ESET Glossary

Vartotojo vadovas

Jei norite peržiūrėti šio dokumento internetinę versiją spustelėkite čia

Digital Security
Progress. Protected.

Autorių teisės ©2023 pagal ESET, spol. s r.o.

ESET Glossary sukūrė ESET, spol. s r.o.

Norėdami gauti daugiau informacijos, apsilankykite https://www.eset.com.

Visos teisės saugomos. Jokia šių dokumentų dalis negali būti atgaminama, saugoma paieškos sistemoje ar perduodama bet kokia forma ar bet kokiomis priemonėmis, elektronine, mechanine, kopijavimo, įrašymo, nuskaitymo ar kitokia forma be autoriaus raštiško leidimo.

ESET, spol. s r.o. pasilieka teisę keisti bet kurią iš aprašytų taikomųjų programų be išankstinio įspėjimo.

Techninė pagalba: https://support.eset.com

REV. 2023.4.19

1 ESET žodyno pristatymas 1
1.1 Reklamos programos 1
1.2 Užgrobtų kompiuterių tinklas botnet 1
1.3 Klaidingai teigiamas (FP) rezultatas 1
1.4 Pakavimo programos 2
1.5 Galimas nesaugias taikomąsias programas 2
1.6 Galimai nepageidaujamos programos 2
1.7 Išpirkos reikalaujantis kenkėjas 6
1.8 Kenkėjiška prieigos programa 7
1.9 Į grįžtamumą orientuotas programavimas 7
1.10 Šnipinėjimo programos 7
1.11 Trojos arklys 8
1.12 Virusas 8
1.13 Kirminas 9
1.14 Kredencialų brukimas 9
1.15 Sričių vardų serverio nuodijimas 9
1.16 DoS ataka 10
1.17 ICMP ataka 10
1.18 Prievadų nuskaitymas 10
1.19 „SMB Relay“ 10
1.20 TCP desinchronizavimas 11
1.21 Kirmino ataka 11
1.22 ARP talpyklos nuodijimas 11
2 El. pašto grėsmės 12
2.1 Reklaminiai skelbimai 12
2.2 Apgaulės 12
2.3 Sukčiavimas apsimetant 13
2.4 Brukalo suktybių atpažinimas 13
2.4 Taisyklės 14
2.4 Baltasis sąrašas 14
2.4 Juodasis sąrašas 14
2.4 Išimtis 15
2.4 Serverio pusės valdymas 15
2.5 Išplėstinis atminties skaitytuvas 15
2.6 Banko mokėjimų apsauga 15
2.7 Apsauga nuo įtraukimo į užgrobtų kompiuterių tinklą 16
2.8 DNR aptikimas 16
2.9 ESET LiveGrid® 17
2.10 Įsilaužimų blokatorius 17
2.11 „Java“ įsilaužimų blokatorius 18
2.12 ESET LiveSense 18
2.13 Mašininis mokymasis 18
2.14 Tinklo apsauga nuo atakų 19
2.15 Apsauga nuo „Ransomware“ 19
2.16 Apsauga nuo scenarijumi paremtų atakų 19
2.17 Saugi naršyklė 20
2.18 UEFI skaitytuvas 20
2.19 Kanarinis failas 21
2.20 Aklavietė 21

ESET žodyno pristatymas

ESET žodyne pateikiama išsami dabartinių grėsmių ir nuo jų saugančių ESET technologijų apžvalga.

Temos skirstomos į šiuos skyrius, kuriuose aprašoma:

- Aptikimai – sudaro: kompiuterių virusai, kirminai, Trojos arkliai, galimai nepageidaujamos programos ir t. t.
- Nuotolinės atakos – Grėsmes, kurios tyko vietiniuose tinkluose arba Internete
- El. pašto grėsmės – sudaro: apgaulė, sukčiavimas apsimetant, suktybės ir kt.
- ESET technologijos – ESET saugos sprendimuose naudojamos produktų funkcijos

Reklamos programos

Reklamos programa yra reklamų remiama programinė įranga. Programos, rodančios reklaminę medžiagą, patenka į šią kategoriją. Reklamos programos dažnai automatiškai interneto naršyklėje atidaro naują iškylantįjį langą su reklaminiais skelbimais arba pakeičia naršyklės pagrindinį puslapį. Reklamos programos dažnai prijungiamos prie nemokamų programų, kad leistų kūrėjams padengti jų taikomųjų programų (paprastai naudingų) išlaidas.

Pati reklamos programa nėra pavojinga – tik vartotojams įkyri reklaminiai skelbimai. Pavojus gali kilti tik dėl to, kad reklamos programa gali atlikti ir sekimo funkcijas (kaip tai daro šnipinėjimo programos).

Jeigu nusprendžiate naudoti nemokamą produktą, būkite itin atidūs diegdami programą. Diegimo programa greičiausiai praneš jums apie papildomos reklamos programos įdiegimą. Dažnai ją galima atšaukti ir įdiegti programą be reklaminių priedų.

Kai kurių programų negalima įdiegti be reklamos programų, arba jų funkcionalumas bus ribotas. Tai reiškia, kad reklamos programa gali patekti į sistemą „legaliu“ būdu, nes naudotojai su tuo sutiko. Tokiu atveju geriau pasisaugoti, negu vėliau gailėtis. Jeigu jūsų kompiuteryje failas aptiktas kaip reklamos programa, rekomenduojama jį pašalinti, nes yra didelė tikimybė, jog jame yra kenkėjiškas kodas.

Užgrobtų kompiuterių tinklas botnet

Botas arba saityno robotas – tai automatizuota kenkimo programa, nuskaitanti tinklo adresų blokus ir užkrečianti pažeidžiamus kompiuterius. Taip programišiai gali vienu metu perimti didelio skaičiaus kompiuterių kontrolę ir paversti juos botais (arba kompiuteriais-zombiais). Programišiai paprastai naudoja botus dideliam skaičiui kompiuterių užkrėsti. Vėliau šie kompiuteriai suformuoja užgrobtų kompiuterių tinklą. Į jūsų kompiuterį patekus botui, jis gali būti be jūsų žinios naudojamas paskirstytosios aptarnavimo perkrovos (DDoS) atakoms, įgaliotųjų serverių funkcijoms ir automatizuotoms užduotims internetu vykdyti (pvz., brukalui, virusams siųsti ar asmeninei bei privačiai informacijai vogti, pvz., banko rekvizitams ar kredito kortelių numeriams).

Klaidingai teigiamas (FP) rezultatas

Neįmanoma užtikrinti 100 % aptikimų dažnio ir 0 % tikimybės išvengti nepavojingų objektų kategorizavimo kaip aptikimų.

Klaidingai teigiamas rezultatas – tai nepavojingas failas arba programa, klaidingai klasifikuojama kaip kenkėjiška programinė įranga arba PUA.

Pakavimo programos

Pakavimo programos yra momentiniai savaime išsipakuojantys vykdomieji failai, kurie gali turėti keletą kenkimo programinės įrangos rūšių viename pakete.

Populiariausios pakavimo programos yra UPX, PE_Compact, PKLite ir ASPack. Ta pati kenkėjiška programa gali būti aptinkama skirtingai, kai ji suglaudinta naudojant skirtingas pakavimo programas. Be to, pakavimo programos turi gebėjimą bėgant laikui keisti savo kodą, kad kenkėjiškas programas būtų sudėtingiau aptikti ir pašalinti.

Galimas nesaugias taikomąsias programas

Yra daug teisėtų programų, kurių paskirtis – supaprastinti tinklo kompiuterių administravimą. Tačiau blogose rankose jos gali būti panaudotos kenkėjiškais tikslais. ESET suteikia galimybę aptikti tokias programas.

Galimos nesaugios programos yra komercinės, teisėtos programinės įrangos klasifikacija. Šiai klasifikacijai priklauso tokios programos kaip nuotolinės prieigos įrankiai, slaptažodžio iššifravimo ir klavišų registravimo programos (programos, įrašančios kiekvieną vartotojo klaviatūros paspaudimą).

Jeigu aptikote, kad jūsų kompiuteryje yra ir veikia galima nesaugi taikomoji programa (ir jūs nediegėte jos), kreipkitės į savo tinklo administratorių arba pašalinkite šią programą.

Galimas nepageidaujamas taikomąsias programas

„Grayware“ arba potencialiai nepageidaujama programa (PUA) yra plati programinės įrangos kategorija, kurios tikslas nėra vienareikšmiškai kenkėjiškas, kaip kitų tipų kenkėjiškos programinės įrangos, pvz., virusų ar Trojos arklių. Visgi ji gali įdiegti nepageidaujamą papildomą programinę įrangą, pakeisti skaitmeninio įrenginio veikimo būdą ar atlikti veiksmus, kurių naudotojas nepatvirtino arba nesitiki.

Kategorijos, kurios gali būti laikomos galimai nepageidaujama programine įranga, apima reklamos rodymo programinę įrangą, atsisiuntimo pakuotuvus, įvairias naršyklės įrankių juostas, klaidinančios elgsenos programinę įrangą, su kuo nors kartu gautą programinę įrangą, sekimo programinę įrangą, tarpinio serverio programinę įrangą (interneto bendrinimo programas), kriptovaliutos kasyklas, registro valytuvus (tik „Windows“ operacinėse sistemose) ar bet kurią kitą ribinę programinę įrangą arba programinę įrangą, kuri naudoja neteisėtą ar bent neetišką verslo praktiką (nepaisant to, kad atrodo teisėta) ir gali būti laikoma nepageidaujama galutinio naudotojo, kuris sužinojo, ką programinė įranga galėtų padaryti, jei būtų leista ją įdiegti.

Potencialiai nesaugi programa yra savaime teisėta (galbūt komercinė) programinė įranga, kuria įsilaužėlis galėtų piktnaudžiauti. ESET programinės įrangos naudotojai gali įjungti arba išjungti šių tipų programų aptikimą.

Tam tikrais atvejais vartotojas gali manyti, kad galimos nepageidaujamos programos keliami pavojai nublanksta prieš jos suteikiamus privalumus. Todėl ESET tokias programas priskiria žemesnės rizikos kategorijai, palyginti su kitų tipų kenkimo programine įranga, pavyzdžiui, Trojos arkliais ar kirminais.

- Įspėjimas – rasta galimai nepageidaujama programa
- Nuostatos

- Programinės įrangos pakuotuvai
- Registro valikliai
- Galimai nepageidaujamas turinys

Iliustruotos instrukcijos
Norėdami nuskaityti ir pašalinti galimai nepageidaujamas programas (PUA) ESET „Windows“ namų produktuose, skaitykite mūsų ESET žinių bazės straipsnį.

