

ESET Glossary

Vodič za korisnike

[Kliknite ovdje za prikazivanje verzije mrežne pomoći dokumenta](#)

Autorska prava ©2023 tvrtke ESET, spol. s r.o.

ESET Glossary razvila je tvrtka ESET, spol. s r.o.

Za više informacija posjetite <https://www.eset.com>.

Sva prava pridržana. Nijedan dio ove dokumentacije ne smije se reproducirati, pohranjivati u sustavu za dohvaćanje ili prenositi u bilo kojem obliku ili na bilo koji način, elektronički, mehanički, fotokopiranjem, snimanjem, skeniranjem ili na drugi način bez dopuštenja autora u pisanim oblicima.

ESET, spol. s r.o. zadržava pravo promijeniti bilo koji od opisanih softvera aplikacije bez prethodne najave.

Tehnička podrška: <https://support.eset.com>

REV. 19.04.2023.

1 Uvod u ESET-ov rječnik	1
1.1 Adware	1
1.2 Botnet	1
1.3 Lažno pozitivan rezultat (LPR)	1
1.4 Packer program	2
1.5 Potencijalno nesigurne aplikacije	2
1.6 Potencijalno nepoželjne aplikacije	2
1.7 Ransomware	6
1.8 Rootkit	7
1.9 Programiranje usmjereni na povratak	7
1.10 Spyware	7
1.11 Trojan	8
1.12 Virus	8
1.13 Crv	9
1.14 Krađa korisničkih podataka	9
1.15 Onečišćenje DNS-a	9
1.16 DoS napad	10
1.17 Napad kroz ICMP	10
1.18 Skeniranje portova	10
1.19 SMB Relay	10
1.20 Desinkronizacija TCP-a	11
1.21 Napad crva	11
1.22 Onečišćenje ARP predmemorije	11
2 Prijetnje putem e-pošte	12
2.1 Oglasni	12
2.2 Lažne obavijesti (Hoax)	12
2.3 Phishing	13
2.4 Prepoznavanje spam prijevara	13
2.4 Pravila	14
2.4 Popis pouzdanih adresa	14
2.4 Popis spam adresa	14
2.4 Iznimka	15
2.4 Provjera sa serverske strane	15
2.5 Napredni skener memorije	15
2.6 Zaštita bankarstva i plaćanja	15
2.7 Zaštita od botneta	16
2.8 Otkrivanja DNA	16
2.9 ESET LiveGrid®	17
2.10 Sprječavanje ranjivosti	17
2.11 Zaštita od zloupotrebe Jave	18
2.12 ESET LiveSense	18
2.13 Strojno učenje	18
2.14 Zaštita od mrežnog napada	19
2.15 Zaštita od ransomwarea	19
2.16 Zaštita od napada na temelju skripti	19
2.17 Zaštićeni preglednik	20
2.18 Skener za UEFI	20
2.19 Lažna datoteka	21
2.20 Mrtva petlja	21

Uvod u ESET-ov rječnik

ESET-ov rječnik pruža sveobuhvatan pregled aktualnih prijetnji i ESET-ovih tehnologija koje vas štite od njih.

Teme su podijeljene u sljedeća poglavlja u kojima se opisuju:

- [Otkrivenе prijetnјe](#) – uključuju računalne viruse, crve, trojance, potencijalno neželjene aplikacije itd.
- [Daljinski napadi](#) – prijetnje koje se događaju na lokalnim mrežama ili internetu
- [Prijetnje putem e-pošte](#) – uključujući lažne obavijesti (hoax), phishing, prijevare i ostalo.
- [ESET-ove tehnologije](#) – funkcije programa dostupne u ESET-ovim sigurnosnim rješenjima

Adware

Adware je skraćenica od advertising-supported software što znači softver koji se financira oglasima. Programi koji prikazuju oglasni materijal pripadaju u tu kategoriju. Adware u web pregledniku često automatski otvara novi prozor koji sadrži oglase ili pak mijenja početnu stranicu web preglednika. Adware se često isporučuje u paketu s besplatnim programima, čime se inženjerima koji razvijaju te (obično korisne) aplikacije pokrivaju troškovi rada.

Adware sam po sebi nije opasan – osim što korisnicima dosađuje oglasima. Opasnost se krije u činjenici da adware ponekad provodi i funkcije praćenja (kao što to radi i spyware).

Ako odlučite koristiti neki besplatni proizvod, posebnu pozornost obratite na instalacijski program. Većina instalacijskih programa obavijestit će vas o instaliranju dodatnog adwarea. Često ćete moći odustati od instalacije adwarea i instalirati samo program koji želite.

Neki se programi ne mogu instalirati ako se ne instalira i adware ili njihove funkcije mogu biti ograničene. To znači da adware često može pristupati sustavu na „legitiman“ način jer su korisnici na to pristali. U takvom je slučaju bolje sprječiti nego liječiti. Ako se na računalu otkrije datoteka koja spada u adware, preporučuje se obrisati je jer postoji velika vjerojatnost da sadrži zlonamjeran kod.

Botnet

Bot ili web robot automatizirani je zlonamjerni program koji skenira blokove mrežnih adresa i zaražava nezaštićena računala. Tako hakeri istodobno mogu preuzeti kontrolu nad više računala i pretvoriti ih u botove (ili tzv. zombije). Hakeri obično koriste botove kako bi zarazili velik broj računala, koja tada čine mrežu ili botnet. Kada botnet dospije na vaše računalo, može se koristiti u napadima uskraćivanja usluge (DDoS), za proxy te za obavljanje automatiziranih zadataka putem interneta bez vašeg znanja (primjerice, slanje spam poruka, virusa ili krađu osobnih podataka kao što su bankovni podaci ili brojevi kreditnih kartica).

Lažno pozitivan rezultat (LPR)

U stvarnosti ne postoji jamstvo 100 %-tne stopi otkrivanja prijetnji, kao ni 0 %-tna vjerojatnost da se izbjegne pogrešna kategorizacija očišćenih objekata kao prijetnji.

Lažno pozitivan rezultat čista je datoteka ili aplikacija koja je pogrešno klasificirana kao zlonamjerni program ili

potencijalno nepoželjna aplikacija.

Packer program

Arhivator je runtime izvršna datoteka koja komprimira nekoliko vrsta zlonamjernog softvera u jedan paket.

Najčešći arhivatori su UPX, PE_Compact, PKLite i ASPack. Isti se zlonamjerni softver može otkriti drukčije kad se komprimira pomoću drugačijeg arhivatora. Osim toga, arhivatori mogu natjerati svoje "potpise" da s vremenom mutiraju zbog čega je zlonamjerni softver teže otkriti i ukloniti.

Potencijalno nesigurne aplikacije

Postoji mnogo legitimnih programa kojima se pojednostavnjuje administracija umreženih računala. Međutim, u pogrešnim se rukama takvi programi mogu zloupotrijebiti. ESET pruža mogućnost otkrivanja takvih aplikacija.

