, mutta ovat itse asiassa itse vakoiluohjelmia.

Jos tietokoneessa oleva tiedosto tunnistetaan vakoiluohjelmaksi, se kannattaa poistaa. On erittäin todennäköistä, että se sisältää haitallista koodia.

Eräs vakoiluohjelma, näppäilyntallennussovellus, voi olla laitteisto- tai ohjelmistopohjainen. Ohjelmistopohjaiset näppäilyntallennussovellukset voivat kerätä vain yhdelle verkkosivustolle tai sovellukselle kirjoitettuja tietoja. Kehittyneemmät näppäilyntallennussovellukset voivat tallentaa kaiken kirjoittamasi, mukaan lukien kopioidut/liitetyt tiedot. Jotkin mobiililaitteisiin kohdistetut näppäilyntallennussovellukset voivat tallentaa puheluita, viestisovellusten tietoja, sijainteja tai jopa mikrofonin ääntä ja kameran kuvaa.

Troijalainen

Perinteisesti troijalaiset on luokiteltu uhiksi, jotka yrittävät vaikuttaa hyötyohjelmilta ja saada käyttäjä suorittamaan ne.

Koska troijalaisten luokka on hyvin laaja, se usein jaetaan useaan alaluokkaan:

- Lataaja – vihamielinen ohjelma, joka voi ladata muita uhkia Internetistä.
- Kantaja – vihamielinen ohjelma, joka on määritetty jättämään muunlaista haittaohjelmistoa altistuneeseen tietokoneeseen.
- Takaportti – vihamielinen ohjelma, joka on yhteydessä mahdollisesti tietokoneeseen pääsevän ja sen hallintaansa ottavan etähyökkääjän kanssa.
- Näppäintallennussovellus – ohjelma, joka tallentaa käyttäjän jokaisen näppäilyn ja lähettää tiedot etähyökkääjille.
- Numeronvalitsin – vihamielinen ohjelma, joka on suunniteltu muodostamaan yhteys maksullisiin puhelinnumeroihin käyttäjän Internet-palveluntarjoajan sijaan. Käyttäjän on lähes mahdotonta huomata, että uusi yhteys on muodostettu. Numeronvalitsimet voivat vahingoittaa vain modeemikäyttäjiä, joiden määrä on nykyään laskussa.

Jos tietokoneessa oleva tiedosto tunnistetaan troijalaiseksi, se kannattaa poistaa, koska se hyvin todennäköisesti sisältää pelkästään vihamielistä koodia.

Virus

Tietokonevirus on osa haitallista koodia, joka on lisätään tai liitetään tietokoneessa oleviin tiedostoihin. Virukset ovat saaneet nimensä biologisista viruksista, koska niiden leviämistapa on samankaltainen. Termiä "virus"

käytetään usein virheellisesti kuvaamaan kaikenlaisia uhkia. Nykyään käyttöön on kuitenkin yleistymässä tarkempi termi "haittaohjelma".

Tietokonevirukset hyökkäävät lähinnä suoritettaviin tiedostoihin ja asiakirjoihin. Seuraavassa on lyhyt kuvaus tietokoneviruksen toiminnasta: Kun tartunnan saanut tiedosto suoritetaan, haitallista koodia kutsutaan ja se suoritetaan ennen alkuperäisen sovelluksen suorittamista. Virus voi tartuttaa mitä tahansa tiedostoja, joihin käyttäjällä on kirjoitusoikeudet.

Tietokonevirusten tarkoitus ja vakavuus vaihtelevat. Jotkin niistä ovat erittäin vaarallisia, koska ne voivat tarkoituksella poistaa tiedostoja kiintolevyltä. Toiset virukset taas eivät aiheuta mitään varsinaista vahinkoa, ne vain haittaavat käyttäjää ja toimivat laatijansa teknisten taitojen osoituksena.

Jos tietokoneessa on virustartunta, jota ei voida puhdistaa, voit lähettää sen ESETin tutkimuslaboratorioon tarkasteltavaksi. Joissakin tapauksissa tartunnan saaneita tiedostoja on voitu muokata siten, ettei niitä voi puhdistaa, vaan tiedostot on korvattava uusilla, puhtailla kopioilla.

Mato

Tietokonemato on ohjelma, joka sisältää haitallista koodia. Madot hyökkäävät isäntäkoneisiin ja leviävät verkon välityksellä. Perustavin ero viruksen ja madon välillä on se, että madot osaavat lisääntyä itsekseen - ne eivät tarvitse isäntätiedostoa (tai käynnistyssektoria). Madot leviävät yhteystietoluettelossa olevien sähköpostiosoitteiden kautta tai hyödyntävät verkkosovellusten tietoturvassa olevia haavoittuvuuksia.

Madot ovat tästä syystä tehokkaampia kuin tietokonevirukset. Internetin laajan levinneisyyden vuoksi madot voivat levitä kaikkialle maailmaan muutamassa tunnissa - jopa minuuteissa - niiden syntymisestä. Tämä kyky lisääntyä itsenäisesti ja nopeasti tekee niistä vaarallisempia kuin muunlaiset haittaohjelmat.

Järjestelmässä aktivoitu mato voi aiheuttaa monenlaisia haittoja: se voi poistaa tiedostoja, heikentää järjestelmän suorituskykyä tai jopa poistaa ohjelmia käytöstä. Tietokonemadon luonne tekee siitä erinomaisen kuljetusvälineen muunlaisille tunkeutumisille.

Jos tietokoneessa on mato, tartunnan saaneet tiedostot kannattaa poistaa, koska niissä on hyvin todennäköisesti haitallista koodia.

Tunnistetietojen täyttö

Tunnistetietojen täyttöhyökkäys on kyberhyökkäys, joka käyttää tunnistetietokannoista vuotaneita tietoja. Hyökkääjät käyttävät botteja ja muita automatisointimenetelmiä ja yrittävät kirjautua lukuisille eri verkkosivustotileille vuotaneiden tietojen avulla. Hyökkääjien kohteena ovat erityisesti käyttäjät, jotka kierrättävät samoja tunnistetietoja useilla verkkosivustoilla ja useissa palveluissa. Kun hyökkäys onnistuu, hyökkääjä voi saada täydet oikeudet tilille ja sille tallennettuihin käyttäjän tietoihin. Hyökkääjät voivat näitä oikeuksia hyödyntämällä varastaa henkilötietoja ja käyttää niitä identiteettivarkauksiin, maksupetoksiin, roskapostin jakamiseen ja muihin haitallisiin toimiin.