Įspėjimas – rasta galimai nepageidaujama programa

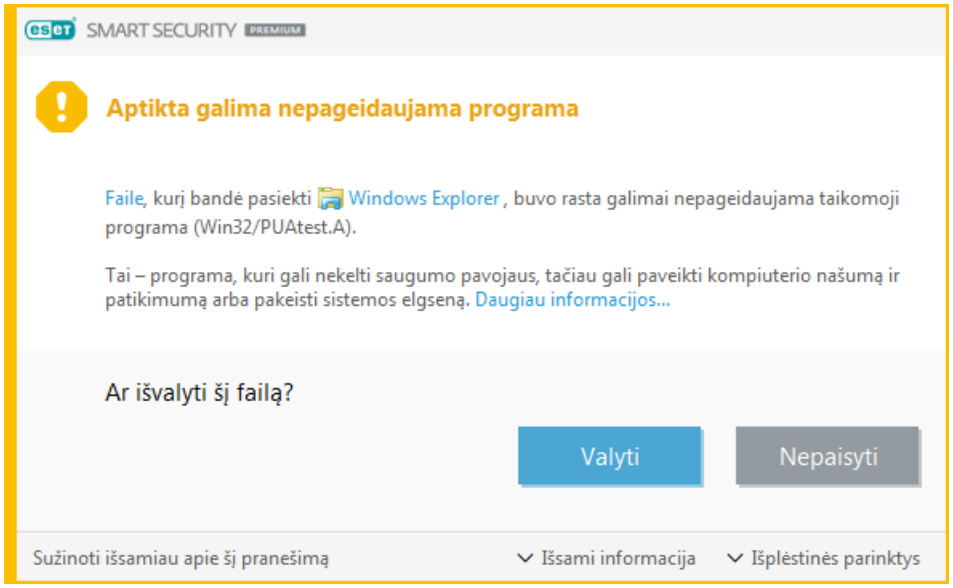
Kai bus aptikta galima nepageidaujama programa, galėsite nuspręsti, ką su ja daryti:

1.„**Clean/Disconnect**“ (valyti / atjungti): ši parinktis nutraukia veiksmą ir neleidžia PUA patekti į jūsų sistemą.
Atsisiuntimo iš svetainės metu matysite parinktį **Disconnect** (atjungti) prie PUA pranešimų ir parinktį **Clean** (valyti) prie disko failo pranešimų.

2.**Nepaisyti**: ši parinktis leidžia PUA patekti į jūsų sistemą.

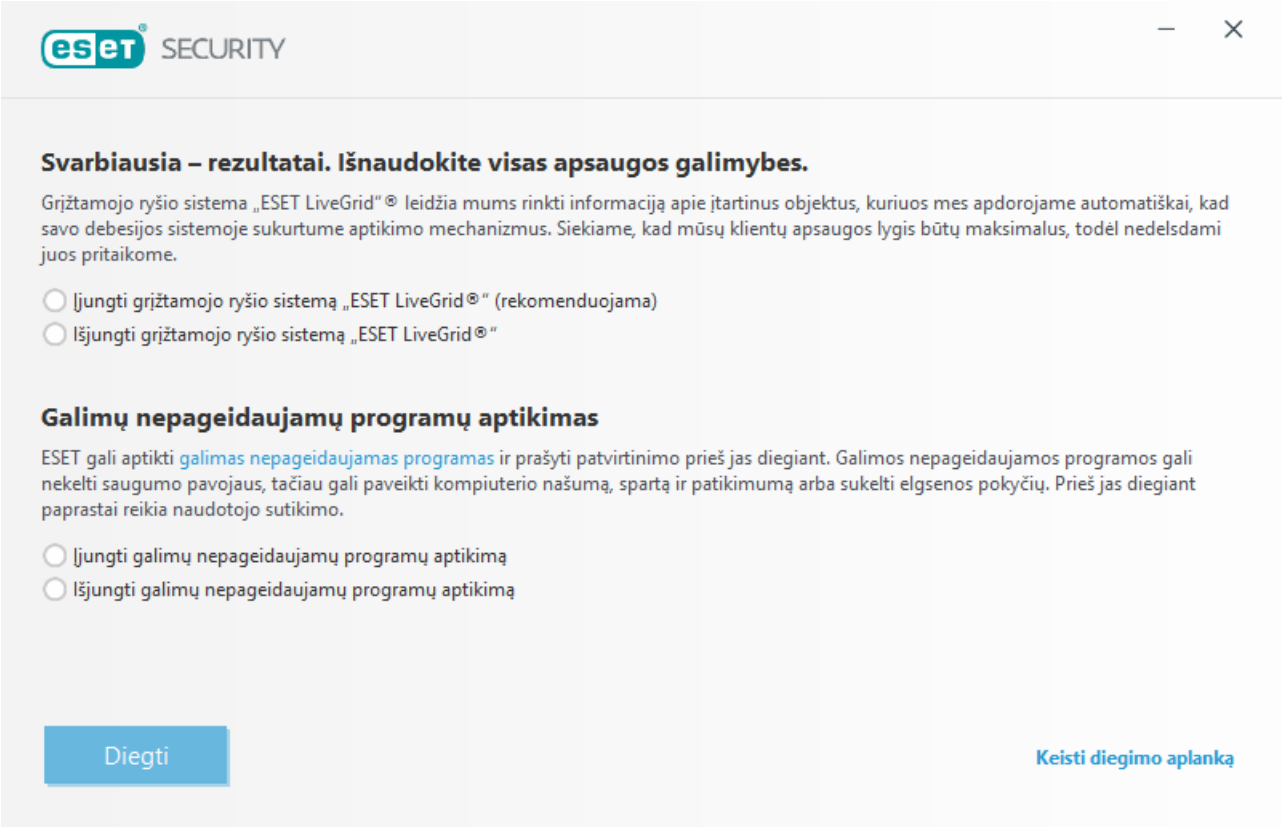
3.**Neįtraukti į aptikimą**: Jei norite, kad kompiuteryje aptiktas failas ateityje veiktų be trukdžių, spustelėkite **Advanced options** (išplėstinės parinktys), pažymėkite žymės langelį šalia Exclude from detection (neįtraukti į aptikimą) ir spustelėkite **Ignore** (nepaisyti).

4.**Neįtraukti parašo į aptikimą**: Jei norite, kad visi failai, aptikti pagal konkretų aptikimo pavadinimą (parašą) ateityje veiktų jūsų kompiuteryje be trikdžių (esamų failų arba atsisiuntimo iš interneto), spustelėkite **Advanced options** (išplėstinės parinktys), pažymėkite žymės langelį šalia **Exclude signature from detection** (neįtraukti parašo į aptikimą) ir spustelėkite **Ignore** (nepaisyti). Jei po to iš karto pasirodo papildomi aptikimo langai su identišku aptikimo pavadinimu, spustelėkite Ignore (nepaisyti), kad juos uždarytumėte (visi papildomi langai yra susiję su aptikimu, kuris įvyko prieš pašalinant parašą iš aptikimo).



Nuostatos

Diegdami ESET produktą galite pasirinkti, ar norite įjungti galimų nepageidaujamų programų aptikimą (parodyta toliau):



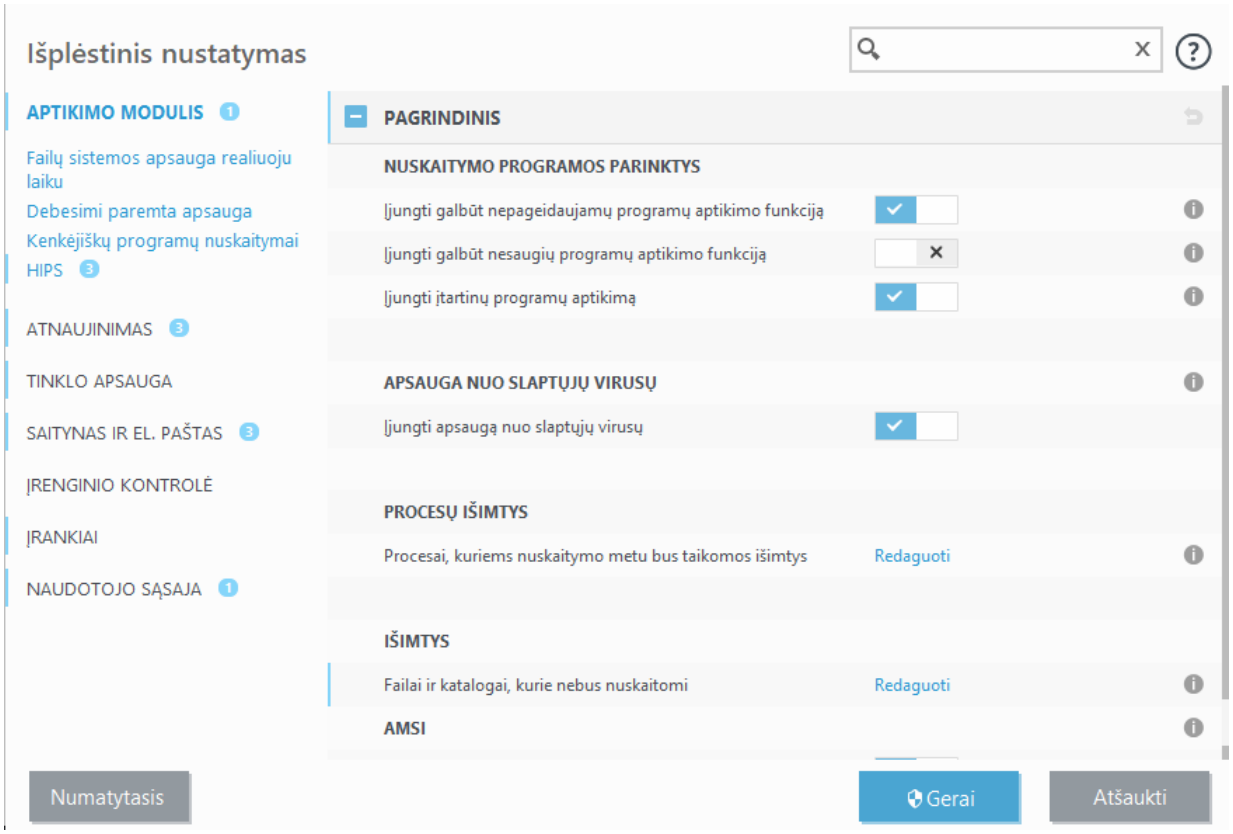
> **Įspėjimas**
> Galimas nepageidaujamas taikomąsias programas gali diegti reklamos programas, įrankių juostas arba jose gali būti kitų nepageidaujamų ir nesaugių programos funkcijų.