Potencijalno nesigurne aplikacije naziv je koji se koristi za komercijalan, legitiman softver. Ta klasa obuhvaća programe kao što su alati za udaljeni pristup, aplikacije za probijanje lozinki i keyloggere (programe koji zapisuju svaki korisnikov pritisak tipke).

Ako otkrijete da se na računalu izvršava neka potencijalno nesigurna aplikacija (a vi je niste instalirali), obratite se administratoru mreže ili uklonite tu aplikaciju.

Potencijalno nepoželjne aplikacije

Grayware ili potencijalno neželjena aplikacija (PUA) široka je kategorija softvera čija namjera nije nedvosmisleno zlonamjerna poput drugih vrsta zlonamjernih programa, kao što su virusi ili trojanci. Međutim, takvi programi mogu instalirati dodatne neželjene programe, promijeniti rad digitalnog uređaja ili provesti aktivnosti koje korisnik nije dopustio ili koje ne očekuje.

Kategorije koje se mogu smatrati graywareom uključuju: softver koji prikazuje oglase, omotače za preuzimanje, različite alatne trake preglednika, softver s varljivim ponašanjem, bundleware, trackware, proxyware (aplikacije za dijeljenje interneta), rudare kriptovaluta, čistače registra (samo u operacijskim sustavima Windows) ili druge vrste graničnog softvera, softver koji upotrebljava nedopuštene ili nemoralne poslovne postupke (iako se doima zakonitim) i softver koji je krajnji korisnik procijenio nepoželjnim kada je postao svjestan toga što će softver učiniti ako mu se dopusti instalacija.

Potencijalno nesigurna aplikacija softver je koji je sâm po sebi zakonit (i može biti komercijalan), ali ga napadač može zloupotrijebiti. Korisnici ESET-ovog softvera mogu aktivirati ili deaktivirati otkrivanje takvih vrsta aplikacija.

U nekim će situacijama korisnik možda ocijeniti da su prednosti potencijalno neželjene aplikacije veće od rizika koji predstavlja. ESET iz tog razloga takvim aplikacijama dodjeljuje kategoriju manjeg rizika u odnosu na ostale vrste zlonamjernog softvera poput trojanskih softvera ili crva.

- [Upozorenje – pronađena je potencijalno nepoželjna aplikacija](#)
- [Postavke](#)
- [Softverski programi otvorenog koda](#)

- [Čistači registra](#)
- [Potencijalno nepoželjan sadržaj](#)

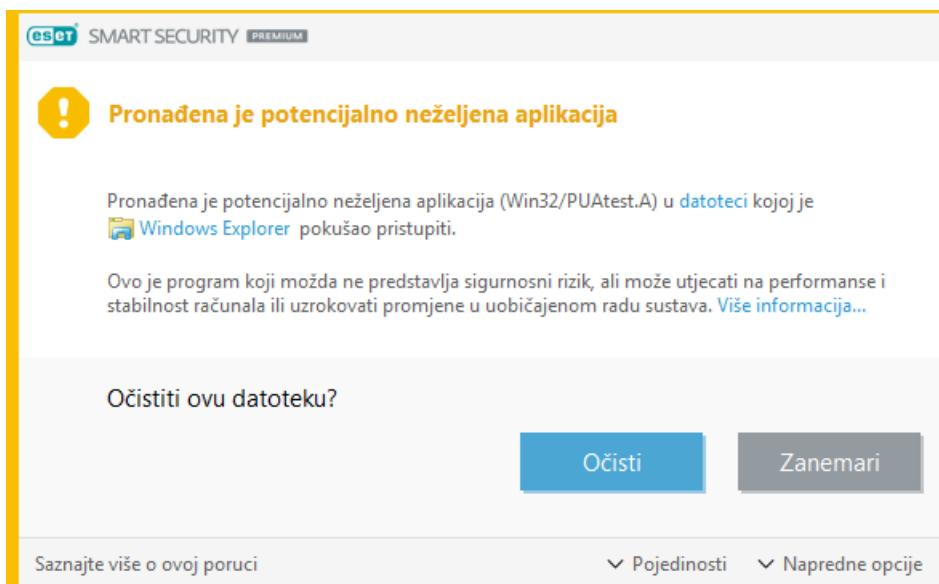
Ilustrirane upute

- ✓ Da biste skenirali i uklonili potencijalno nepoželjne aplikacije (PNA) u ESET-ovim Windows programima za kućne korisnike, pogledajte naš [članak u ESET-ovoj bazi znanja](#).

Upozorenje – pronađena je potencijalno nepoželjna aplikacija

Kada se otkrije potencijalno neželjena aplikacija, možete odlučiti koju će ste radnju poduzeti:

- 1.Očisti / prekini vezu:** ova opcija prekida radnju i sprečava ulazak potencijalno nepoželjne aplikacije u vaš sustav.
Vidjet ćete opciju **Prekini vezu** za obavijesti o potencijalno nepoželjnim aplikacijama tijekom preuzimanja s web stranice i opciju **Očisti** za obavijesti o datoteci na disku.
- Zanemari:** ova opcija omogućuje ulazak potencijalno nepoželjne aplikacije u sustav.
- Izuzmi od otkrivanja:** da biste otkrivenoj datoteci koja se već nalazi na računalu dopustili da se ubuduće pokreće bez prekida, kliknite **Napredne opcije**, a zatim označite potvrđni okvir uz stavku **Izuzmi od otkrivanja** i kliknite **Zanemari**.
- Izuzmi potpis od otkrivanja:** da biste svim datotekama prepoznatima prema određenom nazivu otkrivanja (potpisu) ubuduće dopustili pokretanje na računalu bez prekida (iz postojećih datoteka ili preuzimanjem s interneta), kliknite **Napredne opcije**, označite potvrđni okvir uz stavku **Izuzmi potpis od otkrivanja** i kliknite **Zanemari**. Ako se neposredno nakon toga prikažu dodatni prozori otkrivanja s identičnim nazivom otkrivanja, kliknite Zanemari da biste ih zatvorili (svi su dodatni prozori povezani s otkrivanjem do kojeg je došlo prije nego što ste izuzeli potpis od otkrivanja).



Postavke

Prilikom instalacije ESET-ovog proizvoda možete odlučiti hoćete li aktivirati otkrivanje potencijalno neželjenih aplikacija na dolje prikazan način:

Što više to bolje. Odaberite maksimalnu razinu zaštite.

Sustav za povratne informacije programa ESET LiveGrid® omogućuje prikupljanje informacija o sumnjivim objektima koje automatski obrađujemo kako bismo stvorili mehanizme za otkrivanje u našem cloud sustavu. Zatim te informacije odmah primjenjujemo kako bismo osigurali da naši korisnici imaju maksimalnu razinu zaštite.