DNS Poisoning

DNS Poisoning -hyökkäyksessä hyökkääjä pyrkii harhauttamaan tietokoneen DNS-palvelimen tulkitsemaan keksityt tiedot aidoiksi. Keksityt tiedot tallennetaan välimuistiin tietyksi ajaksi, jolloin hyökkääjä voi kirjoittaa IP-osoitteiden DNS-vastauksia uudelleen. Näin käyttäjät saadaan lataamaan Internetistä alkuperäisen sisällön sijaan

viruksia tai matoja.

DoS-hyökkäys

DoS- tai palvelunestohyökkäyksellä pyritään estämään käyttäjiä käyttämästä tiettyä tietokonetta tai verkkoa. Tiedonsiirto hyökkäyksen kohteeksi joutuneiden käyttäjien välillä estetään, eikä järjestelmä toimi oikein. DoS-hyökkäyksen kohteeksi joutuneet tietokoneet on yleensä käynnistettävä uudelleen, jotta ne toimisivat oikein.

Useimmiten hyökkäyksien kohteita ovat web-palvelimet. Hyökkäyksien tarkoituksena on poistaa ne käyttäjien käytöstä tietyksi ajaksi.

ICMP-hyökkäys

ICMP (Internet Control Message Protocol) on suosittu, laajalti käytössä oleva Internet-protokolla. Se on ensisijaisesti verkkotietokoneiden käyttämä ratkaisu erilaisten virheilmoitusten lähettämiseen.

Etähyökkääjät yrittävät hyödyntää ICMP-protokollan heikkouksia. ICMP-protokolla on suunniteltu yhdensuuntaiseen tiedonsiirtoon, jossa ei vaadita todennusta. Tämä antaa etähyökkääjille mahdollisuuden käynnistää DoS- (Denial of Service) eli palvelunestohyökkäyksiä tai hyökkäyksiä, joissa luvattomat käyttäjät pääsevät käsiksi saapuviin ja lähteviin paketteihin.

ICMP-hyökkäyksen tyypillisiä muotoja ovat ping-kuormitushyökkäys (ping flood), ICMP_ECHO-kuormitushyökkäys ja Smurf-hyökkäys. ICMP-hyökkäyksen kohteeksi joutuneet tietokoneet hidastuvat merkittävästi (tämä koskee kaikkia Internetiä käyttäviä sovelluksia) ja niillä on Internet-yhteyden muodostamiseen liittyviä ongelmia.

Portin tutkiminen

Portin tutkimisella selvitetään, mitkä tietokoneen portit ovat avoinna verkkoisännässä. Portintutkija on ohjelmisto, joka on suunniteltu löytämään tällaiset portit.

Tietokoneen portti on virtuaalinen piste, joka käsittelee saapuvaa ja lähtevää tietoa. Tämä on erityisen tärkeää suojauksen kannalta. Suuressa verkossa portintutkijoiden keräämät tiedot voivat auttaa tunnistamaan mahdollisia heikkouksia. Tällainen käyttö on laillista.

Hakkerit käyttävät portin tutkimista usein tietoturvan heikentämiseen. Ensin he lähettävät paketteja kuhunkin porttiin. Vastaustyypin perusteella voidaan päätellä, mitkä portit ovat käytössä. Tutkiminen ei aiheuta vahinkoa, mutta tämä saattaa paljastaa mahdollisia heikkouksia ja sallia hyökkääjien saada etätietokoneita hallintaansa.

Verkonvalvojia kehotetaan estämään kaikki käyttämättömät portit ja suojaamaan käytössä olevat portit luvattomalta käytöltä.

SMB-välitys

SMB Relay ja SMB Relay 2 ovat erityisohjelmia, jotka voivat hyökätä etätietokoneita vastaan. Ohjelmat hyödyntävät NetBIOSin Server Message Block (palvelinviestilohko) -tiedostojakoprotokollaa. Jos käyttäjä jakaa kansion tai hakemiston lähiverkossa, hän todennäköisesti käyttää tätä tiedostonjakoprotokollaa.

Salasananippuja vaihdetaan usein paikallisverkkoliikenteessä.

SMB Relay vastaanottaa tietoliikenteen UDP-porteissa 139 ja 445, välittää asiakkaan ja palvelimen vaihtamat paketit ja muokkaa niitä. Kun yhteys on muodostettu ja todennettu, asiakkaan yhteys katkaistaan. SMB Relay luo uuden virtuaalisen IP-osoitteen. Uusi osoite voidaan tarkistaa komennolla "net use \\192.168.1.1". Windows-verkkotoiminnot voivat käyttää osoitetta. SMB Relay välittää SMB-protokollaliikenteen neuvottelua ja todennusta lukuun ottamatta. Etähyökkääjät voivat käyttää IP-osoitetta, kun asiakaskone on muodostanut yhteyden.

SMB Relay 2 toimii samalla periaatteella kuin SMB Relay, paitsi että se käyttää NetBIOS-nimiä IP-osoitteiden sijaan. Molemmat voivat toteuttaa "välikäsihyökkäyksiä". Näissä hyökkäyksissä etähyökkääjät voivat lukea, lisätä tai muokata tietoliikenteen päätepisteiden välisiä viestejä huomaamatta. Tälle hyökkäykselle altistuneet tietokoneet lopettavat usein toimintansa tai käynnistyvät uudelleen odottamatta.

Vältä hyökkäyksiä käyttämällä todennussalasanoja tai -avaimia.

TCP-desynkronointi

TCP-desynkronointi on TCP Hijacking -hyökkäyksissä käytettävä tekniikka. Se käynnistetään prosessilla, jossa saapuvien pakettien järjestysnumero poikkeaa odotetusta järjestysnumerosta. Paketit, joilla on odottamaton järjestysnumero, hylätään (tai tallennetaan puskurimuistiin, jos ne ovat mukana senhetkisessä tietoliikennejaksossa).

Desynchronization-menetelmässä tietoliikenteen päätepisteet hylkäävät vastaanotetut paketit, jolloin etähyökkääjä voi tunkeutua ja lähettää paketteja, joissa on oikea järjestysnumero. Hyökkääjät voivat jopa käsitellä tietoliikennettä tai muokata sitä.