Šiuos parametrus galima bet kuriuo metu keisti programos parametruose. Jei norite įjungti arba išjungti galimų nepageidaujamų, nesaugių ar įtartinų programų aptikimą, vykdykite šiuos nurodymus:

1. Atidarykite ESET produktą.

2. Paspauskite klavišą **F5**, kad atidarytumėte **Išplėstinis nustatymas**.

3. Spustelėkite **Detection engine** (senesnėse versijose vadintą **Antivirus** arba **Computer**) ir pagal poreikį įjunkite arba išjunkite parinktis **Enable detection of potentially unwanted applications** (įjungti galimai nepageidaujamų programų aptikimą), **Enable detection of potentially unsafe applications** (įjungti galimai nesaugių programų aptikimą) ir **Enable detection of suspicious applications** (įjungti įtartinų programų aptikimą). Patvirtinkite paspausdami **OK** (gerai).



Iliustruotos instrukcijos

Jei reikia išsamesnių nurodymų, kaip konfigūruoti produktus, skirtus PUA aptikti arba nepaisyti, peržiūrėkite ESET žinių bazės straipsnius:

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

Programinės įrangos pakuotuvai

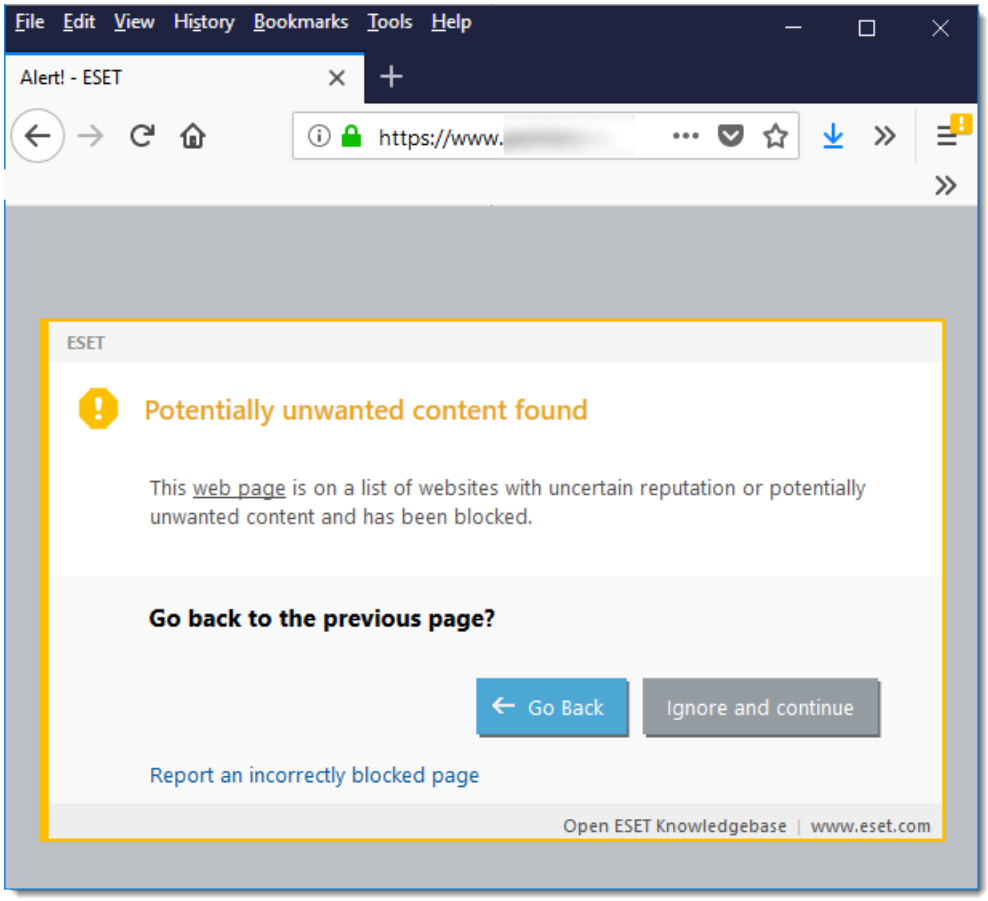
Programinės įrangos pakuotuvas – tai specialaus tipo programos modifikacija, kuri naudojama kai kuriose failų saugojimo svetainėse. Tai trečiųjų šalių įrankis, kuriuo įdiegiama programa, skirta duomenims atsisiųsti, tačiau kartu pridedama papildoma programinė įranga, pavyzdžiui, įrankių juostos ar reklamos programos. Papildoma programinė įranga gali atlikti jūsų saityno naršyklės pagrindinio puslapio ar paieškos nustatymų pakeitimus. Be to, failų prieglobos svetainės dažnai neįspėja programinės įrangos teikėjo ar atsisiuntimo gavėjo, kad buvo atlikti tam tikri pakeitimai, ir dažnai slepia atsisakymo pasirinkimus. Dėl to ESET programinės įrangos pakuotuvus priskiria galimų nepageidaujamų programų tipui, kad naudotojai galėtų pasirinkti, ar nori duomenis atsisiųsti, ar ne.

Registro valikliai

Registro valytuvai yra programos, kurios gali siūlyti, kad „Windows“ registro duomenų bazei reikia nuolatinės priežiūros ar valymo. Naudojant registro valytuvą gali kilti tam tikrų pavojų jūsų kompiuterio sistemai. Be to, kai kurie registro valytuvai pateikia nekvalifikuotus, nepatvirtintus ar kitaip nepalaikomus teiginius apie jų naudą ir (arba) kuria klaidinančias ataskaitas apie kompiuterinę sistemą, pagrįstas „nemokamo nuskaitymo“ rezultatais. Šiais klaidinančiais teiginiais ir ataskaitomis siekiama jus įtikinti įsigyti visą versiją ar prenumeratą, paprastai neleidžiant įvertinti registro valytuvo prieš apmokėjimą. Dėl šių priežasčių „ESET“ klasifikuoja tokias programas kaip PUA ir suteikia galimybę jas leisti arba blokuoti.

Galimai nepageidaujamas turinys

Jei jūsų „ESET“ produkte įjungtas PUA aptikimas, svetainės, turinčios PUA reklamavimo arba vartotojų klaidinimo, kad šie atliktų jų sistemai ar naršymo patirčiai neigiamų padarinių galinčius turėti veiksmus, reputaciją, bus blokuojamos kaip galimai nepageidaujamas turinys. Jei gausite pranešimą, kad svetainė, kurią bandote pasiekti, laikoma galimai nepageidaujamu turiniu, galite spustelėti „**Go Back**“ (eiti atgal), kad išeitumėte iš blokuojamo tinklalapio, arba „**Ignore and continue**“ (nepaisyti ir tęsti), kad leistumėte svetainei atsidaryti.



Papildomos informacijos šia tema galima rasti šiame ESET žinių bazės straipsnyje.

Išpirkos reikalaujantis kenkėjas

Išpirkos reikalaujantis kenkėjas (taip pat vadinamas failų šifravimo programa) yra kenkėjiška programinė įranga, užblokuojanti įrenginį arba užšifruojanti įrenginio turinį ir reikalaujanti pinigų, kad būtų grąžinta prieiga prie turinio. Ši kenkėjiška programinė įranga taip pat gali turėti laikmatį su nustatytu išpirkos terminu, iki kurio reikia sumokėti. Nesumokėjus iki termino, kaina padidėja arba įrenginys užblokuojamas visam laikui.

Kai įrenginys užkrečiamas, failų šifravimo programa gali bandyti užšifruoti bendrinamus įrenginio diskus. Dėl šio proceso gali atrodyti, kad ši kenkėjiška programinė įranga plinta tinklu, bet taip nėra. Ši padėtis susidaro, kai bendrinamas diskas failų serveryje yra užšifruojamas, bet pačiame serveryje viruso nėra (nebent galutiniame serveryje).

Išpirkos reikalaujančio kenkėjo kūrėjai sukuria privatų ir viešą raktus, ir viešą raktą įterpia į kenkėjišką programinę įrangą. Pats išpirkos reikalaujantis kenkėjas gali būti Trojos arklio dalis arba failas ar paveikslėlis, kurį gavote el. paštu, socialiniame tinkle arba tiesioginių pranešimų programoje. Patekusi į jūsų kompiuterį kenkėjiška programinė įranga sugeneruoja atsitiktinį simetrišką raktą ir užšifruoja įrenginio duomenis. Ji naudoja viešą

kenkėjiškos programinės įrangos raktą simetriškam raktui užšifruoti. Tada išpirkos reikalaujantis kenkėjas reikalauja išpirkos, kad būtų iššifruoti duomenys. Įrenginyje rodomas išpirkos reikalaujantis pranešimas gali būti melagingas įspėjimas, kad jūsų sistema naudojama neteisėtai veiklai arba joje yra neteisėto turinio. Išpirkos reikalaujantis kenkėjas reikalauja aukos sumokėti išpirką įvairiais mokėjimo būdais. Dažniausiai būdai yra sunkiausiai atsekami, pvz., skaitmeninės (kripto) valiutos, mokamos SMS žinutės arba iš anksto apmokėti kuponai. Išpirkos reikalaujančio kenkėjo autorius, gavęs išpirką, turėtų atrakinti įrenginį arba pasinaudoti privačiu raktu simetriškam raktui iššifruoti ir iššifruoti aukos duomenis; tačiau ši operacija nėra garantuota.

> **Daugiau informacijos apie išpirkos reikalaujantį kenkėją**
> ESET produktai naudoja kelių sluoksnių technologijas, apsaugančias įrenginius nuo išpirkos reikalaujančių kenkėjų. Peržiūrėkite mūsų ESET žinių bazės straipsnį, kad sužinotumėte geriausią praktiką, kaip apsaugoti savo sistemą nuo išpirkos reikalaujančių kenkėjų.

Kenkėjiška prieigos programa

Kenkėjiškos prieigos programos yra kenkėjiškos programos, kurios suteikia interneto įsilaužėliams neribotą prieigą prie sistemos ir užmaskuoja jų buvimą. Kenkėjiškos prieigos programos, patekusios į sistemą (paprastai panaudodamos sistemos pažeidžiamumą), naudoja operacinės sistemos funkcijas, kad jų neaptiktų antivirusinė programinė įranga: jos slepia procesus, failus ir „Windows“ registrų duomenis. Todėl jų beveik neįmanoma aptikti naudojant įprastinius tikrinimo metodus.