- Aktiviraj sustav za povratne informacije programa ESET LiveGrid® (preporučuje se)
- Deaktiviraj sustav za povratne informacije programa ESET LiveGrid®

Otkrivanje potencijalno neželjenih aplikacija

ESET može otkriti [potencijalno neželjene aplikacije](#) i zatražiti pristanak prije nego što se instaliraju. Potencijalno neželjene aplikacije možda ne predstavljaju sigurnosni rizik, ali mogu utjecati na performanse računala, njegovu brzinu i pouzdanost ili pak uzrokovati promjene u uobičajenom radu. Obično se prije njihove instalacije traži pristanak korisnika.

- Aktiviraj otkrivanje potencijalno neželjenih aplikacija
- Deaktiviraj otkrivanje potencijalno neželjenih aplikacija

[Instaliraj](#)[Promijeni mapu za instalaciju](#)

Upozorenje

 Potencijalno neželjene aplikacije mogu instalirati adware, alatne trake ili mogu sadržavati druge neželjene i nesigurne funkcije programa.

Te postavke u svakom trenutku možete izmijeniti u postavkama programa. Da biste aktivirali ili deaktivirali otkrivane potencijalno neželjenih, nesigurnih ili sumnjivih aplikacija, slijedite ove upute:

1. [Otvorite ESET-ov program](#).
2. Pritisnite tipku **F5** da biste pristupili odjeljku **Napredno podešavanje**.
3. Kliknite **Modul detekcije** (u starijim verzijama poznat i kao **Antivirus** ili **Računalo**) i aktivirajte ili deaktivirajte opcije **Aktiviraj otkrivanje potencijalno nepoželjnih aplikacija**, **Aktiviraj otkrivanje potencijalno nesigurnih aplikacija** i **Aktiviraj otkrivanje sumnjivih aplikacija** prema vlastitom odabiru. Potvrdite tako da kliknete **U redu**.

MODUL DETEKCIJE 

Rezidentna zaštita sistemskih datoteka

Zaštita potpomognuta cloudom

Skeniranje

HIPS NADOGRADNJA 

MREŽNA ZAŠTITA

WEB I E-POŠTA 

KONTROLA UREĐAJA

ALATI

KORISNIČKO SUČELJE

OSNOVNO**OPCIJE SKENERA**Aktiviraj otkrivanje potencijalno neželjenih aplikacija  Aktiviraj otkrivanje potencijalno nesigurnih aplikacija  Aktiviraj otkrivanje sumnjivih aplikacija  **ANTI-STEALTH**Aktiviraj tehnologiju Anti-Stealth  **IZUZETI PROCESI**Procesi koji će se izuzeti iz skeniranja  **IZUZECI**Datoteke i mape koje će se izuzeti od skeniranja  

Standardno

 U redu

Odustani

Ilustrirane upute

Detaljnije upute o konfiguriranju programa tako da otkrivaju ili zanemaruju potencijalno neželjene aplikacije potražite u člancima ESET-ove baze znanja:

-  • [ESET NOD32 Antivirus / ESET Internet Security / ESET Smart Security Premium](#)
- [ESET Cyber Security za macOS / ESET Cyber Security Pro za macOS](#)
- [ESET Endpoint Security / ESET Endpoint Antivirus for Windows](#)
- [ESET Mobile Security za Android](#)

Softverski programi otvorenog koda

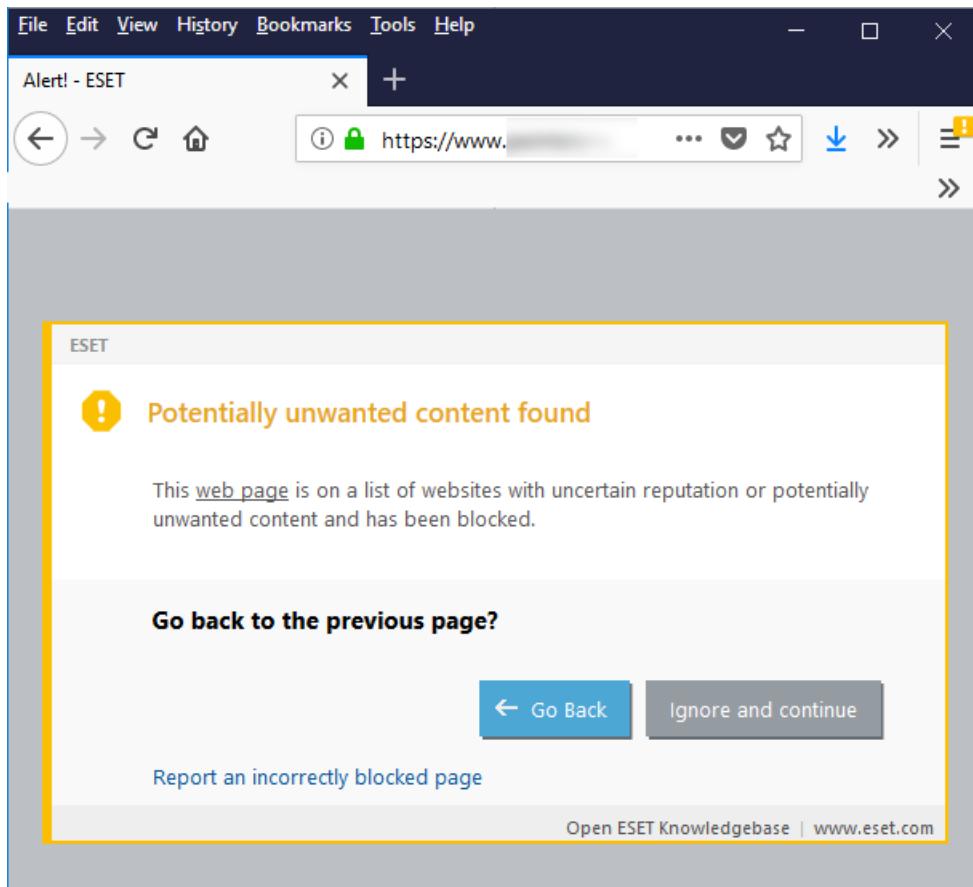
Softverski program otvorenog koda posebna je vrsta izmjene aplikacije koju upotrebljavaju neke web stranice za hosting datoteka. To je alat drugih dobavljača koji instalira program koji ste željeli preuzeti, ali s dodatnim softverom poput alatnih traka ili [adwarea](#). Dodatni softver isto tako može promijeniti početnu stranicu i postavke pretraživanja vašeg web preglednika. Osim toga, web stranice za hosting datoteka često ne šalju obavijesti prodavaču softvera ili korisnicima koji ga preuzimaju o izvršenim izmjenama i skrivaju mogućnosti za njihovo odbacivanje. Iz tog razloga ESET softverske programe otvorenog koda klasificira kao potencijalno neželjene aplikacije kako bi korisnicima omogućio da sami odaberu hoće li ih preuzeti ili ne.