TCP-kaappaushyökkäysten tavoitteena on keskeyttää palvelin-asiakas- tai vertaiskonetietoliikenne. Monet hyökkäykset voidaan estää käyttämällä todennusta jokaisessa TCP-segmentissä. Kannattaa myös käyttää verkkolaitteiden suositeltavia määrityksiä.

Matohyökkäys

Tietokonemato on ohjelma, jossa on vihamielistä koodia ja joka hyökkää isäntäkoneeseen ja leviää verkon välityksellä. Verkkomadot hyödyntävät eri sovellusten suojausaukkoja. Internetin levinneisyyden vuoksi madot voivat levitä kaikkialle maailmaan muutamassa tunnissa niiden syntymisestä.

Useimmat matohyökkäykset (Sasser, SqlSlammer) voidaan välttää käyttämällä palomuurin oletusasetuksia tai estämällä suojaamattomat ja käyttämättömät portit. Käyttöjärjestelmä tulee myös pitää päivitettynä uusimmilla suojauspäivityksillä.

ARP Cache Poisoning

ARP-protokolla (Address Resolution Protocol) suorittaa muunnoksia siirtoyhteyskeskuksessa (MAC-osoitteet) ja verkkotasolla (IP-osoitteet) olevien osoitteiden välillä. ARP Cache Poisoning -hyökkäyksen avulla hyökkääjät voivat seurata verkkolaitteiden välistä viestintää vääristämällä verkon ARP-taulukoita (MAC-IP-laitekartoitukset).

Hyökkääjä lähettää väärän ARP-vastaussanoman oletusverkkoyhdyskäytävään ilmoittaen, että MAC-osoite liittyy toisen kohteen IP-osoitteeseen. Kun oletusyhdyskäytävä vastaanottaa tämän sanoman ja lähettää muutokset kaikkiin muihin verkon laitteisiin, kaikki kohteen liikenne muihin verkkolaitteisiin kulkee hyökkääjän tietokoneen kautta. Tämän avulla hyökkääjä voi tarkkailla tai muokata liikennettä ennen sen välittämistä aiottuun määränpäähän.

Sähköpostiuhat

Sähköposti on nykyaikainen viestintäväline, jolla on monia etuja.

Nimettömän luonteensa vuoksi sähköposti ja Internet antavat valitettavasti mahdollisuuksia myös rikolliseen toimintaan, kuten roskapostiviestien lähettämiseen. Roskapostia ovat muun muassa tarpeettomat mainokset, huijaukset ja haitallisia ohjelmia (haittaohjelmia) levittävät viestit. Käyttäjälle aiheutuvaa haittaa ja vaaraa lisää se, että roskapostin lähettäminen on lähes ilmaista ja että roskapostin laatijoiden on helppo hankkia itselleen uusia sähköpostiosoitteita. Roskapostin määrää ja muotoja on lisäksi erittäin vaikeata säännellä. Mitä pidempään sähköpostiosoitetta käytetään, sitä todennäköisemmin se joutuu roskapostimoduulin tietokantaan.

Joitakin ohjeita ongelmien estämiseksi:

- Jos mahdollista, älä julkaise sähköpostiosoitettasi Internetissä.
- Anna sähköpostiosoitteesi vain luotettaville henkilöille.
- Jos mahdollista, älä käytä yleisiä tunnuksia. Mitä monimutkaisempi tunnus on, sitä epätodennäköisemmin sitä seurataan.
- Älä vastaa Saapuneet-kansioon saapuneeseen roskapostiin.
- Ole varovainen, kun täytät Internet-lomakkeita. Varo erityisesti valintaruutuja, kuten ”Kyllä, haluan vastaanottaa tietoja".
- Käytä sähköpostiosoitteita tarkoituksen mukaan, esimerkiksi yhtä työasioihin ja toista yhteydenpitoon ystävien kanssa.
- Vaihda sähköpostiosoitteesi aika ajoin
- Käytä roskapostinestoratkaisua.

Mainokset

Internet-mainonta on yksi nopeimmin kasvavista mainostamistavoista. Sen tärkeimpiä etuja ovat olemattomat kustannukset ja suora yhteys kohderyhmään. Lisäksi viestit välitetään kohderyhmälle lähes heti. Useat yritykset käyttävät sähköpostimarkkinointia yhteydenpitovälineenä nykyisten ja mahdollisten uusien asiakkaiden kanssa.

Tällainen mainostaminen on hyväksyttyä, koska käyttäjä voi haluta kaupallisia tietoja joistakin tuotteista. Monet yritykset lähettävät kuitenkin valtavia määriä ei-toivottuja kaupallisia viestejä. Sellaisissa tapauksissa on kyse sähköpostimarkkinoinnin sijaan roskapostista.

Ei-toivotusta sähköpostista on tullut ongelma, ja sen määrä kasvaa koko ajan. Ei-toivottujen sähköpostiviestien laatijat yrittävät usein naamioida roskapostiviestit hyväksyttäviksi viesteiksi.

Huijaukset

Huijauksella tarkoitetaan Internetissä leviävää väärää tietoa. Huijauksia levitetään yleensä sähköpostin tai esimerkiksi ICQ:n ja Skypen välityksellä. Itse viesti on usein vitsi tai urbaani legenda.

Tietokonevirushuijaukset pyrkivät levittämään pelkoa, epävarmuutta ja epäluuloja vastaanottajien joukossa. Vastaanottajat saadaan uskomaan, että verkossa leviää "tunnistamattomissa oleva virus", joka poistaa tiedostoja ja hankkii salasanoja tai suorittaa joitakin muita haitallisia toimenpiteitä järjestelmässä.

Joissakin huijauksissa vastaanottajia pyydetään lähettämään viesti edelleen ystävilleen, mikä pitää huijausta elossa. Huijaukset voivat olla esimerkiksi matkapuhelinhuijauksia tai avunpyyntöjä, mutta sinulle voidaan myös luvata lähettää rahaa ulkomailta. Useimmissa tapauksissa huijauksen alkuunpanijan tarkoitusperiä ei voi selvittää.

Jos näet viestin, jossa sinua kehotetaan lähettämään se kaikille tuntemillesi ihmisille, kyseessä voi hyvinkin olla huijaus. Internetissä on monia sivustoja, joista voi tarkistaa sähköpostiviestien luotettavuuden. Jos epäilet viestin olevan huijaus, hae siitä Internetistä tietoja, ennen kuin lähetät sen eteenpäin.