Yra du aptikimo lygmenys, leidžiantys apsisaugoti nuo kenkėjiškų prieigos programų:

1. Kai jos bando patekti į sistemą: Jų dar nėra sistemoje, todėl jos neaktyvios. Daugelis antivirusinių sistemų gali eliminuoti kenkėjiškas prieigos programas šiame lygmenyje (jeigu jos realiai aptinka tokius failus kaip užkrėstus).

2. Kai jos paslėptos nuo įprastinio tikrinimo: ESET naudotojai gali naudotis apsaugos nuo slaptųjų virusų technologija, kuri gali aptikti ir eliminuoti aktyvias kenkėjiškos prieigos programas.

Į grįžtamumą orientuotas programavimas

Į grįžtamumą orientuotas programavimas (ROP) yra tipinė kodo pakartotinio naudojimo ataka, kai užpuolikas nukreipia valdymo srautą per esamą kodą su kenkėjišku rezultatu. ROP ataka yra pažangi rietuvės naikinimo atakos versija. Rietuvės buferio perpildymas įvyksta tada, kai programa įrašo duomenis į programos iškvietimų rietuvės atminties adresą, esantį už numatytos duomenų struktūros ribų, paprastai su fiksuoto ilgio buferiu.

ROP yra išnaudojimo technika, leidžianti vykdyti kodą tikslinėje sistemoje. Gavęs prieigą prie iškvietimų rietuvės valdymo, užpuolikas valdo kompiuteryje veikiančios patikimos programinės įrangos srautą ir manipuliuoja ja, kad atliktų kitą užduotį, nei buvo numatyta.

Šnipinėjimo programos

Ši kategorija apima visas programas, kurios siunčia asmeninę informaciją be vartotojo leidimo ar žinios. Šnipinėjimo programos naudoja sekimo funkcijas, kad išsiųstų įvairius statistinius duomenis, tokius kaip aplankytų svetainių sąrašas, el. pašto adresai iš vartotojo kontaktų sąrašo arba įrašytų klaviatūros paspaudimų sąrašas.

Šnipinėjimo programų autoriai tikisi, kad šie metodai padės daugiau sužinoti apie vartotojų poreikius bei interesus ir leis siųsti tikslingesnius reklaminius skelbimus. Problema yra ta, kad nėra aiškios ribos tarp naudingų ir

kenkėjiškų programų, ir niekas negali būti tikras, jog gauta informacija nebus panaudota kenkėjiškais tikslais. Tarp šnipinėjimo programų gaunamų duomenų gali būti saugos kodų, PIN, bankų sąskaitų numerių ir t. t. Šnipinėjimo programos dažnai autorių sujungiamos su nemokamomis programų versijomis, kad galėtų gauti pajamų arba paskatintų pirkti programinę įrangą. Dažnai vartotojai yra informuojami apie šnipinėjimo programų įdiegimą diegiant programinę įrangą, kad paskatintų juos įsigyti mokamą versiją be šnipinėjimo programų.

Gerai žinomų nemokamų produktų, pateikiamų su šnipinėjimo programomis, pavyzdžiai yra kliento programos P2P (lygiaverčių mazgų) tinkluose. „Spyfalcon“ arba „Spy Sheriff“ (ir daugelis kitų) priklauso specifinei šnipinėjimo programų kategorijai – jos atrodo kaip apsaugos nuo šnipinėjimo programos, tačiau iš tikrųjų yra šnipinėjimo programos.

Jeigu failas jūsų kompiuteryje aptiktas kaip šnipinėjimo programa, patariama jį panaikinti, nes yra didelė tikimybė, kad jame yra kenkėjiškas kodas.

Šnipinėjimo programų subkategorija registravimo programos (angl. „keyloggers“) gali būti tiek aparatinės, tiek programinės. Programine įranga grįstos registravimo programos gali rinkti tik vienoje svetainėje ar programoje įvestą informaciją. Sudėtingesnės registravimo programos gali įrašyti viską, ką įvedate, įskaitant informaciją, kurią kopijuojate / įklijuojate. Kai kurios registravimo programos, skirtos mobiliesiems įrenginiams, gali įrašyti skambučius, informaciją iš pokalbių programėlių, buvimo vietą ar net mikrofono ir fotoaparato informaciją.

Trojos arklys

Istoriškai kompiuteriniai Trojos arkliai buvo priskirti klasei grėsmių, kurios bando pasirodyti kaip naudingos programos, kad vartotojai jas vykdytų.

Kadangi Trojos arkliai labai plati kategorija, ji dažnai dalijama į keletą pogrupių:

- Atsisiuntimo programa – kenkėjiškos programos, galinčios atsisiųsti kitas grėsmes iš interneto.

- Trojos arklių platintojas – kenkėjiškos programos , galinčios įkelti kitų tipų kenkėjišką programinę įrangą į užkrėstus kompiuterius.

- Užpakalinės durys – kenkėjiškos programos , palaikančios ryšį su nuotoliniais įsilaužėliais, leidžiančios jiems gauti prieigą prie kompiuterio ir perimti jos valdymą.

- Klaviatūros paspaudimų registravimo programa – (klaviatūros paspaudimų registratorius) – programa, kuri įrašo kiekvieną klaviatūros paspaudimą naudotojui rašant ir siunčia informaciją nuotoliniams įsilaužėliams.

- Numerio rinkiklis – kenkėjiškos programos, naudojamos prisijungiant prie padidinto tarifo numerių vietoj naudotojo interneto paslaugų teikėjo. Naudotojui beveik neįmanoma pastebėti, kad buvo užmegztas naujas ryšys. Numerio rinkikliai gali pridaryti žalos tik naudotojams, turintiems telefoninius modemus, kurie šiuo metu retai naudojami.

Jeigu failas jūsų kompiuteryje yra aptiktas kaip Trojos arklys, patariama jį panaikinti, nes jame greičiausiai yra ne kas kita, o kenkėjiškas kodas.

Virusas

Kompiuterinis virusas yra kenkėjiško kodo dalis, kuri pridedama prie jūsų kompiuteryje esančių failų. Virusai gavo biologinių virusų pavadinimą, nes naudoja panašią metodiką plisdami iš vienos vietos į kitą. Terminas „virusas“ dažnai neteisingai vartojamas, apibūdinant bet kokio tipo grėsmes. Toks vartojimas palaipsniui išstumiamas ir

pakeičiamas nauju tikslesniu terminu „kenkėjiška programa“ (kenkėjiška programinė įranga).

Kompiuterių virusai dažniausiai atakuoja vykdomuosius failus ir dokumentus. Trumpai tariant, štai kaip veikia kompiuterio virusas: paleidus užkrėstą failą, iškviečiamas kenkėjiškas kodas ir įvykdomas prieš paleidžiant taikomąją programą. Virusas gali užkrėsti bet kuriuos failus, kuriems esamas vartotojas yra suteikęs leidimą.

Kompiuterių virusus galima skirstyti pagal paskirtį ir pavojingumą. Kai kurie jų itin pavojingi dėl savo gebėjimo tikslingai naikinti failus iš standžiojo disko. Tačiau kai kurie virusai nedaro jokios žalos – jie skirti tik paerzinti vartotoją ir pademonstruoti jų autorių techninius sugebėjimus.

Jei jūsų kompiuteris yra užkrėstas virusu ir jo neįmanoma išvalyti, pateikite jį į ESET tyrimų laboratoriją ištirti. Tam tikrais atvejais užkrėsti failai gali būti taip pakeisti, kad jų išvalyti neįmanoma ir failai turi būti pakeisti švaria kopija.

Kirminas

Kompiuterio kirminas yra kenkėjišką kodą turinti programa, kuri atakuoja pagrindinius kompiuterius ir plinta tinklu. Pagrindinis skirtumas tarp viruso ir kirmino yra tai, kad kirminai gali daugintis / sklisti patys; jie nėra priklausomi nuo šeimininko failų (arba paleidimo sektorių). Kirminai plinta per el. pašto adresus jūsų kontaktų sąraše arba išnaudoja tinklo programų saugos spragas.

Todėl kirminai yra daug gyvybingesni nei kompiuterių virusai. Pasinaudodami didžiuliu interneto prieinamumu jie gali išplisti po visą pasaulį per kelias valandas ar net minutes nuo to laiko, kai buvo išleisti. Dėl šios galimybės nepriklausomai ir greitai daugintis jie yra daug pavojingesni nei kitų tipų kenkėjiškos programos.

Sistemoje suaktyvintas kirminas gali sukelti daug nepatogumų: jis gali naikinti failus, bloginti sistemos efektyvumą arba net deaktyvinti programas. Dėl savo prigimties kompiuterių kirminas kvalifikuojamas kaip „transporto priemonė“ kitų tipų įsiskverbimams.

Jeigu jūsų kompiuteris yra užkrėstas kirminu, rekomenduojame sunaikinti užkrėstus failus, nes juose gali būti kenkėjiškas kodas.

Kredencialų brukimas

Kredencialų brukimas (angl. „credential stuffing“) yra kibernetinė ataka, kuri naudoja duomenis iš nutekintų kredencialų duomenų bazių. Užpuolikai naudoja robotus ir kitus automatizavimo metodus, kad prisijungtų prie paskyrų daugelyje svetainių, naudodami nutekėjusius duomenis. Užpuolikai naudojasi vartotojais, kurie naudoja vienodus kredencialus keliose svetainėse ir paslaugose. Sėkmingos atakos atveju užpuolikai gali gauti visišką prieigą prie paskyros ir vartotojų duomenų, saugomų toje paskyroje. Pasinaudodami prieiga užpuolikai gali pavogtų asmens duomenis, kad pavogtų tapatybę, atliktų apgaulingas operacijas, platintų šlamštą ar atliktų kitus kenkėjiškus veiksmus.

Sričių vardų serverio nuodijimas

Naudodami DNS (sričių vardų serveris – angl. Domain Name Server) nuodijimą, programišiai gali apgauti bet kurio kompiuterio DNS serverį, kad jis patikėtų, jog jų tiekiami apgaulingi duomenys yra teisėti ir autentiški. Apgaulinga informacija yra tam tikrą laiką laikoma talpykloje ir leidžia įsilaužėliams perrašyti DNS IP adresų atsakymus. Tuomet vartotojai, bandydami patekti į interneto svetaines, vietoj originalaus jų turinio atsisiųs virusų arba kirminų.