Čistači registra

Čistači registra programi su koji vas mogu obavijestiti da baza podataka registra Windows zahtijeva redovito održavanje ili čišćenje. Upotrebom čistača registra mogu se unijeti određeni rizici u vaš računalni sustav. Uz to, neki čistači registra iznose tvrdnje o svojim prednostima koje nisu dokazane, ne mogu se provjeriti ili na drugi način potkrijepiti i/ili generiraju zavaravajuća izvješća o računalnom sustavu na temelju rezultata "besplatnog skeniranja". Cilj takvih zavaravajućih tvrdnji i izvješća jest navesti vas da kupite cijelovitu verziju ili pretplatu, obično bez mogućnosti procjene čistača registra prije plaćanja. Zbog toga ESET kategorizira takve programe kao potencijalno nepoželjne aplikacije i pruža vam mogućnost da ih dozvolite ili blokirate.

Potencijalno nepoželjan sadržaj

Ako je u vašem ESET-ovom programu aktivirano otkrivanje potencijalno nepoželjnih aplikacija, web stranice koje su poznate po promicanju takvih aplikacija ili po zavaravanju korisnika kako bi vršile radnje koje bi mogle negativno utjecati na njihov sustav ili iskustvo pregledavanja na internetu blokirat će se kao potencijalno nepoželjan sadržaj. Ako primite obavijest da je web stranica koju pokušavate posjetiti kategorizirana kao potencijalno nepoželjan sadržaj, možete kliknuti "**Vrati se natrag**" da biste napustili blokiranu web stranicu ili kliknuti "**Zanemari i nastavi**" da biste dozvolili učitavanje stranice.



Dodatne informacije o ovoj temi mogu se pronaći u [članku ESET-ove baze znanja](#).

Ransomware

Ransomware (poznat i pod nazivom filecoder) je vrsta zlonamjernog programa koja zaključava vaš uređaj ili šifrira sadržaj na njemu te iznuđuje novac od vas da biste ponovno dobili pristup sadržaju. Ova vrsta zlonamjernog programa također može imati ugrađeni brojač vremena s unaprijed programiranim rokom za plaćanje. Ako se uplata ne izvrši do zadanog roka, cijena se povećava ili se uređaju u konačnici više ne može pristupiti.

Kada se zarazi uređaj, filecoder može pokušati šifrirati dijeljene pogone na uređaju. Zbog tog procesa može se činiti da se zlonamjerni program širi preko mreže, ali to nije slučaj. To se događa kada je dijeljeni pogon na datotečnom serveru šifriran, ali sam server nije zaražen zlonamjernim programom (osim ako je riječ o terminalskom serveru).

Autori ransomwarea izrađuju par ključeva, javni i privatni, i umeću javni ključ u zlonamjerni program. Sam ransomware može biti dio trojanca ili se činiti kao datoteka ili slika koju možete primiti u poruci e-pošte, na društvenim mrežama ili u programima za razmjenu instant-poruka. Nakon što se infiltrira u vaše računalo,

zlonamjerni program izradit će nasumičan simetrični ključ i šifrirati podatke na uređaju. Za šifriranje simetričnog ključa upotrebljava javni ključ u zlonamjernom programu. Zatim ransomware traži uplatu da bi se podaci dešifrirali. Poruka kojom se traži uplata i koja se prikazuje na uređaju može biti lažno upozorenje da je vaš sustav upotrijebljen za nezakonite aktivnosti ili da se na njemu nalazi nezakonit sadržaj. Od žrtve napada ransomwareom traži se da plati otkupninu putem različitih načina plaćanja. Ti su načini obično oni koji se teško mogu pratiti, primjerice digitalne (kripto)valute, SMS poruke s posebnom tarifom ili vaučeri s unaprijed uplaćenim sredstvima. Po primitku uplate autor ransomwarea trebao bi otključati uređaj ili svojim privatnim ključem dešifrirati simetrični ključ i podatke osobe čiji je uređaj zaražen, no to nije zajamčeno.

Više informacija o zaštiti od ransomwarea

 ESET-ovi programi imaju više slojeva tehnologije koji štite uređaje od ransomwarea. Najbolje prakse za zaštitu vašeg sustava od ransomwarea potražite u našem članku [ESET-ove baze znanja](#).

Rootkit

Rootkiti su zlonamjerni programi koji napadačima s interneta omogućuju neograničeni pristup nekom sustavu uz prikrivanje njihove prisutnosti. Nakon pristupanja nekom sustavu rootkiti (obično zahvaljujući nekoj slaboj točki sustava) koriste funkcije operacijskog sustava da ih antivirusni softver ne bi otkrio: prikrivaju procese, datoteke i podatke o registru sustava Windows. Iz tog ih je razloga gotovo nemoguće otkriti uobičajenim tehnikama testiranja.

Postoje dvije razine otkrivanja kako bi se spriječili rootkiti:

1. Kada pokušaju pristupiti sustavu: Još nisu prisutni i stoga nisu aktivni. Većina antivirusnih sustava uspijeva eliminirati rootkite na toj razini (uz pretpostavku da i inače prepoznaju takve datoteke kao zaražene).
2. Kad su skriveni od uobičajenog testiranja: korisnici programa ESET imaju prednost Anti-Stealth tehnologije koja može otkriti i ukloniti aktivne rootkite.

Programiranje usmjereni na povratak

Programiranje usmjereni na povratak (ROP) je tipičan napad ponovne upotrebe koda, gdje napadač usmjerava kontrolni tijek pomoću postojećeg koda sa zlonamjernim rezultatom. ROP napad predstavlja naprednu verziju napada uništavanja stoga (engl. stack smashing). Do preljeva međuspremnika stoga (engl. stack buffer overflow) dolazi kada program zapisuje na memorijsku adresu na stog poziva programa izvan predviđene strukture podataka, obično s međuspremnikom fiksne duljine.

ROP je tehnika zloupotrebe koja omogućuje izvođenje koda na ciljnem sustavu. Dobivanjem kontrole nad stogom poziva napadač kontrolira tijek postojećeg pouzdanog softvera koji je pokrenut na računalu i manipulira njime kako bi izvršio zadatok koji nije bio namijenjen za izvršenje.

Spyware

Kategorija obuhvaća sve aplikacije koje šalju privatne podatke bez pristanka ili znanja korisnika. Spyware koristi funkcije praćenja za slanje raznih statističkih podataka kao što su popis posjećenih web stranica, adrese e-pošte s popisa korisnikovih kontakata ili popis pritisnutih tipki.