Tietojenkalastelu

Tietojenkalastelu tarkoittaa rikollista toimintaa, jossa käytetään sosiaalista manipulointia (manipuloidaan käyttäjiä, jotta saadaan selville luottamuksellisia tietoja). Sen tavoitteena on saada selville luottamuksellisia tietoja, kuten tilinumeroita, PIN-koodeja ja niin edelleen.

Käyttöoikeus saadaan yleensä lähettämällä sähköpostiviesti, joka vaikuttaa olevan peräisin luotettavalta henkilöltä tai organisaatiolta (esimerkiksi rahalaitokselta tai vakuutusyhtiöltä). Sähköpostiviesti voi näyttää hyvin aidolta ja siinä on grafiikkaa ja sisältöä, joka voi olla peräisin lähteestä, jota matkitaan. Käyttäjää pyydetään eri syistä (tietojen vahvistus, rahoitustoiminnot) antamaan henkilötietoja, kuten pankkitilinumeroita tai käyttäjänimiä ja salasanoja. Kaikki tällaiset lähetetyt tiedot on helppo varastaa tai käyttää väärin.

Pankit, vakuutusyhtiöt ja muut lailliset yritykset eivät koskaan pyydä käyttäjätunnuksia ja salasanoja sähköpostitse.

Roskapostin tunnistaminen

Voit tunnistaa postilaatikossasi olevan roskapostin (ei-toivotut sähköpostiviestit) yleensä muutaman tunnusmerkin perusteella. Jos viesti täyttää ainakin muutaman seuraavista ehdoista, se on todennäköisesti roskapostiviesti.

- Lähettäjän sähköpostiosoite ei kuulu kenellekään yhteystietoluettelossa olevalle henkilölle.
- Sinulle tarjotaan suuri summa rahaa, mutta sinun on ensin maksettava pieni summa.
- Sinua pyydetään erilaisin verukkein (tietojen tarkistus, talousasiat) antamaan henkilökohtaiset tietosi, kuten tilinumerosi, käyttäjänimesi ja salasanasi.
- Viesti on kirjoitettu vieraalla kielellä.
- Sinua pyydetään ostamaan tuote, josta et ole kiinnostunut. Jos haluat kuitenkin ostaa sen, varmista, että viestin lähettäjä on luotettava toimittaja (ota yhteyttä tuotteen alkuperäiseen valmistajaan).
- Jotkin sanat on kirjoitettu roskapostisuodattimen harhauttamiseksi väärin, esimerkiksi ”vaigra” viagran sijaan.

Säännöt

Roskapostiratkaisujen ja sähköpostiohjelmien yhteydessä sääntöjen avulla voidaan käsitellä sähköpostitoimintoja. Niissä on kaksi loogista osaa:

1.Ehto (esimerkiksi tietystä osoitteesta saapuva sähköpostiviesti, jolla on tietty otsikko)

2.Toiminto (kuten viestin poistaminen tai siirtäminen tiettyyn kansioon).

Sääntöjen määrä ja sääntöjen yhdistelmä määräytyy roskapostiratkaisun mukaan. Nämä säännöt toimivat roskapostin (ei-toivotun sähköpostin) torjuntakeinoina. Tavallisia esimerkkejä:

1. Ehto: Saapuvassa sähköpostiviestissä on sanoja, jotka tavallisesti esiintyvät roskapostiviesteissä
2. Toimenpide: Poista viesti

1. Ehto: Saapuvassa sähköpostiviestissä on liite, jonka tunniste on .exe
2. Toimenpide: Poista liite ja välitä viesti postilaatikkoon

1. Ehto: Saapuva viesti tulee työnantajalta
2. Toimenpide: Siirrä viesti Työ-kansioon

Jotta voit helpottaa hallintaa ja suodattaa roskapostia tehokkaasti, suosittelemme, että käytät sääntöjen yhdistelmiä roskapostinesto-ohjelmissa.

Sallittujen osoitteiden luettelo

Sallittujen osoitteiden luettelo on luettelo kohteista tai henkilöistä, jotka on hyväksytty tai joille on myönnetty käyttöoikeus. Sähköpostin sallittujen osoitteiden luettelo -termillä tarkoitetaan luetteloa yhteyshenkilöistä, joilta käyttäjä haluaa vastaanottaa viestejä. Sallittujen osoitteiden luettelot perustuvat avainsanoihin, joita etsitään sähköpostiosoitteista, toimialueista tai IP-osoitteista.

Jos sallittujen osoitteiden luettelo toimii "poistavassa tilassa", muista osoitteista, toimialueista tai IP-osoitteista ei oteta vastaan viestejä. Jos luettelo ei ole poistava, näitä viestejä ei poisteta, mutta ne suodatetaan jollain muulla tavalla.

Sallittujen osoitteiden luettelo toimii päinvastoin kuin estettyjen osoitteiden luettelo. Sallittujen osoitteiden luetteloa on helppo ylläpitää, samaten kuin estettyjen osoitteiden luetteloa. Roskapostiviestit voidaan suodattaa mahdollisimman tehokkaasti, kun käytetään sekä estettyjen että sallittujen osoitteiden luetteloa.

Estettyjen osoitteiden luettelo

Estettyjen osoitteiden luettelo on eräänlainen "musta lista". Se on tekniikka, joka sallii sähköpostiviestien vastaanottamisen luetteloon kuulumattomilta henkilöiltä.

Kahdenlaisia estettyjen osoitteiden luetteloja on olemassa: käyttäjien roskapostinestosovelluksessaan luomia luetteloja ja aiheeseen erikoistuneiden tahojen ammattimaisesti ja säännöllisesti ylläpitämiä estettyjen osoitteiden luetteloja, joita on saatavana Internetistä.

Estettyjen osoitteiden luettelon käyttäminen on tärkeä tekijä roskapostinsuodatuksessa. Luettelojen ylläpitäminen on kuitenkin erittäin vaikeaa, sillä uusia estettäviä kohteita esiintyy joka päivä. On suositeltavaa käyttää sekä sallittujen että estettyjen osoitteiden luetteloja roskapostin tehokasta suodattamista varten.

Poikkeus

Poikkeusluettelossa (myös ”poikkeusten luettelo”) on yleensä sähköpostiosoitteet, jotka voivat olla hämäystä ja lähettää roskapostia. Sähköpostiviestit, jotka ovat tulleet poikkeusluettelossa olevista osoitteista, tarkistetaan aina roskapostin varalta. Oletusarvoisesti poikkeusluettelo sisältää kaikki sähköpostiosoitteet aiemmin määritetyistä sähköpostiohjelmien tileistä.