DoS ataka

DoS, arba aptarnavimo perkrovos ataka (angl. Denial of Service), yra bandymas padaryti kompiuterį arba tinklą nepasiekiamą jo vartotojams. Ryšys tarp paveiktų vartotojų yra blokuojamas ir nebegali tinkamai veikti. DoS atakos paveiktus kompiuterius paprastai reikia paleisti iš naujo, kad jie vėl tinkamai veiktų.

Daugeliu atvejų atakos objektai yra saityno serveriai, o atakos tikslas – padaryti juos tam tikrą laiką nepasiekiamus vartotojams.

ICMP ataka

ICMP (interneto valdymo pranešimų protokolas – angl. Internet Control Message Protocol) yra populiarus ir plačiai naudojamas interneto protokolas. Jį tinkle esantys kompiuteriai pirmiausia naudoja įvairiems klaidų pranešimams siųsti.

Nuotoliniai įsilaužėliai bando išnaudoti silpnąsias ICMP protokolo vietas. ICMP protokolas yra skirtas vienpusiam ryšiui ir nereikalauja atpažinimo. Tai leidžia nuotoliniams įsilaužėliams paleisti vadinamąsias DoS (aptarnavimo perkrovos ataka) atakas arba atakas, kurios suteikia neįgaliotiems asmenims prieigą prie gaunamų ir siunčiamų paketų.

Tipiniai ICMP atakų pavyzdžiai yra ryšio užklausos užpildymas, ICMP_ECHO užpildymas ir didelio srauto atakos. Kompiuteriai, patyrę ICMP ataką, veikia daug lėčiau (tai taikoma visoms internetą naudojančioms programoms) ir iškyla problemų jungiantis prie interneto.

Prievadų nuskaitymas

Prievadų nuskaitymas yra naudojamas siekiant nustatyti, kurie kompiuterio prievadai yra atidaryti pagrindiniame tinklo kompiuteryje. Prievadų skaitytuvas yra programa, skirta ieškoti tokių prievadų.

Kompiuterio prievadas yra virtualus taškas, kuris tvarko gaunamus ir siunčiamus duomenis – tai labai svarbu saugos požiūriu. Dideliame tinkle prievado skaitytuvų gaunama informacija gali padėti identifikuoti galimas pažeidžiamas vietas. Toks naudojimas yra teisėtas.

Tačiau prievadų nuskaitymą dažnai naudoja programišiai bandydami pasikėsinti į saugą. Jie pirmiausia siunčia paketus į kiekvieną prievadą. Atsižvelgiant į atsakymo tipą galima nustatyti, kurie prievadai yra naudojami. Pats nuskaitymas nedaro žalos, tačiau atsiminkite, kad tokiais veiksmais galima aptikti galimas pažeidžiamas vietas ir leisti įsilaužėliams kontroliuoti nuotolinius kompiuterius.

Tinklo administratoriams patariama blokuoti visus nenaudojamus prievadus, o naudojamus apsaugoti nuo neįgaliotos prieigos.

„SMB Relay“

„SMB Relay“ ir „SMB Relay 2“ yra specialios programos, galinčios rengti atakas prieš nuotolinius kompiuterius. Šios programos pasinaudoja serverio pranešimų bloko failų bendrinimo protokolu, kuris veikia „NetBIOS“ lygmenyje. Vartotojas, bendrinantis bet kokius aplankus arba katalogus LAN tinkle, greičiausiai naudoja šį failų bendrinimo protokolą.

Vietinio tinklo ryšyje pakeičiamos slaptažodžių maišos.

„SMB Relay“ gauna ryšį su UDP 139 ir 445 prievadais, perima tarp kliento ir serverio siunčiamus paketus ir juos modifikuoja. Prisijungęs ir atpažintas klientas yra atjungiamas. „SMB Relay“ sukuria naują virtualųjį IP adresą. Naujas adresas gali būti pasiekiamas naudojant komandą „net use \\192.168.1.1“. Tada adresą gali naudoti visos „Windows“ tinklo funkcijos. „SMB Relay“ perima visus SMB protokolo ryšius, išskyrus derybas ir tapatumo nustatymą. Nuotoliniai įsilaužėliai gali naudoti IP adresą, kol kliento kompiuteris yra prisijungtas.

„SMB Relay 2“ veikia taip pat kaip „SMB Relay“, tik ši programa naudoja „NetBIOS“ vardus, o ne IP adresus. Abi jos gali rengti „tarpininko“ atakas. Šios atakos leidžia nuotoliniams įsilaužėliams nepastebimai skaityti, įterpti ir keisti pranešimus, kuriais keičiasi du ryšio taškai. Kompiuteriai, paveikti tokių atakų, dažnai nebeatsako arba netikėtai paleidžiami iš naujo.

Kad išvengtumėte atakų, rekomenduojame naudoti atpažinimo slaptažodžius arba raktus.

TCP desinchronizavimas

TCP desinchronizavimas yra metodas, naudojamas TCP užgrobimo atakoms atlikti. Jį aktyvina procesas, kurio eilės numeris gaunamame pakete skiriasi nuo laukiamo eilės numerio. Paketai su nelauktais eilės numeriais atmetami (arba saugomi buferio atmintyje, jeigu jie yra esamo ryšio lange).

Dėl desinchronizavimo abu ryšio galiniai taškai praleidžia gautus paketus, čia nuotoliniai įsilaužėliai gali įsiskverbti ir tiekti paketus su teisingais eilės numeriais. Įsilaužėliai gali net manipuliuoti arba keisti ryšį.

TCP užgrobimo atakos skirtos pertraukti serverio-kliento arba lygiaverčių mazgų ryšius. Daugelio atakų galima išvengti naudojant kiekvieno TCP segmento atpažinimą. Be to, patariama naudoti rekomenduojamas tinklo įrenginių konfigūracijas.

Kirmino ataka

Kompiuterio kirminas yra kenkėjišką kodą turinti programa, kuri atakuoja pagrindinius kompiuterius ir plinta tinklu. Tinklo kirminai išnaudoja įvairių taikomųjų programų saugos spragas. Pasinaudodami internetu jie gali išplisti po visą pasaulį per kelias valandas nuo jų išleidimo.

Daugelio kirminų atakų („Sasser“, „SqlSlammer“) galima išvengti naudojant užkardos numatytuosius saugos parametrus arba blokuojant neapsaugotus ir nenaudojamus prievadus. Be to, itin svarbu, kad jūsų operacinė sistema būtų atnaujinta naudojant naujausias saugos pataisas.

ARP talpyklos nuodijimas

Adresų nustatymo protokolas (ARP) konvertuoja adresus tarp duomenų susiejimo lygmens (MAC adresai) ir tinklo lygmens (IP adresai). ARP talpyklos nuodijimo ataka leidžia įsilaužėliams perimti ryšį tarp tinklo įrenginių, sugadinant tinklo ARP lenteles (įrenginių konvertavimas iš MAC į IP).

Įsilaužėlis nusiunčia klaidingą ARP atsakymo pranešimą į numatytąjį tinklo šliuzą, informuodamas, kad MAC adresas yra susietas su kito tikslinio objekto IP adresu. Kai numatytasis šliuzas gauna šį pranešimą ir transliuoja pakeitimus visiems kitiems tinklo įrenginiams, visas tikslinio objekto srautas į bet kurį kitą tinklo įrenginį eina per įsilaužėlio kompiuterį. Šis veiksmas leidžia įsilaužėliui patikrinti arba modifikuoti srautą prieš persiunčiant jį į numatytą paskirties vietą.

El. pašto grėsmės

El. paštas yra ryšio forma, turinti daugybę pranašumų.

Deja, dėl aukšto anonimiškumo lygio el. paštas ir internetas sudarė sąlygas neteisėtai veiklai, tokiai kaip brukalo siuntimas. Brukalą sudaro neprašyti reklaminiai skelbimai, apgaulės ir kenkėjiškų programų – kenkėjiškos programinės įrangos platinimas. Nepatogumą ir didėjantį pavojų kelia tai, kad brukalo siuntimo išlaidos yra minimalios, o jo autoriai turi daug priemonių įsigyti naujus el. pašto adresus. Be to, brukalo apimtis ir įvairovė labai apsunkina jo kontrolę. Kuo ilgiau naudojate savo el. pašto adresą, tuo didesnė tikimybė, kad jis pateks į brukalo modulio duomenų bazę.

Keletas patarimų, kaip to išvengti:

- Jei įmanoma, neskelbkite savo el. pašto adreso internete
- Duokite savo el. pašto adresą tik patikimiems asmenims
- Jei įmanoma, nenaudokite įprastų alternatyviųjų vardų – sudėtingesni alternatyvieji vardai sumažina atsekimo tikimybę
- Neatsakykite į brukalą, kuris jau pateko į jūsų pašto dėžutę
- Būkite atsargūs pildydami interneto formas – itin atidžiai įvertinkite tokias parinktis kaip „Taip, aš noriu gauti informaciją“.
- Naudokite „specializuotus“ el. pašto adresus, pvz., vieną verslui, vieną siekdami bendrauti su draugais ir t. t.
- Periodiškai keiskite savo el. pašto adresą
- Naudokite apsaugos nuo brukalo priemones

Reklaminiai skelbimai

Interneto reklamos – tai viena greičiausiai augančių reklamos formų. Jos pagrindiniai rinkos privalumai yra minimalios sąnaudos ir aukštas kryptingumo lygis; be to, pranešimai pateikiami beveik iškart. Daugelis įmonių naudoja el. pašto rinkodaros įrankius, siekdamos efektyviai bendrauti su esamais ir galimais klientais.

Tokio tipo reklamos yra teisėtos, nes jūs galite būti suinteresuoti gauti komercinę informaciją apie kai kurios produktus. Tačiau daug įmonių siunčia neprašytus didelius komercinius laiškus. Tokiais atvejais el. pašto reklamos peržengia ribas ir tampa brukalu.

Nepageidaujamų el. laiškų kiekis jau tapo problema ir neatrodo, kad jis pradės mažėti. Nepageidaujamų el. laiškų autoriai dažnai bando maskuoti brukalą kaip teisėtus laiškus.

Apgaulės

Apgaulė yra internetu platinama klaidinanti informacija. Apgaulės paprastai siunčiamos el. paštu arba tokiomis ryšių priemonėmis kaip ICQ ir „Skype“. Pačiame laiške paprastai pateikiami pokštai arba prasimanymai.

Kompiuterių virusų apgaulės bando sukelti baimę, nepasitikėjimą ir abejones gavėjams, bandydamos įtikinti, kad yra „neaptinkamas virusas“, naikinantis failus ir išgaunantis slaptažodžius arba atliekantis kitus kenkėjiškus veiksmus sistemoje.