Autori spywarea tvrde da tim tehnikama žele saznati više o potrebama i interesima korisnika te postići bolje ciljano oglašavanje. Problem je u tome što ne postoji jasna granica između korisnih i zlonamjernih aplikacija te

nitko ne može sa sigurnošću tvrditi da se prikupljeni podaci neće zloupotrijebiti. Podaci koje prikupljaju spyware aplikacije mogu obuhvaćati sigurnosne kodove, PIN-ove, brojeve bankovnih računa itd. Neki autori besplatnih programa svoje proizvode često isporučuju u paketu sa spyware programima radi ostvarenja prihoda ili ponude poticaja za kupnju softvera. Korisnike se često obavješćuje o prisutnosti spyware programa tijekom instalacije neke aplikacije da bi ih se potaknulo na kupnju verzije bez tog dodatka.

Dobro poznati primjeri besplatnih proizvoda koji se isporučuju u paketu sa spyware programima su klijentske aplikacije koje koriste P2P (peer-to-peer) mrežu računala. Spyfalcon i Spy Sheriff (i još mnogi drugi) pripadaju posebnoj potkategoriji spywarea – predstavljaju se kao programi za zaštitu od spywarea, ali su zapravo i sami spyware.

Ako je na računalu otkriven spyware, preporučuje se da ga izbrišete jer postoji velika vjerojatnost da sadrži zlonamjerni kôd.

Kao potkategorija spywarea, keyloggeri se mogu temeljiti na hardveru ili softveru. Keyloggeri koji se temelje na softveru mogu prikupljati samo podatke upisane na jednu web stranicu ili u jednu aplikaciju. Napredniji keyloggeri mogu zabilježiti sve što utipkate, uključujući podatke koje kopirate/zalijepite. Neki keyloggeri kojima su meta mobilni uređaji mogu snimati pozive, bilježiti informacije iz aplikacija za slanje poruka, lokacije ili čak snimke mikrofona i kamere.

Trojan

Nekad se trojanski softver (trojanski softver) opisivao kao klasa prijetnji koja se pokušava prikazati kao koristan program da bi korisnik dopustio njegovo pokretanje.

Trojanski softver je vrlo opsežna kategorija pa je dijelimo na nekoliko potkategorija:

- Downloader – zlonamjerni programi koji imaju mogućnost preuzimanja drugih prijetnji s interneta.
- Dropper – zlonamjerni programi koji imaju mogućnost uvođenja drugih vrsti zlonamjernih programa na zaraženo računalo.
- Backdoor – zlonamjerni programi koji komuniciraju s udaljenim napadačima, omogućujući im pristup računalu i preuzimanje kontrole nad njime.
- Keylogger – (keystroke logger) – program koji zapisuje svaki korisnikov pritisak tipke i šalje te podatke udaljenim napadačima.
- Dialer – zlonamjerni programi namijenjeni pozivanju brojeva s posebnom tarifom umjesto onog korisnikova pružatelja internetskih usluga. Korisnik gotovo i ne može primijetiti da je stvorena nova veza. Ovi programi mogu našteti samo korisnicima s dial-up vezom, koja se sve rjeđe koristi.

Ako se na računalu otkrije datoteka koja pripada trojanskom softveru, preporučuje se da je izbrišete jer najvjerojatnije sadrži zlonamjerni kôd.

Virus

Računalni virus primjerak je zlonamjernog koda koji se dodaje ispred ili uz postojeće datoteke na računalu. Virusi su dobili naziv prema biološkim virusima jer koriste slične tehnike za širenje s jednog mjesta na drugo. Pojam „virus“ često se neispravno koristi kao naziv za bilo koju vrstu prijetnje. Takva se praksa postepeno napušta i sve se više koristi novi, precizniji pojam „zlonamjerni program“.

Računalni virusi napadaju uglavnom izvršne datoteke i dokumente. Funkcioniranje virusa može se ukratko opisati ovako: nakon izvršenja zaražene datoteke poziva se zlonamjerni kôd i izvršava se prije izvršenja izvorne aplikacije. Virus može zaraziti bilo koju datoteku za koju trenutni korisnik ima ovlasti za pisanje.

Računalni se virusi razlikuju prema svrsi i težini. Neki su krajnje opasni jer namjerno brišu datoteke s tvrdog diska. Drugi pak ne uzrokuju nikakvu ozbiljnu štetu – jedini im je zadatak da zasmetaju korisniku u radu i prikažu tehničku vještinu svojih autora.

Ako je vaše računalo zaraženo virusom i čišćenje nije moguće, pošaljite ga na analizu u Laboratorij za istraživanje tvrtke ESET. U određenim slučajevima zaražene datoteke toliko su izmijenjene da čišćenje nije moguće i datoteke je potrebno zamjeniti čistom kopijom.

Crv

Računalni je crv program sa zlonamjernim kodom koji napada računala i širi se putem mreže. Osnovna je razlika između virusa i crva to što crvi imaju mogućnost samostalnog razmnožavanja – oni ne ovise o datotekama glavnog računala (ni boot sektorima). Crvi se šire na adrese e-pošte s popisa kontakata ili koriste sigurnosne slabosti u mrežnim aplikacijama.

Crvi su zbog svega toga daleko otporniji od virusa. Zbog dostupnosti interneta mogu se proširiti cijelom svijetom za samo nekoliko sati ili minuta od nastanka. To obilježje samostalnog i brzog razmnožavanja čini ih opasnijim od ostalih vrsta zlonamjernog softvera.

Crv aktiviran u sustavu može izazvati brojne neugodnosti: izbrisati datoteke, smanjiti performanse sustava ili čak deaktivirati programe. Svojstva računalnog crva čine ga prikladnim „prijevoznim sredstvom“ za druge vrste infiltracija.

Ako je vaše računalo zaraženo računalnim crvom, preporučuje se da izbrišete zaražene datoteke jer vjerojatno sadrže zlonamjerni kôd.

Krađa korisničkih podataka

Krađa korisničkih podataka je mrežni napad pri kojem se upotrebljavaju podaci iz razotkrivenih baza podataka s korisničkim podacima. Napadači upotrebljavaju botove i druge metode automatizacije da bi se prijavili u račune na brojnim web stranicama s pomoću razotkrivenih podataka. Napadačima su meta korisnici koji upotrebljavaju iste korisničke podatke za prijavu na više web stranica i servisa. Kada je napad uspješan, napadači mogu ostvariti potpuni pristup podacima o računu i korisniku koji su pohranjeni na ovom računu. Napadači mogu iskoristiti ovaj pristup da bi krali osobne podatke u svrhu krađe identiteta, lažnih transakcija, slanja spam sadržaja ili u svrhu drugih zlonamjernih radnji.

Onečišćenje DNS-a

Pomoću onečišćenja DNS-a (Domain Name Server, server naziva domene) hakeri mogu zavarati DNS server bilo kojeg računala da su poslani lažni podaci legitimni i autentični. Ti se lažni podaci zatim na neko vrijeme stavljuju u predmemoriju, što napadačima omogućuje prepisivanje DNS odgovora IP adresa. Time se postiže da korisnici koji pokušaju pristupiti web stranicama na internetu preuzimaju računalne viruse ili crve umjesto izvornog sadržaja.