Palvelinpuolen hallinta

Palvelinpuolen hallintatoiminto on tekniikka, jolla voidaan tunnistaa massaroskapostitus vastaanotettujen sähköpostiviestien lukumäärän ja käyttäjien toimenpiteiden perusteella. Kukin viesti jättää yksilöllisen, viestin sisältöön perustuvan digitaalisen "sormenjäljen". Yksilöllinen tunnistenumero ei kerro mitään sähköpostiviestin sisällöstä. Kahdella samanlaisella viestillä on samanlainen sormenjälki, kun taas erilaisten viestien sormenjäljet ovat erilaisia.

Jos viesti merkitään roskapostiksi, sen sormenjälki lähetetään palvelimeen. Jos palvelin vastaanottaa useita samanlaisia sormenjälkiä, jotka vastaavat tiettyä roskapostiviestiä, sormenjälki tallennetaan roskapostien sormenjälkitietokantaan. Ohjelma lähettää viestien sormenjäljet palvelimeen saapuvien viestin tarkistuksen yhteydessä. Palvelin palauttaa tiedot sormenjäljistä, jotka vastaavat käyttäjien aiemmin roskapostiviesteiksi merkitsemiä sähköpostiviestejä.

Laajennettu muistin tarkistus

Laajennettu muistin tarkistus toimii yhdessä hyödynnän eston kanssa. Se vahvistaa suojausta haittaohjelmilta, jotka on suunniteltu välttämään haittaohjelmien torjuntaohjelmien tunnistus tarkoituksellista monimutkaistamista tai salausta hyödyntämällä. Laajennettu muistin tarkistus tunnistaa epäilyttävän toiminnan ja tekee uhkatarkistukset niiden paljastaessa itsensä järjestelmän muistista myös tapauksissa, joissa tavanomainen emulaatio tai heuristiikka ei havaitse uhkia. Tämä ratkaisu toimii tehokkaasti myös sellaisia haittaohjelmia vastaan, jotka on suojattu monimutkaisilla tunnistuksen estomenettelyillä.

Toisin kuin hyödynnän esto laajennettu muistin tarkistus on ohjelmien suorituksen jälkeen tehtävä tarkistus, joten siihen liittyy riski siitä, että uhka ehtii tehdä haitallisia toimia ennen sen tunnistamista. Laajennettu muistin tarkistus on kuitenkin tärkeä lisäsuojaustaso tilanteeseen, jossa muut tunnistustekniikat ovat epäonnistuneet.

Pankkitoimintojen ja maksujen suojaus

Pankkitoimintojen ja maksujen suojaus on lisäsuojakerros, jolla voit suojata rahaliikennetietoja verkkotapahtumien yhteydessä.

ESET Smart Security Premium ja ESET Internet Security sisältävät kiinteän luettelon ennalta määritetyistä

sivustoista, jotka avaavat suojatun selaimen. Voit lisätä sivuston tuotteen kokoonpanoon tai muokata sivustoluetteloa.

Ota Suojaa kaikki selaimet asetus käyttöön, jos haluat käynnistää kaikki tuetut selaimet suojatussa tilassa.

Saat lisätietoja tästä ominaisuudesta lukemalla seuraavat ESET-tietopankin artikkelit:

- Kuinka käytän ESETin pankki- ja maksusuojausta?
- Pankkitoimintojen ja maksujen suojauksen keskeyttäminen tai poistaminen käytöstä ESETin kotikäyttöön tarkoitetuissa Windows-tuotteissa
- ESETin pankkitoimintojen ja maksujen suojaus – yleiset virheet

Suojatun selauksen käyttäminen edellyttää HTTPS-salattua tietoliikennettä. Seuraavat selaimet tukevat Pankkitoimintojen ja maksujen suojausta:

- Internet Explorer 8.0.0.0
- Microsoft Edge 83.0.0.0
- Google Chrome 64.0.0.0
- Firefox 24.0.0.0

Avaa Pankkitoimintojen ja maksujen suojaus haluamaasi verkkoselaimeen

Kun avaat Pankkitoimintojen ja maksujen suojauksen suoraan tuotevalikon **Työkalut**-välilehdestä, se avataan selaimessa, jonka olet asettanut Windows-oletusselaimeksi. Muussa tapauksessa suojattujen sivustojen luettelon verkkosivustot ohjataan samantyyppiseen ESETin suojaamaan verkkoselaimeen, kun avaat haluamasi verkkoselaimen (muualta kuin tuotevalikosta).

Bottiverkkosuojaus

Bottiverkkosuojaus (botnet-suojaus) etsii haittaohjelmia analysoimalla sen verkkotietoliikenteen protokollia. Bottiverkon haittaohjelma muuttuu usein verrattuna verkkoprotokolliin, jotka eivät ole muuttuneet viime vuosina. Tämä uusi teknologia auttaa ESETiä estämään haittaohjelmia, jotka yrittävät välttää havaituksi joutumista ja yrittävät yhdistää tietokoneesi bottiverkkoon.

DNA-tunnistukset

Tunnistustyypit vaihtelevat tarkoista hajautusmäärityksistä ESET DNA -tunnistuksiin, jotka ovat monimutkaisia haitallisen toiminnan ja haittaohjelmien ominaispiireiden määritelmiä. Hyökkääjät voivat muokata ja piilottaa haitallista koodia helposti, mutta objektien toimintatapoja ei voi muuttaa helposti. ESET DNA -tunnistukset on suunniteltu hyödyntämään juuri tätä periaatetta.

Koodi syväanalysoidaan ja siitä poimitaan sen toiminnasta vastuulliset ”geenit”, joista muodostetaan ESET DNA -tunnistukset. Näitä tunnistuksia verrataan levystä tai prosessimuistista löydettyyn epäilyttävään koodiin. DNA-tunnistusten avulla voidaan havaita helposti haittaohjelmia, tunnettujen haittaohjelmaperheiden uusia variantteja ja jopa aiemmin havaitsemattomia tai tuntemattomia haittaohjelmia, joissa on haitalliseen toimintaan

viittaavia geenejä.