Kai kurios apgaulės veikia prašydamos gavėjų persiųsti laiškus savo kontaktams ir taip platinti apgaulę. Yra mobiliųjų telefonų apgaulės, prašymai padėti, žmonės, siūlantys atsiųsti jums pinigų iš užsienio, ir t. t. Dažnai neįmanoma suprasti jų kūrėjų kėslų.

Jeigu matote laišką, raginantį peradresuoti jį visiems pažįstamiems, tai greičiausiai gali būti apgaulė. Yra daug svetainių internete, kurios gali patikrinti, ar el. laiškas yra teisėtas. Prieš persiųsdami atlikite laiško, kuris, įtariate, yra apgaulė, paiešką internete.

Sukčiavimas apsimetant

Terminas „sukčiavimas apsimetant“ apibrėžia nusikalstamą veiklą, kurią atliekant naudojami socialinės inžinerijos metodai (manipuliavimas vartotojais siekiant išgauti konfidencialią informaciją). Šios veiklos tikslas – gauti prieigą prie slaptų duomenų, tokių kaip banko sąskaitų numeriai, PIN kodai ir t. t.

Prieiga paprastai gaunama nusiuntus el. laišką apsimetant patikimu asmeniu arba įmone (pvz., finansine institucija, draudimo įmone). El. laiškas gali atrodyti labai autentiškai, o jo grafika bei turinys gali būti nukopijuoti iš šaltinio, kurį jis imituoja. Jūsų dėl kokių nors priežasčių (duomenų tikrinimas, finansinės operacijos) paprašys įvesti kai kuriuos asmeninius duomenis – banko sąskaitų numerius arba vartotojų vardus ir slaptažodžius. Pateikus šiuos duomenis jie gali būti lengvai pavogti ir panaudoti nusikalstamiems tikslams įgyvendinti.

Bankai, draudimo bendrovės ir kitos teisėtos įmonės niekada neprašo pateikti vartotojų vardų ir slaptažodžių neprašytuose el. laiškuose.

Brukalo suktybių atpažinimas

Apskritai yra keli požymiai, padedantys aptikti brukalą (nepageidaujamus el. laiškus) jūsų pašto dėžutėje. Jeigu laiškas atitinka bent keletą toliau pateikiamų kriterijų, greičiausiai tai yra brukalas.

- Siuntėjo adreso nėra jūsų kontaktų sąraše.
- Jums siūloma didelė pinigų suma, tačiau jūsų pirmiausia prašoma pervesti nedidelę sumą.
- Jūsų dėl kokių nors priežasčių (duomenų tikrinimas, finansinės operacijos) prašo įvesti kai kuriuos asmeninius duomenis – banko sąskaitų numerius arba vartotojų vardus ir slaptažodžius.
- Jis parašytas užsienio kalba.
- Jums siūlo pirkti produktą, kuris jūsų nedomina. Jeigu vis tiek nuspręsite pirkti, įsitikinkite, kad laiško siuntėjas yra patikimas tiekėjas (pasiteiraukite originalaus produkto gamintojo).
- Kai kurie žodžiai klaidingai parašyti bandant suklaidinti jūsų brukalo filtrą. Pavyzdžiui „vaigra“ vietoj „viagra“.

Taisyklės

Kalbant apie apsaugos nuo brukalo sprendimus ir el. pašto programas, taisyklės padeda manipuliuoti el. pašto funkcijomis. Jas sudaro dvi loginės dalys:

1.Sąlyga (pvz., gaunamas laiškas iš tam tikro adreso arba su tam tikra el. laiško tema)

2.Veiksmas (pvz., laiško pašalinimas arba perkėlimas į nurodytą aplanką)

Taisyklių skaičius ir deriniai gali būti skirtingi įvairiuose apsaugos nuo brukalo sprendimuose. Šios taisyklės padeda apsisaugoti nuo brukalo (nepageidaujamų el. laiškų). Tipiniai pavyzdžiai:

1. Sąlyga: gaunamame el. laiške yra kai kurie žodžiai, paprastai randami brukalo laiškuose
2. Veiksmas: naikinti laišką

1. Sąlyga: gaunamas el. laiškas turi priedą su plėtiniu .exe
2. Veiksmas: naikinti priedą, o laišką pateikti į pašto dėžutę

1. Sąlyga: gaunamas el. laiškas atėjo iš jūsų darbdavio
2. Veiksmas: perkelti pranešimą į aplanką „Darbas“

Rekomenduojame apsaugos nuo brukalo programose naudoti kelių taisyklių derinius, kad būtų palengvinamas administravimas ir užtikrinamas efektyvesnis brukalo filtravimas.

Baltasis sąrašas

Apskritai baltasis sąrašas yra elementų arba asmenų, kurie yra priimtini arba kuriems suteiktas leidimas, sąrašas. Terminu „el. pašto baltasis sąrašas“ (leidžiami adresai) apibrėžiamas kontaktų, iš kurių naudotojas nori gauti pranešimus, sąrašas. Tokie baltieji sąrašai sudaromi remiantis raktažodžiais, ieškomais el. pašto adresuose, domeno vardais ar IP adresais.

Jeigu baltasis sąrašas veikia „išskirtiniu režimu“, pranešimai iš visų kitų adresų, domenų ar IP adresų nebus gaunami. Jeigu baltasis sąrašas nėra išskirtinis, tokie laiškai nebus naikinami, tačiau filtruojami kitais būdais.

Baltasis sąrašas yra paremtas priešingu principu nei juodasis sąrašas. Baltuosius sąrašus santykinai paprasta tvarkyti, daug paprasčiau nei juoduosius sąrašus. Mes rekomenduojame naudoti ir baltąjį, ir juodąjį sąrašus, kad efektyviau būtų filtruojamas brukalas.

Juodasis sąrašas

Apskritai juodasis sąrašas yra nepageidaujamų arba draudžiamų elementų ar asmenų sąrašas. Virtualiajame pasaulyje tai yra metodika, leidžianti priimti laiškus iš visų šiame sąraše nesančių vartotojų.

Yra dviejų tipų juodieji sąrašai: Vartotojų sukurti naudojant savo apsaugos nuo brukalo programas ir

profesionalūs, reguliariai atnaujinami juodieji sąrašai, kuriuos kuria specializuotos institucijos (juos galima rasti internete).

Svarbu naudoti juoduosius sąrašus, kad būtų sėkmingai blokuojamas brukalas, tačiau juos sunku prižiūrėti, nes kasdien atsiranda naujų elementų, kuriuos reikia blokuoti. Mes rekomenduojame naudoti ir baltąjį, ir juodąjį sąrašus, kad veiksmingiausiai būtų filtruojamas brukalas.

Išimtis

Išimčių sąraše paprastai būna galimai apgaulingi el. pašto adresai, iš kurių siunčiamas brukalas. El. laiškai, gauti iš adresų, kurie nurodyti išimčių sąraše, visada bus nuskaitomi ieškant brukalo. Pagal numatytuosius nustatymus išimčių sąraše yra visi esamų el. pašto programos paskyrų adresai.

Serverio pusės valdymas

Serverio pusės valdymas yra masinio brukalo aptikimo metodika, paremta gautų laiškų skaičiumi ir vartotojų reakcija. Kiekvienas laiškas palieka unikalų skaitmeninį „pėdsaką“, paremtą laiško turiniu. Unikalus ID numeris nieko nesako apie el. laiško turinį. Du identiški laiškai turės identiškus pėdsakus, o skirtingi laiškai turės skirtingus pėdsakus.

Jeigu laiškas pažymėtas kaip brukalas, jo pėdsakas siunčiamas į serverį. Jeigu serveris gauna daugiau identiškų pėdsakų (atitinkančių tam tikrą brukalo laišką), pėdsakas yra išsaugomas brukalo pėdsakų duomenų bazėje. Nuskaitydama gaunamus laiškus programa siunčia laiškų pėdsakus į serverį. Serveris grąžina informaciją, kurie pėdsakai atitinka laiškus, vartotojo jau pažymėtus kaip brukalas.

Išplėstinis atminties skaitytuvas

Išplėstinis atminties skaitytuvas veikia kartu su įsilaužimų blokatoriumi ir sustiprina apsaugą nuo kenkėjiškų programų, kurios buvo sukurtos siekiant išvengti apsaugos nuo kenkėjiškų programų produktų pasitelkiant klaidinimo ir (arba) šifravimo priemones. Tais atvejais, kai įprastinės emuliacijos ar euristikos priemonės negali aptikti grėsmės, išplėstinis atminties skaitytuvas gali nustatyti įtartiną veiklą ir nuskaityti grėsmes, jei jos pasirodo sistemos atmintyje. Šis sprendimas efektyviai saugo nuo sunkiai aptinkamų kenkėjiškų programų.

Kitaip nei įsilaužimų blokatorius, išplėstiniame atminties skaitytuve naudojamas metodas, pagal kurį aptinkamas jau vykdytas procesas, todėl yra pavojus, kad prieš aptinkant kenkėjišką veiksmą jis jau gali būti atliktas; tačiau tuo atveju, kai to nepavyko padaryti naudojantis kitais metodais, ši priemonė suteikia papildomą apsaugos lygmenį.

Banko mokėjimų apsauga

Bankininkystės ir mokėjimų apsauga – tai papildomas apsaugos lygis, skirtas finansiniams duomenims apsaugoti, kai atliekate operacijas internetu.

ESET Smart Security Premium ir ESET Internet Security yra integruotas sąrašas su iš anksto nustatytomis svetainėmis, kurioms bus atidaroma Saugi naršyklė. Pridėti svetainių ar redaguoti svetainių sąrašą galite produkto konfigūracijoje.

Įjunkite nustatymą „Apsaugoti visas naršykles“, kad visos palaikomos žiniatinklio naršyklės būtų paleidžiamos saugiuoju režimu.

Jei reikia daugiau informacijos apie šią funkciją, skaitykite šiuos ESET žinių bazės straipsnius:

- Kaip naudotis ESET bankininkystės ir mokėjimų apsauga?
- Banko mokėjimų apsaugos pristabdymas arba išjungimas ESET „Windows“ namų produktams
- ESET banko mokėjimų apsauga – dažniausios klaidos

HTTPS Šifruoto ryšio naudojimas yra būtinas norint atlikti apsaugotą naršymą. Bankininkystės ir mokėjimų apsaugą palaiko šios naršyklės:

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

Atidrykite nustatymą „Bankininkystės ir mokėjimų apsauga“ pageidaujamoje žiniatinklio naršyklėje

Atidarant nustatymą „Bankininkystės ir mokėjimų apsauga“ tiesiai iš skirtuko **Įrankiai** produkto meniu, jis atidaromas žiniatinklio naršyklėje, kurią Windows nustatėte kaip numatytąją. Priešingu atveju, atidarius pageidaujamą žiniatinklio naršyklę (ne iš produkto meniu), svetainės iš apsaugotų svetainių sąrašo bus nukreiptos į to paties tipo žiniatinklio naršyklę, apsaugotą ESET.