DoS napad

DoS, odnosno denial of service (uskraćivanje usluga) vrsta je napada zbog kojih računalni resursi postaju nedostupni korisnicima. Komunikacija između korisnika pogođenih napadom zapriječena je i ne može se normalno nastaviti. Računala izložena DoS napadima obično treba ponovno pokrenuti da bi radila ispravno.

U većini su slučajeva mete web serveri, a cilj je napada učiniti ih nedostupnima korisnicima tijekom određenog razdoblja.

Napad kroz ICMP

ICMP (Internet Control Message Protocol) popularan je internetski protokol u širokoj upotrebi. Prvenstveno ga koriste umrežena računala za slanje različitih poruka o pogreškama.

Udaljeni napadači pokušavaju iskoristiti slabosti protokola ICMP. ICMP protokol osmišljen je za jednosmjernu komunikaciju za koju nije potrebna autorizacija. To udaljenim napadačima omogućuje takozvane DoS (eng. denial of service – uskraćivanje usluge) napade ili napade kojima se neautoriziranim pojedincima daje pristup dolaznim i odlaznim paketima.

Tipični su primjeri napada kroz ICMP različiti napadi slanjem brojnih zahtjeva za pingom, brojnih ICMP_ECHO zahtjeva i smurf napadi. Računala izložena napadu kroz ICMP znatno su sporija (to se odnosi na sve aplikacije koje koriste Internet) i imaju problema s povezivanjem s internetom.

Skeniranje portova

Skeniranje portova koristi se za određivanje koji su računalni portovi otvoreni na računalu. Skener portova softver je namijenjen pronalaženju takvih portova.

Računalni port virtualna je točka koja upravlja dolaznim i odlaznim podacima – to je ključno sa sigurnosne točke gledišta. U velikim mrežama informacije koje prikupe skeneri portova mogu pridonijeti prepoznavanju potencijalnih slabih točaka. Takva je upotreba legitimna.

No skeniranje portova često koriste hakeri u pokušajima narušavanja sigurnosti. Njihov je prvi korak slanje paketa na svaki port. Ovisno o vrsti odgovora može se odrediti koji se portovi koriste. Samo skeniranje ne uzrokuje štetu, ali uzmite u obzir da ta aktivnost može otkriti potencijalne slabe točke i napadačima omogućiti preuzimanje kontrole nad udaljenim računalima.

Administratorima mreže savjetuje se da sve nekorištene portove blokiraju, a korištene zaštite od neovlaštenog pristupa.

SMB Relay

SMB Relay i SMB Relay2 posebni su programi koji mogu napadati udaljena računala. Ti programi koriste protokol za zajedničko korištenje datoteka Server Message Block (serverski blok poruka), koji se u slojevima polaze na NetBIOS. Korisnik koji zajednički koristi neku mapu ili direktorij unutar LAN-a najvjerojatnije koristi taj protokol za zajedničko korištenje datoteka.

Unutar komunikacije lokalnom mrežom izmjenjuju se šifre lozinki.

SMB Relay prima vezu na UDP portovima 139 i 445, prenosi pakete koje izmjenjuju klijent i server te ih mijenja. Nakon povezivanja i autorizacije veza s klijentom se prekida. SMB Relay stvara novu virtualnu IP adresu. Novoj adresi može se pristupiti naredbom „net use \\192.168.1.1“. Adresu potom može koristiti svaka mrežna funkcija sustava Windows. SMB Relay prenosi komunikaciju SMB protokolom, izuzev pregovora i autorizacije. Udaljeni napadači mogu koristiti IP adresu sve dok je klijentsko računalo povezano.

SMB Relay2 funkcioniра на истом principu као SMB Relay, осим што umjesto IP adresa koristi NetBIOS nazine. Oba programa mogu provoditi napade vrste „man-in-the-middle“ (posrednik). Ti napadi omogućuju udaljenim napadačima da neprimiječeni čitaju, umeću i mijenjaju poruke koje razmjenjuju dvije krajnje točke u komunikaciji. Računala izložena takvim napadima često prestaju reagirati ili se neočekivano restartaju.

Da biste izbjegli napade, preporučujemo da koristite lozinke ili ključeve za autorizaciju.

Desinkronizacija TCP-a

Desinkronizacija TCP-a tehnika je koja se koristi u napadima otimanja TCP-a (TCP Hijacking attacks). Pokreće se procesom u kojem se redni broj dolaznih paketa razlikuje od očekivanog rednog broja. Paketi s neočekivanim rednim brojem odbacuju se (ili spremaju u pohranu međuspremnika ako su prisutni u aktualnom komunikacijskom prozoru).

Kod desinkronizacije obje komunikacijske krajnje točke odbacuju primljene pakete i u tom se trenutku udaljeni napadači mogu uvući u pakete i dodijeliti im ispravan serijski broj. Napadači mogu čak i manipulirati komunikacijom ili je izmijeniti.

Napadi otimanjem TCP-a nastoje prekinuti komunikaciju između servera i klijenta, odnosno između ravnopravnih računala. Mnogi se napadi mogu izbjegići autorizacijom svakog TCP segmenta. Preporučuje se i korištenje preporučenih konfiguracija za vaše mrežne uređaje.

Napad crva

Računalni je crv program sa zlonamjernim kodom koji napada računala i širi se putem mreže. Mrežni crvi koriste sigurnosne slabosti u raznim aplikacijama. Zbog dostupnosti interneta mogu se proširiti cijelim svijetom za samo nekoliko sati od nastanka.

Većina napada crva (npr. Sasser ili SqlSlammer) može se izbjegići korištenjem standardnih sigurnosnih postavki u firewallu, odnosno blokiranjem nezaštićenih i nekorištenih portova. Izuzetno je važno da i sustav nadograđujete najnovijim sigurnosnim zakrpama.

Onečišćenje ARP predmemorije

Protokol za razrješavanje adrese (ARP) prevodi adrese između sloja podatkovne veze (MAC adrese) i mrežnog sloja (IP adrese). Napad onečišćenjem ARP predmemorije omogućuje napadačima da presretnu komunikaciju između mrežnih uređaja tako da oštete ARP tablice mreže (mapiranja MAC-a s IP-jem uređaja).

Napadač šalje lažnu poruku odgovora ARP-a standardnom mrežnom pristupniku uz obavijest da je MAC adresa povezana s IP adresom drugog cilja. Kad standardni pristupnik primi ovu poruku i proslijeđuje promjene svim drugim uređajima na mreži, sav promet cilja prema bilo kojem drugom mrežnom uređaju prolazi kroz napadačevo računalo. To omogućuje napadaču da pregledava ili mijenja promet prije nego što ga proslijedi na predviđeno odredište.

Prijetnje putem e-pošte

E-pošta je oblik komunikacije koji ima mnogo prednosti.