ESET LiveGrid®

ESET LiveGrid® (perustuu varhaisen varoituksen ESET ThreatSense.Net -järjestelmään) hyödyntää tietoja, joita ESET-käyttäjät eri puolilla maailmaa lähettävät, ja lähettää ne ESETin tutkimuslaboratorioon. ESET LiveGrid® kerää tietoja epäilyttävistä näytteistä ja metatiedoista, mikä pitää ESETin tietoisena uusimmista uhista ja auttaa ESETiä reagoimaan asiakkaidensa tarpeisiin välittömästi.

ESETin haittaohjelmatutkijat kokoavat tiedoista täsmällisen koosteen maailmanlaajuisten uhkien luonteesta ja laajuudesta, mikä auttaa kohdistamaan toimintamme oikeita kohteita vastaan. ESET LiveGrid® antaa siis tietoja, joilla on merkittävä rooli automaattisten prosessiemme prioriteettien määrittämisessä.

Lisäksi järjestelmä sisältää mainejärjestelmän, joka auttaa parantamaan haittaohjelmien torjuntaratkaisujemme yleistä tehokkuutta. Käyttäjä voi tarkistaa käynnissä olevien prosessien ja tiedostojen maineen suoraan ohjelmaliittymästä tai pikavalikosta ja hyödyntää ESET LiveGrid® -lisätietoja. Kun käyttäjän järjestelmässä oleva ohjelmatiedosto tai arkisto tarkistetaan, ensimmäisenä sen hajautustunnistetta verrataan vaarattomien ja estettävien kohteiden tietokannan tietoihin. Jos tunniste löytyy vaarattomien kohteiden luettelosta, tarkistettu tiedosto katsotaan turvalliseksi ja merkitään jätettäväksi pois myöhemmistä tarkistuksista. Jos tunniste löytyy estettävien kohteiden luettelosta, tiedosto käsitellään uhan luonteen edellyttämällä tavalla. Jos tunnistetta ei löydy tietokannasta, tiedosto tarkistetaan perinpohjaisesti. Tarkistuksen perusteella tiedosto luokitellaan joko uhaksi tai muuksi kuin uhaksi. Tämä menettely nopeuttaa tarkistusta huomattavasti. Tämän mainejärjestelmän avulla haittaohjelmanäytteet voidaan tunnistaa tehokkaasti jo ennen kuin haittaohjelmien määritystiedot on toimitettu käyttäjän tietokoneelle virustietokannan päivityksessä (joita tehdään useita kertoja päivän aikana).

ESET LiveGrid® -mainejärjestelmän lisäksi ESET LiveGrid® -palautejärjestelmä kerää tietokoneesta tietoja, jotka liittyvät juuri havaittuihin uhkiin. Tiedot voivat sisältää näytteen uhan sisältäneestä tiedostosta tai tiedoston kopion, tiedoston polun, tiedostonimen, päivämäärän ja kellonajan, prosessin, jonka yhteydessä uhka esiintyi, sekä tietoja tietokoneen käyttöjärjestelmästä.

ESET LiveGrid® -palvelimet

ESET LiveGrid® -palvelimemme sijaitsevat Bratislavassa, Wienissä ja San Diegossa. Nämä palvelimet huolehtivat kuitenkin vain asiakaspyyntöihin vastaamisesta. Lähetetyt näytteet käsitellään Bratislavassa, Slovakiassa.

ESET LiveGrid® -toiminnon ottaminen käyttöön tai poistaminen käytöstä ESET-tuotteissa

Tarkemmat kuvitetut ohjeet ESET LiveGrid® -toiminnon ottamisesta käyttöön tai poistamisesta käytöstä ESET-tuotteissa on ESET-tietopankin artikkelissa.

Hyödynnän esto

Hyödynnän esto on suunniteltu paikkaamaan tietoturvahyökkäyksissä yleisesti hyödynnettyjä sovelluksia, kuten verkkoselaimia, PDF-lukuohjelmia, sähköpostiohjelmia ja Microsoft Office -ohjelmia. Se myös tarjoaa suojaa ROP-hyökkäyksiltä. Hyödynnän esto on käytettävissä ja oletusarvoisesti käytössä kaikissa ESETin kotikäyttöön tarkoitetuissa Windows-tuuotteissa, Windows Serverin ESET-tuotteissa ja Windowsin ESET-päätepistetuotteissa.

Sen toimii etsimällä epäilyttäviä, hyödyntämiseen viittaavia merkkejä prosesseista.

Kun Hyödynnän esto tunnistaa epäilyttävän prosessin, se pysäyttää prosessin välittömästi ja tallentaa uhkaa