Apsauga nuo įtraukimo į užgrobtų kompiuterių tinklą

Apsauga nuo botnet aptinka kenkėjišką programinę įrangą, analizuodama savo tinklo ryšio protokolus. Užgrobtų kompiuterių tinklo formavimo kenkimo programinė įranga dažnai kinta, lyginant su tinklo protokolais, kurie kelis pastaruosius metus nekito. Ši nauja technologija padeda ESET nugalėti kenkimo programinę įrangą, kuri mėgina išvengti aptikimo ir prijungti jūsų kompiuterį prie užgrobtų kompiuterių tinklo.

DNR aptikimas

Yra įvairių aptikimo tipų – nuo konkrečių informacijos rinkinių iki ESET DNR aptikimo, sudėtingų kenkėjiškų veiksmų ir kenkėjiškos programinės įrangos charakteristikų apibrėžčių. Nors įsilaužėliai gali lengvai pakeisti ar užmaskuoti kenkėjišką kodą, pakeisti objektų veiksmus yra sudėtingiau, o ESET DNR aptikimo funkcija yra sukurta taip, kad šį principą išnaudotų.

Atliekame išsamią kodo analizę bei išimame „genus“, atsakingus už jo veiksmus, ir sudarome ESET DNR aptikimo atvejus, kurie naudojami įvertinti galimai įtartiną kodą, nepriklausomai nuo to, ar jis rastas diske, ar veikiančių procesų atmintyje. DNR aptikimas gali atpažinti konkrečius žinomus kenkėjiškos programinės įrangos pavyzdžius, naujus žinomos kenkėjiškos programinės įrangos grupės variantus ar anksčiau nematytą ar nežinomą kenkėjišką programinę įrangą, kurioje yra genų, nurodančių kenkėjiškus veiksmus.

ESET LiveGrid®

ESET LiveGrid® (pagal ESET ThreatSense.Net išplėstinę ankstyvojo įspėjimo sistemą) naudoja duomenis, kuriuos ESET pateikia vartotojai iš viso pasaulio ir siunčia juos į ESET tyrimų laboratoriją. Pateikdama įtartinus pavyzdžius ir metaduomenis iš pasaulio ESET LiveGrid® suteikia mums galimybę greitai prisitaikyti prie klientų poreikių ir padeda ESET reaguoti į naujausias grėsmes.

ESET kenkėjiškos programinės įrangos tyrėjai pasinaudodami šia informacija kuria tikslias pasaulinių grėsmių pobūdžio ir masto momentines ekrano kopijas, kurios padeda mums sutelkti jėgas reikiamose tikslinėse srityse. ESET LiveGrid® duomenys yra labai svarbūs nustatant automatinio apdorojimo prioritetus.

Be to, per šią priemonę veikia reputacijos sistema, padedanti gerinti bendrąjį mūsų apsaugos nuo kenkėjiškos programinės įrangos sprendimų efektyvumą. Vartotojas gali patikrinti vykdomų procesų ir failų reputaciją tiesiog naudodamasis programos sąsaja arba kontekstiniu meniu su papildoma informacija, gauta iš ESET LiveGrid®. Kai vykdomasis failas arba archyvas tikrinamas naudotojo sistemoje, jo maišos žyma pirmiausia sulyginama su baltajam ir juodajam sąrašams priklausančių elementų duomenų baze. Jei jis randamas baltajame sąraše, patikrintas failas laikomas nepavojingu ir pažymima, kad jo galima neįtraukti į vėlesnius nuskaitymus. Jei jis priklauso juodajam sąrašui, įvertinus grėsmės pobūdį imamasi atitinkamų veiksmų. Jei jo atitikmenų nerandama, atliekamas išsamus failo nuskaitymas. Remiantis šio nuskaitymo rezultatais, failai suskirstomi į kategorijas priskiriant juos grėsmėms arba ne grėsmėms. Šis metodas teigiamai veikia nuskaitymo efektyvumą. Ši reputacijos sistema suteikia galimybę efektyviai aptikti kenkėjiškos programinės įrangos pavyzdžius dar prieš pristatant jų parašus į naudotojų kompiuterius per atnaujintą virusų duomenų bazę (tai atliekama kelis kartus per dieną).

Be ESET LiveGrid® sistemos, ESET LiveGrid® surinks informaciją apie naujai aptiktas grėsmes, susijusias su jūsų kompiuteriu. Ši informacija gali turėti failo, kuriame atsirado grėsmė, pavyzdį arba kopiją, kelią į šį failą, failo pavadinimą, datą ir laiką, procesą, kurio metu grėsmė atsirado jūsų kompiuteryje, ir informaciją apie jūsų kompiuterio operacinę sistemą.

> **ESET LiveGrid® serveriai**
> Mūsų ESET LiveGrid® serveriai yra Bratislavoje, Vienoje ir San Diege, bet šie serveriai tik atsako į klientų užklausas. Pateikti pavyzdžiai apdorojami tik Bratislavoje, Slovakijoje.

> **ESET LiveGrid® įjungimas arba išjungimas ESET produktuose**
> Jei reikia išsamesnių ir iliustruotų nurodymų, kaip įjungti arba išjungti ESET LiveGrid® ESET produktuose, peržiūrėkite ESET žinių bazės straispnį.

Įsilaužimų blokatorius

Įsilaužimų blokatorius sustiprina programas, į kurias įsilaužiama dažniausiai, pavyzdžiui, žiniatinklio naršykles, PDF skaitymo programas, el. pašto programas ir „Microsoft Office“ komponentus, bei saugo nuo ROP atakų. Įsilaužimų blokatorius prieinamas ir įgalintas pagal numatytuosius nustatymus visuose ESET „Windows“ namų produktuose, ESET produktuose, skirtuose „Windows Server“, ir ESET įrenginių produktuose, skirtuose „Windows“.

Jis stebi procesų veikimą ir ieško įtartinos veiklos, kuri gali nurodyti galimą įsilaužimą.

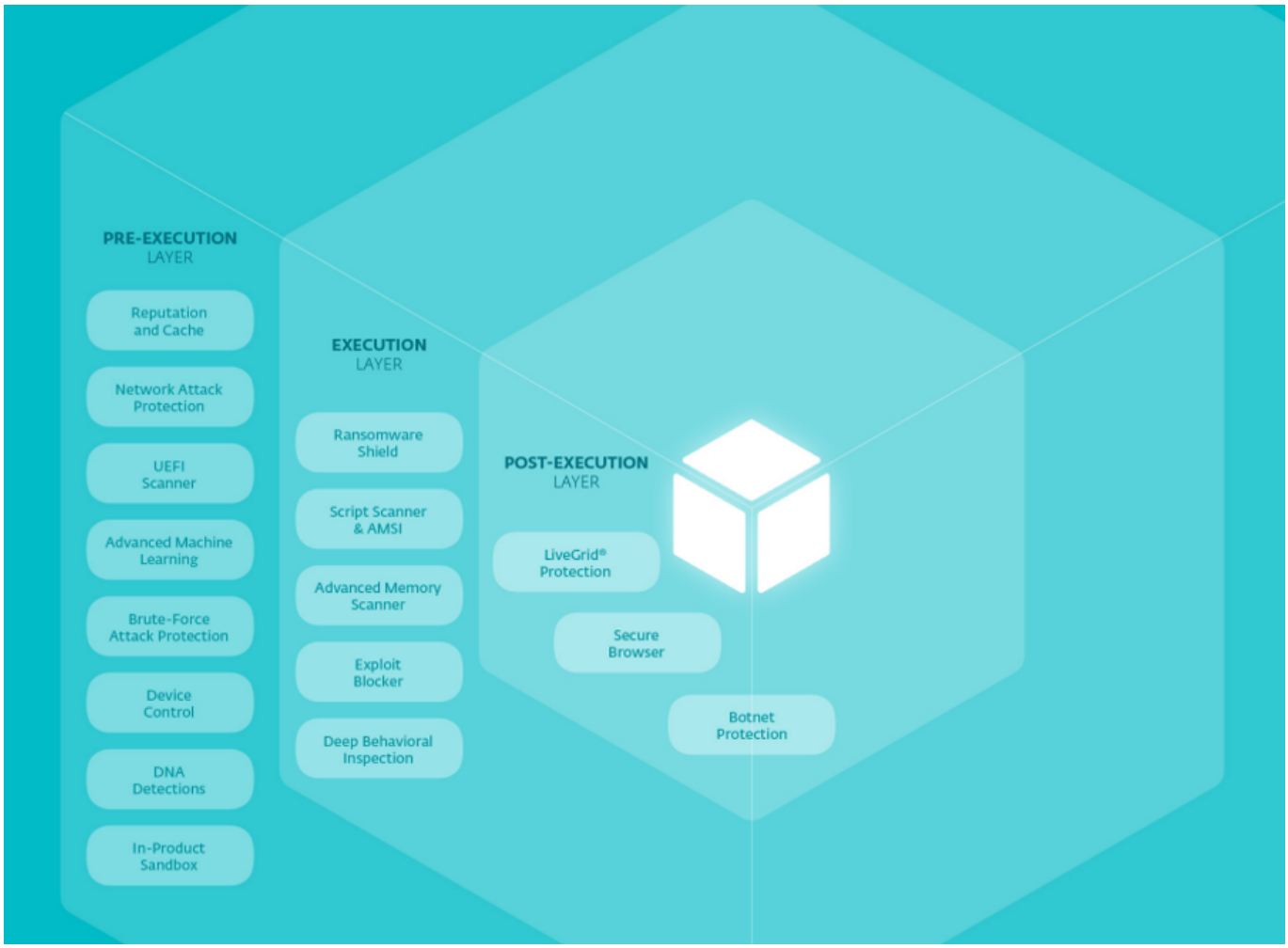
Kai įsilaužimų blokatorius aptinka įtartiną procesą, jis iškart nutraukia procesą ir įrašo duomenis apie grėsmę bei nusiunčia juos į ESET LiveGrid® debesų sistemą. Šie duomenys apdorojami ESET tyrimų laboratorijoje ir naudojami visų vartotojų apsaugai nuo nežinomų grėsmių bei pačių naujausių atakų (naujai išleistos kenkimo programinės įrangos, neturinčios iš anksto sukonfigūruotų apsaugos priemonių) stiprinti.