No, zbog visoke razine anonimnosti e-pošta i internet, nažalost, ostavljaju prostora za ilegalne aktivnosti kao što je slanje spam poruka. Spam obuhvaća nepoželjne oglase, lažne obavijesti (hoax) i širenje [zlonamjernih programa](#). Neugodnosti i opasnosti za korisnika povećavaju se zbog činjenice da su troškovi slanja minimalni, a autorima spam poruka na raspolaganju je mnogo alata za nabavljanje novih adresa e-pošte. Spam poruke, k tome, zbog njihove količine i raznolikosti vrlo je teško regulirati. Što se dulje koristite nekom adresom e-pošte, postoje veći izgledi da će završiti u bazi podataka nekog sustava za slanje spam poruka.

Evo nekih savjeta za prevenciju:

- Ako je moguće, ne objavljujte svoju adresu e-pošte na internetu
- Svoju adresu e-pošte dajte samo pouzdanim pojedincima.
- Ako je moguće, nemojte se služiti uobičajenim zamjenskim imenima jer su izgledi da vam netko uđe u trag manji ako imate složenije zamjensko ime
- Ne odgovarajte na spam poruku koja vam je stigla u ulaznu poštu.
- Budite oprezni pri ispunjavanju obrazaca na internetu, a osobito kod potvrđnih okvira uz koje стоји „Da, želim primati informacije“.
- Koristite „specijalizirane“ adrese e-pošte – npr. jednu za posao, jednu za komunikaciju s prijateljima itd.
- Povremeno mijenjajte svoju adresu e-pošte
- Koristite neko rješenje za antispam zaštitu.

Oglasni

Oглаšavanje na internetu jedan je od oblika oglašavanja s najbržim rastom. Najvažnije su marketinške prednosti takvog oglašavanja niski troškovi i visoka razina izravnosti i učinkovitosti, a poruke se isporučuju gotovo istog trenutka. Mnoge tvrtke koriste alate za oglašavanje e-poštom kako bi učinkovito komunicirale s postojećim i potencijalnim kupcima.

Taj je način oglašavanja legitiman jer je korisnik često zainteresiran za primanje komercijalnih informacija o nekim proizvodima. No istina je da tvrtke često šalju neželjene masovne poruke s oglasima. U tim slučajevima oglašavanje e-poštom prelazi granicu dopuštenog i postaje spam.

Količina neželjene pošte postala je stvaran problem jer ne pokazuje nikakve znakove jenjavanja. Autori neželjene pošte, naravno, pokušavaju spam poruke prikazati kao legitimnu poštu.

Lažne obavijesti (Hoax)

Lažna obavijest (hoax) poruka je koja internetom širi lažne informacije. Najčešće se šalje e-poštom, a katkada i putem komunikacijskih alata kao što su ICQ i Skype. Sama je poruka često šala ili urbana legenda.

Lažne obavijesti (hoax) o računalnim virusima pokušavaju u primatelja izazvati strah, nesigurnost ili sumnju navodeći ih da vjeruju da neki „virus koji nije moguće otkriti“ briše datoteke, dohvaća lozinke ili izvršava neke druge štetne aktivnosti u njihovu sustavu.

Neke lažne obavijesti (hoax) od primatelja traže da poruku proslijede svojim kontaktima, čime se lažna obavijest (hoax) dalje širi. Postoje i lažne obavijesti (hoax) za mobilne telefone, zamolbe za pomoć, ponude za slanje novca iz inozemstva itd. U većini je slučajeva nemoguće spoznati namjere njihovih autora.

Ako dobijete poruku u kojoj se od vas traži da je proslijedite svima koje znate, vrlo lako bi se moglo raditi o lažnoj obavijesti. Na internetu postoji mnogo specijaliziranih web stranica na kojima se može provjeriti je li neka poruka e-pošte legitimna. Ako sumnjate da je neka poruka lažna obavijest (hoax), prije nego što je proslijedite, potražite informacije o njoj na internetu.

Phishing

Pojam phishing odnosi se na protuzakonitu aktivnost koja koristi tehnike društvenog inženjeringu (manipuliranje korisnicima radi stjecanja povjerljivih informacija). Njen je cilj pristupanje tajnim podacima kao što su brojevi bankovnih računa, PIN kodovi itd.

Pristup se obično postiže slanjem e-pošte čiji se autor lažno prikazuje kao pouzdana osoba ili tvrtka (primjerice finansijska ustanova ili osiguravajuće društvo). Takva e-pošta može izgledati vrlo autentično te sadržavati slike i sadržaj koji možda potječe s izvora čijim se identitetom pošiljatelj koristi. Od vas se pod različitim izlikama (provjera podataka, finansijske operacije) traži da unesete neke osobne podatke – bankovne račune, korisnička imena i lozinke. Svi ti podaci, ako ih pošaljete, lako mogu biti ukradeni ili zloupotrijebljeni.

Uzmite u obzir da banke, osiguravajuća društva i ostale legitimne tvrtke nikad neće zahtijevati korisnička imena ni lozinke u neželjenoj pošti.

Prepoznavanje spam prijevara

Općenito uvezši, postoji nekoliko pokazatelja koji pridonose prepoznavanju spam poruka (nepoželjnih poruka e-pošte) u poštanskom sandučiću. Ako neka poruka ispunjava barem neke od sljedećih kriterija, vjerojatno je riječ o spam poruci.

- Adresa pošiljatelja ne pripada nikome s vašeg popisa kontakata.
- Nudi vam se velik novac, ali vi prvo morate uplatiti neki manji iznos.
- Od vas se pod različitim izlikama (provjera podataka, finansijske operacije) traži da unesete neke osobne podatke: bankovne račune, korisnička imena, lozinke itd.
- Poruka je pisana na stranom jeziku.
- Od vas se traži da kupite proizvod koji vas ne zanima. Ako ga ipak odlučite kupiti, provjerite je li pošiljatelj poruke pouzdan dobavljač (obratite se izvornom proizvođaču).
- Neke su riječi pogrešno napisane u pokušaju zavaravanja filtra spam poruka. Na primjer, „vaigra“ umjesto „viagra“.

Pravila

U kontekstu antispam rješenja i klijenata e-pošte pravila pomažu u manipuliranju funkcijama e-pošte. Sastoje se od dviju logičkih cjelina:

1.Uvjeta (primjerice, poruka koja dolazi s određene adrese ili ima određeni naslov)

2.Radnje (primjerice, uklanjanje poruke ili njezin prijenos u određenu mapu)

Broj i kombinacija pravila ovisi o antispam rješenju. Ta pravila služe kao mjere protiv spam poruka (neželjene e-pošte). Tipični primjeri:

1. uvjet: dolazna e-pošta sadrži neke riječi koje se obično pojavljuju u spam poruci

2. akcija: brisanje poruke

1. uvjet: dolazna e-pošta sadrži privitak s ekstenzijom .exe

2. akcija: brisanje privitka i isporučivanje poruke u poštanski sandučić

1. uvjet: dolaznu poruku šalje vaš poslodavac

2. akcija: Premjestite poruku u mapu „Posao”

Za pojednostavljenje administracije i učinkovitije filtriranje spam poruka preporučujemo korištenje kombinacije pravila u antispam programima.