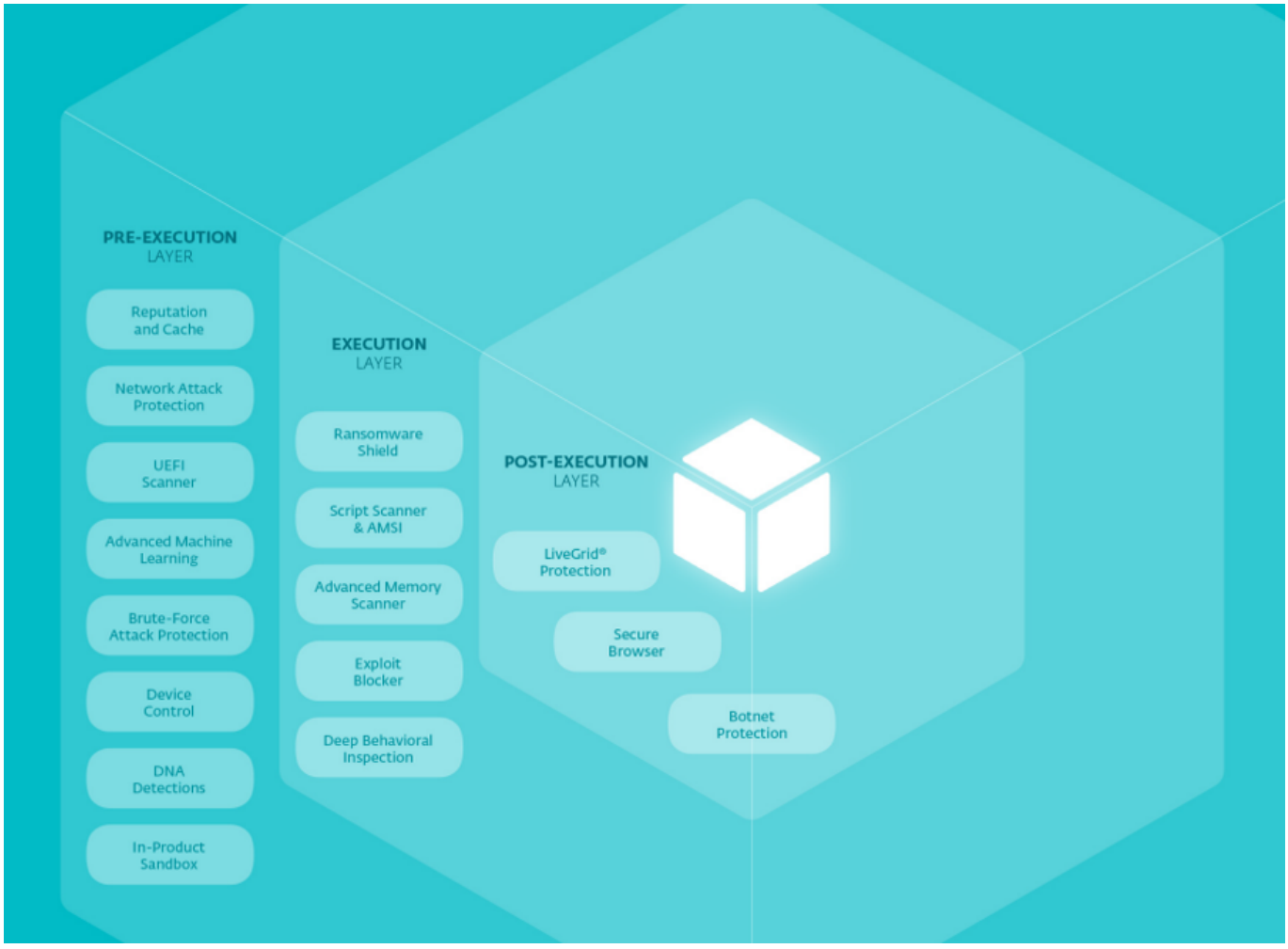
koskevat tiedot ja lähettää ne ESET LiveGrid® -pilvijärjestelmään. ESETin tutkimuslaboratorio käsittelee tiedot ja hyödyntää niitä kaikkien käyttäjien suojaamisessa tuntemattomilta uhilta ja zero-day-hyökkäyksiltä (uusilta haittaohjelmilta, joita vastaan ei ole vielä kehitetty torjuntamenettelyjä).

Java hyödynnän esto

Java hyödynnän esto on laajennus aiempiin hyödynnänestotekniikoihin. Se valvoo Java-ohjelmia ja etsii hyödynnältä vaikuttavaa toimintaa. Estetyt näytteet voidaan ilmoittaa haittaohjelmien analysoijille, jotta niistä voidaan luoda allekirjoituksia eri tasoisia torjuntatoimintoja (URL-torjunta, tiedostojen lataus jne.) varten.

ESET LiveSense

ESET käyttää monia ainutlaatuisia, omia, kerroksellisia suojaustekniikoita, jotka toimivat yhdessä ESET LiveSense -nimellä. Alla olevassa kuvassa esitetään joitakin ESETin ydinteknologioita ja kerrotaan, milloin ja missä ne voivat havaita uhan järjestelmän elinkaaren aikana ja lopulta estää sen.



Koneoppiminen

ESET kehittänyt koneoppimisalgoritmeja uhkien tunnistamiseen ja estämiseen jo vuodesta 1990. Neuraaliverkot lisättiin ESET-tuotteen tunnistusohjelmaan vuonna 1998.

Koneoppiminen sisältää DNA-tunnistukset, jotka käyttävät koneoppimiseen perustuvia malleja tehokkaaseen työskentelyyn pilviyhteydellä tai ilman. Koneoppimisalgoritmit ovat myös oleellinen osa alkuperäistä saapuvien näytteiden lajittelua ja luokittelua sekä niiden asettelua kuvitteelliselle ”kyberturvakartalle”.

ESET on kehittänyt oman sisäisen koneoppimisohjelmansa. Se käyttää neuraaliverkkojen tehoa (kuten syväoppimista ja pitkäkestoista lähimuistia) ja itse valitun kuuden luokittelualgoritmin ryhmää. Tällä tavalla se voi muodostaa yhdistetyn tuloksen, joka auttaa merkitsemään saapuvan näytteen puhtaaksi, mahdollisesti ei-toivotuksi tai haitalliseksi.

ESETin koneoppimisohjelma on hienosäädetty tekemään yhteistyötä muiden suojaavien tekniikoiden, kuten DNA:n, sandboxin ja muistianalyysin kanssa, sekä purkamaan toiminnallisia ominaisuuksia. Näin tunnistus on paras mahdollinen, ja vääriä hälytyksiä ilmenee mahdollisimman vähän.

Tarkistinkokoonpano ESET-tuotteen lisäasetuksissa

- ESET Windows -kodintuotteet (versiosta 13.1 alkaen)
- ESET Windows -päätelaitetuotteet (versiosta 7.2 alkaen)

Verkkohyökkäyssuojaus

Verkkohyökkäyssuojaus on palomuurin laajennus, joka parantaa tunnettujen haavoittuvuuksien hyödyntämisen tunnistusta verkkotasolla. Se tunnistaa yleiset hyödyntämisyritykset laajasti käytetyistä protokollista (kuten SMB, RPC ja RDP), mikä on tärkeä kerros haittaohjelmien leviämiseltä, verkosta tehtäviltä hyökkäyksiltä ja sellaisilta haavoittuvuuksilta suojautumisessa, joille ei ole vielä julkaistu korjausta tai joiden korjausta ei ole vielä otettu käyttöön.

Kiristyshaittaohjelmasuojaus

Kiristysohjelmasuojaus toimintaan perustuva tunnistustekniikka, joka valvoo kiristysohjelmien/tiedostokoodaajien toimintaa muistuttavalla tavalla tiedostoja muokkaavien sovellusten ja prosessien toimintaa. Jos sovelluksen toimintaa pidetään haitallisena tai maineperustaisessa tarkistuksessa ilmenee, että sovellus on epäilyttävä, sovellus estetään ja prosessi pysäytetään tai käyttäjää pyydetään estämään tai sallimaan se.