„Java“ įsilaužimų blokatorius

„Java“ įsilaužimų blokatorius – tai esamos įsilaužimų blokatoriaus technologijos plėtinys. Jis stebi „Java“ vykdymą ir ieško į įsilaužimus panašios elgsenos. Užblokuoti pavyzdžiai gali būti pateikti kenkėjiškos programinės įrangos analitikams, kad jie galėtų sukurti juos įvairiuose sluoksniuose blokuoti galintį kodą (URL blokavimas, failų atsisiuntimas ir pan.).

ESET LiveSense

ESET naudoja daug unikalių, patentuotų, daugiasluoksnių apsaugos technologijų, kurios veikia kartu kaip „ESET LiveSense“. Toliau pateiktame paveikslėlyje pavaizduotos kai kurios pagrindinės ESET technologijos ir apytiksliai nurodyta, kada ir kur jos gali aptikti ir galiausiai blokuoti grėsmę jos gyvavimo ciklo sistemoje metu.



Mašininis mokymasis

ESET dirba su mašininio mokymosi algoritmais nuo 1990 m., kad aptiktų grėsmes ir užkirstų joms kelią. 1998 m. į ESET produkto aptikimo modulį įtraukti neuroniniai tinklai.

Mašininis mokymasis apima DNR aptikimą pasitelkus mašininio mokymosi pagrindu veikiančius modelius, siekiant užtikrinti našų darbą tiek prisijungus prie debesies, tiek neprisijungus. Mašininio mokymosi algoritmai taip pat neatsiejami nuo pradinio gaunamų pavyzdžių rūšiavimo, jų klasifikavimo bei atvaizdavimo įsivaizduojamame

kibernetinio saugumo žemėlapyje.

ESET yra sukūrusi savo mašininio mokymosi modulį, kuriame naudojami bendri neuroninių tinklų (pvz., giliojo mokymosi ir ilgos trumpalaikės atminties) ir rūpestingai atrinktų šešių klasifikavimo algoritmų pajėgumai. Taip modulis gali sugeneruoti konsoliduotus rezultatus ir padėti tinkamai sužymėti gaunamus pavyzdžius kaip nepavojingus, galimai nepageidaujamus arba kenkėjiškus.

ESET mašininio mokymosi modulis tiksliai suderintas taip, kad veiktų su kitomis apsauginėmis technologijomis, pvz., DNR, smėlio dėže ir atminties analize bei elgsenos ypatumų išskleidimu, kad aptikimas būtų tikslus, o klaidingai teigiamų rezultatų – kuo mažiau.

Skaitytuvo konfigūracija atliekant ESET produktų išplėstinį nustatymą

- ESET „Windows“ namų produktai (nuo 13.1 versijos)
- ESET „Windows“ įrenginių produktai (nuo 7.2 versijos)

Tinklo apsauga nuo atakų

Tinklo apsauga nuo atakų – tai užkardos plėtinys, padedantis geriau aptikti žinomą tinklo pažeidžiamų vietų išnaudojimą. Vykdydamas bendrųjų pažeidžiamų vietų išnaudojimo paiešką dažniausiai naudojamuose protokoluose, pavyzdžiui, SMB, RPC ir RDP, jis pakeičia kitą svarbų apsaugos lygį, susijusį su plintančiomis kenkėjiškomis programomis, tinkle vykdomomis atakomis ir pažeidžiamų vietų išnaudojimu, kai dar nėra išleistos ar įdiegtos pataisos nuo šių grėsmių.

Apsauga nuo „Ransomware“

Apsauga nuo išpirkos reikalaujančių programų – tai elgsena paremtas aptikimo metodas, kuris stebi programų ir procesų, bandančių pakeisti failus taip, kaip tai darytų išpirkos reikalaujanti ar failų kodavimo programa, elgseną. Jei programos elgsena laikoma kenkėjiška arba jei reputacija paremto nuskaitymo rezultatai rodo, kad programa yra įtartina, programa užblokuojama ir procesas sustabdomas arba naudotojo prašoma ją užblokuoti ar leisti.

ESET LiveGrid® turi būti įjungta, kad funkcija „Apsauga nuo „Ransomware“ tinkamai veiktų. Peržiūrėkite mūsų ESET žinių bazės straipsnį, kad įsitikintumėte, jog ESET LiveGrid® įgalintas ir veikia jūsų ESET produkte.

Apsauga nuo scenarijumi paremtų atakų

Apsaugą nuo scenarijumi paremtų atakų sudaro apsauga nuo „javascript“ interneto naršyklėse ir apsaugos nuo kenkėjiškų programų nuskaitymo sąsaja (AMSI), sauganti nuo scenarijų „PowerShell“.

HIPS
Kad ši funkcija veiktų, būtina įjungti HIPS.

Apsaugą nuo scenarijumi paremtų atakų palaiko šios interneto naršyklės:

- Mozilla Firefox
- Google Chrome
- Internet Explorer

- Microsoft Edge

> **Naudokite palaikomą žiniatinklio naršyklę**
> Minimalios palaikomos interneto naršyklių versijos gali skirtis, nes gana dažnai keičiasi naršyklių failų parašai. Tačiau naujausia interneto naršyklės versija visada palaikoma.

Saugi naršyklė

Saugi naršyklė – tai papildomas apsaugos lygis, skirtas slaptiems duomenims apsaugoti, kai naršote internete (pvz., (pavyzdžiui, finansiniams duomenims, atliekant operacijas internetu).

ESET Endpoint Security 8 ir naujesnėje yra integruotas sąrašas su iš anksto nustatytomis svetainėmis, kurioms bus atidaroma apsaugota naršyklė. Pridėti svetainių ar redaguoti svetainių sąrašą galite produkto konfigūracijoje. Įdiegus, saugi naršyklė išjungiama pagal numatytuosius nustatymus.

Jei reikia daugiau informacijos apie šią funkciją, skaitykite šį ESET žinių bazės straipsnį.

HTTPS Šifruotasis ryšys yra būtina apsaugoto naršymo sąlyga. Jei norite naudotis saugiu naršymu, interneto naršyklė turi atitikti minimalius toliau pateikiamus reikalavimus.

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

> Tik Firefox ir Microsoft Edge yra palaikomos įrenginiuose su ARM procesoriais.

Atidarykite ESET saugią naršyklę pageidaujamoje žiniatinklio naršyklėje

Kai atidarote ESET saugią naršyklę tiesiai iš skirtuko **Įrankiai** produkto meniu, ESET saugi naršyklė atidaroma žiniatinklio naršyklėje, kurią nustatėte kaip numatytąją. Priešingu atveju, atidarius pageidaujamą žiniatinklio naršyklę (ne iš produkto meniu), ESET vidinis sąrašas bus nukreiptas į to paties tipo žiniatinklio naršyklę, apsaugotą ESET.

UEFI skaitytuvas

Bendrosios išplėstinės programinės-aparatinės įrangos sąsajos (UEFI) skaitytuvas yra pagrindinio kompiuterio apsaugos nuo įsilaužimo sistemos (HIPS) dalis, sauganti UEFI programinę-aparatinę įrangą jūsų kompiuteryje. UEFI yra programinė-aparatinė įranga, kuri įkeliama į atmintį paleidimo proceso pradžioje. Kodas yra „flash“ atminties luste, prilituotame prie pagrindinės plokštės. Jį užkrėtę, įsilaužėliai gali įdiegti kenkėjišką programą, kuri išlieka net ir iš naujo įdiegus ir perkrovus sistemą. Kenkėjiška programinė įranga taip pat lengvai gali likti nepastebėta apsaugos nuo kenkėjiškos programinės įrangos sprendimų, nes dauguma jų netikrina šio sluoksnio.

UEFI skaitytuvas įjungiamas automatiškai. Taip pat galite paleisti kompiuterio nuskaitymą rankiniu būdu, pagrindiniame programos lange spustelėdami **Kompiuterio nuskaitymas** > **Išplėstiniai nuskaitymai** > **Pasirinktinis nuskaitymas** ir pasirinkdami tikslą **Įkrauti sektorius / UEFI**.

Jei jūsų kompiuteris jau užkrėstas UEFI kenkėjiška programine įranga, perskaitykite šį ESET žinių bazės straipsnį:
Mano kompiuteris užkrėstas UEFI kenkėjiška programine įranga. Ką turėčiau daryti?

Kanarinis failas

Kanarinis failas – tai suklastotas kompiuterinis dokumentas, patalpintas tarp tikrų dokumentų, kad būtų galima anksti aptikti neteisėtą prieigą prie duomenų, jų kopijavimą ar keitimą.

Aklavietė

Aklavietė yra situacija, kai kiekvienas kompiuterio procesas laukia ištekliaus, priskirto kitam procesui. Esant tokiai situacijai, nė vienas iš procesų nevykdomas, nes reikalingą išteklių turi kitas procesas, kuris taip pat laukia, kol atsilaisvins kitas išteklius. Svarbu užkirsti kelią aklavietei prieš jai atsirandant. Išteklių planuoklė, kuri padeda operacinei sistemai sekti visus skirtingiems procesams skirtus išteklius, gali aptikti aklavietės įvykį. Aklavietė gali atsirasti, jei vienu metu susiklosto šios keturios sąlygos:

- **Jokio prevencinio veiksmo** – išteklius gali būti atlaisvintas tik savanoriškai, kai procesas jį laiko po to, kai šis procesas užbaigia savo užduotį.
- **Abipusis išskyrimas** – specialus dvejetainio semaforo tipas, naudojamas prieigai prie bendro naudojimo ištekliaus kontroliuoti. Tai leidžia blokuoti dabartines didesnio prioriteto užduotis trumpiausią įmanomą laiką.
- **Laikykite ir palaukite** – esant tokiai sąlygai, procesai turi būti sustabdyti nuo vieno ar kelių išteklių laikymo, tuo pat metu laukiant vieno ar kelių kitų išteklių.
- **Ciklinis laukimas** – nustatomas bendras visų išteklių tipų užsakymas. Esant cikliniam laukimui taip pat reikalaujama, kad kiekvienas procesas prašytų išteklių didėjančia vardijimo tvarka.

Yra trys būdai, kaip išeiti iš aklavietės:

- Neleiskite sistemai atsidurti aklavietėje.
- Leiskite atsirasti aklavietei, tada iš anksto numatykite, kad jai atsiradus išspręsite šį klausimą.
- Atsiradus aklavietei, paleiskite sistemą iš naujo.