ESET LiveGrid® on oltava käytössä, jotta Kiristysohjelmasuojaus toimii oikein. Varmista ESET-tietopankin artikkelista, että ESET LiveGrid® on otettu käyttöön ja toimii ESET-tuotteessasi.

Komentosarjapohjaisilta hyökkäyksiltä suojautuminen

Komentosarjapohjaisilta hyökkäyksiltä suojautuminen koostuu selaimissa käytettävästä JavaScript-suojauksesta ja PowerShell-liittymien komentosarjojen AMSI (Antimalware Scan Interface) -suojauksesta.

HIPS
Tämä ominaisuus edellyttää, että HIPS on otettu käyttöön.

Komentosarjapohjaisilta hyökkäyksiltä suojautuminen tukee seuraavia selaimia:

- Mozilla Firefox

- Google Chrome
- Internet Explorer
- Microsoft Edge

> **Käytä tuettua selainta**
> Selainten tuetut vähimmäisversiot saattavat vaihdella, koska selaintiedostojen allekirjoitukset muuttuvat varsin usein. Selaimen uusinta versiota tuetaan aina.

Suojattu selain

Suojattu selain on lisäsuojakerros, jolla voit suojata arkaluonteisia tietojasi verkkoa selatessasi (esimerkiksi rahaliikennetietoja verkkotapahtumien yhteydessä).

ESET Endpoint Security 8 ja uudemmat sisältävät kiinteän luettelon ennalta määritetyistä sivustoista, jotka avaavat suojatun selaimen. Voit lisätä sivuston tuotteen kokoonpanoon tai muokata sivustoluetteloa. Suojattu selain on oletusarvoisesti poissa käytöstä asennuksen jälkeen.

Saat lisätietoja tästä ominaisuudesta lukemalla seuraavan ESET-tietämyskannan artikkelin.

Suojattu selaus edellyttää HTTPS-salattua tietoliikennettä. Suojattua selain käytettäessä Internet-selaimen on oltava alla olevien vähimmäisvaatimusten mukainen:

- Internet Explorer 8.0.0.0
- Microsoft Edge 83.0.0.0
- Google Chrome 64.0.0.0
- Firefox 24.0.0.0

> Vain Firefox- ja Microsoft Edge -selaimia tuetaan laitteissa, joissa on ARM-suorittimet.

Avaa ESET Suojattu selain haluamaasi verkkoselaimeen

Kun avaat ESET Suojatun selaimen suoraan tuotevalikon **Työkalut**-välilehdestä, ESET Suojattu selain avataan selaimessa, jonka olet asettanut oletusselaimeksi. Muussa tapauksessa ESETin sisäisen luettelon sivustot ohjataan samantyyppiseen ESETin suojaamaan verkkoselaimeen, kun avaat haluamasi verkkoselaimen (muualta kuin tuotevalikosta).

UEFI-tarkistus

UEFI (Unified Extensible Firmware Interface) -tarkistus on osa HIPS-järjestelmää (Host-based Intrusion Prevention System), joka suojaa tietokoneesi UEFI-ohjelmistoa. UEFI on laiteohjelmisto, joka latautuu muistiin tietokoneen käynnistysprosessin aluksi. Ohjelmiston koodi on emolevyyn juotetussa Flash-muistipiirissä. Tartuttamalla tämän koodin hyökkääjät voivat käyttää haittaohjelmia, jotka jäävät tietokoneeseen, vaikka käyttöjärjestelmä asennetaan tai käynnistetään uudelleen. Tällainen haittaohjelma jää myös helposti huomaamatta, koska useimmat haittaohjelmasuojausratkaisut eivät tarkista tätä järjestelmän osaa.

UEFI-tarkistus on käytössä automaattisesti. Voit myös käynnistää tietokoneen tarkistuksen manuaalisesti

ohjelman pääikkunasta napsauttamalla **Tietokoneen tarkistus** > **Tarkistuksen lisäasetukset** > **Mukautettu tarkistus** ja valitsemalla tarkistuskohteeksi **Käynnistyssektorit/UEFI**.

> Jos tietokoneessasi on jo UEFI-haittaohjelmatartunta, lue seuraava ESET-tietämyskannan artikkeli: Tietokoneessani on UEFI-haittaohjelmatartunta. Mitä teen?

Canary-tiedosto

Canary-tiedosto on todellisten asiakirjojen joukossa oleva väärennetty asiakirja, joka auttaa havaitsemaan ajoissa tietojen luvattoman käytön, kopioinnin tai muuttamisen.

Lukkiutuminen

Lukkiutuminen on tilanne, jossa tietokoneprosessi odottaa resurssia, joka on osoitettu toiselle prosessille. Tässä tilanteessa mitään prosesseista ei suoriteta, koska tarvittava resurssi on toisen prosessin hallussa, joka myös odottaa toisen resurssin vapautumista. Lukkiutuminen on tärkeää estää, ennen kuin se voi ylipäätään ilmetä. Resurssiajastin voi havaita lukkiutumisen, mikä auttaa käyttöjärjestelmää seuraamaan kaikkia eri prosesseille varattuja resursseja. Lukkiutuminen voi ilmetä, jos seuraavat neljä ehtoa toteutuvat samanaikaisesti:

- **Ei korvaavia toimia** – Resurssin voi vapauttaa omasta tahdostaan vain se prosessi, joka pitää resurssia hallussaan sen jälkeen, kun prosessi on suorittanut tehtävänsä.
- **Keskinäinen poissulkeminen** – Erityinen binaarinen semafority yppi, jota käytetään jaetun resurssin käytön hallintaan. Sen avulla suuremman prioriteetin tehtävien eston kesto voidaan pitää mahdollisimman lyhyenä.
- **Pitäminen ja odottaminen** – Tällä ehdolla prosesseja estetään pitämästä yksittäisiä tai useita resursseja hallussaan, jos samanaikaisesti odotetaan yhtä tai useampaa muuta prosessia.
- **Kehäodotus** – Järjestää kaikki resurssityypit järjestykseen kattavasti. Kehäodotus edellyttää myös, että jokainen prosessi pyytää resursseja luettelon mukaisessa järjestyksessä.

Lukkiutuminen voidaan käsitellä kolmella tavalla:

- Älä anna järjestelmän lukkiutua.
- Anna järjestelmän lukkiutua, ja tee sitten korvaavat toimet sen käsittelemiseksi, kun se tapahtuu.
- Jos lukkiutuminen tapahtuu, käynnistä järjestelmä uudelleen.