Popis pouzdanih adresa

Općenito popis pouzdanih adresa označava popis prihvaćenih, odnosno poželjnih stavki ili osoba. Pojam "popis pouzdanih adresa e-pošte" (dopuštene adrese), odnosno popis pouzdanih stavki u kontekstu e-pošte označava popis kontakata od kojih korisnik želi primati poruke. Takvi se popisi pouzdanih adresa temelje na ključnim riječima prema kojima se pretražuju adrese e-pošte, nazivi domena i IP adrese.

Ako popis pouzdanih stavki funkcioniра u „isključivom načinu rada”, poruke s bilo koje druge adrese, domene ni IP adrese neće biti primljene. Ako pak popis pouzdanih adresa nije isključiv, takve poruke neće se izbrisati već filtrirati na neki drugi način.

Popis pouzdanih adresa temelji se na načelu suprotnom od [popisa spam adresa](#). Popisi pouzdanih adresa u usporedbi s popisima spam adresa održavaju se relativno jednostavno. Preporučujemo da radi učinkovitijeg filtriranja spam poruka koristite i popis spam adresa i popis pouzdanih adresa.

Popis spam adresa

Općenito uzevši, engleski izraz "blacklist" (crni popis) označava popis nepoželjnih ili odbijenih stavki ili osoba. U virtualnom svijetu to je naziv tehnike koja omogućuje prihvatanje poruka od svih korisnika koji se ne nalaze na takvom popisu.

Postoje dvije vrste popisa spam adresa: One koje korisnici naprave u svojoj aplikaciji za zaštitu od neželjene pošte i profesionalni, redovito aktualizirani popisi spam adresa koje stvaraju specijalizirane ustanove, a koji se mogu pronaći na internetu.

Korištenje popisa spam adresa ključan je element uspješnog blokiranja spama, ali njihovo je održavanje vrlo teško jer se nove stavke koje treba blokirati pojavljuju svaki dan. Preporučujemo da radi učinkovitijeg filtriranja spam poruka koristite i popis spam adresa i popis pouzdanih adresa.

Iznimka

Popis iznimki obično sadržava adrese e-pošte koje se mogu lažirati i upotrebljavati za slanje spam poruka. Poruke e-pošte primljene s adrese navedene na popisu iznimki uvek će se skenirati da bi se utvrdilo jesu li spam poruke. Popis iznimki standardno sadržava sve adrese e-pošte iz postojećih računa klijenta e-pošte.

Provjera sa serverske strane

Provjera sa serverske strane tehnika je za identifikaciju masovne količine spam poruka na temelju broja primljenih poruka i reakcija korisnika. Svaka poruka na temelju svojeg sadržaja ostavlja jedinstven digitalni „otisak“. Jedinstveni ID broj ne otkriva ništa o sadržaju e-pošte. Dvije će identične poruke imati identične otiske, a različite će poruke imati različite otiske.

Ako je neka poruka označena kao spam, njezin se otisak šalje na server. Ako server primi više identičnih otisaka (koji odgovaraju određenoj spam poruci), otisak se pohranjuje u bazu podataka s otiscima spam poruka. Prilikom skeniranja dolaznih poruka program serveru šalje otiske poruka. Server uzvraća informacijama o tome koji otisci odgovaraju porukama koje su korisnici već označili kao spam poruke.

Napredni skener memorije

Napredni skener memorije radi zajedno sa zaštitom od zloupotrebe na ojačavanju zaštite od zlonamjernog softvera koji je osmišljen tako da skrivanjem i/ili šifriranjem izbjegava da ga otkriju programi za zaštitu od zlonamjernog softvera. U slučajevima kada obična emulacija ili heuristika ne mogu otkriti prijetnje, napredni skener memorije može identificirati sumnjivo ponašanje i skenirati prijetnje kada se otkriju u sistemskoj memoriji. Ovo rješenje učinkovito je u zaštiti od iznimno skrivenog zlonamjernog softvera.

Za razliku od zaštite od zloupotrebe, napredni skener memorije metoda je koja slijedi nakon izvršavanja, što znači da postoji opasnost da je neka zlonamjerna aktivnost izvršena prije nego što je on otkrio prijetnju, no u slučaju da su druge tehnike otkrivanja bile neuspješne, on nudi dodatni sloj sigurnosti.

Zaštita bankarstva i plaćanja

Zaštita bankarstva i plaćanja dodatni je sloj zaštite osmišljen za zaštitu financijskih podataka tijekom mrežnih transakcija.

ESET Smart Security Premium i ESET Internet Security sadrže ugrađeni popis web stranica koje će pokrenuti otvaranje zaštićenog preglednika. U konfiguraciji programa možete dodati web stranicu ili uređiti popis web stranica.

Uključite opciju zaštite svih preglednika za pokretanje svih podržanih web preglednika u sigurnom načinu rada.

Više informacija o toj značajci pročitajte u sljedećim člancima ESET-ove baze znanja:

- [Kako koristiti ESET-ovu zaštitu bankovnih plaćanja?](#)
- [Pauziranje ili deaktivacija Zaštite bankarstva i plaćanja u ESET-ovim Windows programima za kućne korisnike](#)
- [ESET-ova Zaštita bankarstva i plaćanja – uobičajene pogreške](#)

Za zaštićeno pregledavanje weba nužna je upotreba šifrirane HTTPS komunikacije. Zaštitu bankarstva i plaćanja podržavaju sljedeći preglednici:

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

Otvorite zaštitu bankarstva i plaćanja u željenom web pregledniku

Kada otvorite zaštitu bankarstva i plaćanja izravno s kartice **Alati** u izborniku programa, otvara se u web pregledniku koji ste postavili kao standardni za Windows. U suprotnom, kada otvorite željeni web preglednik (ne iz izbornika programa), web stranice s popisa zaštićenih web stranica će se preusmjeriti na istu vrstu web preglednika koju štiti ESET.

Zaštita od botneta

Zaštita od botneta otkriva zlonamjerni program analizirajući njegove protokole mrežne komunikacije. Botnet se često mijenja, dok se mrežni protokoli nisu promijenili proteklih nekoliko godina. Ova nova tehnologija pomaže tvrtki ESET u borbi protiv zlonamjernih programa koji pokušavaju izbjegći otkrivanje i povezati vaše računalo s botnet mrežom.

Otkrivanja DNA

Vrste otkrivanja u rasponu su od vrlo specifičnih ključeva do ESET-ova otkrivanja DNA, što su kompleksne definicije zlonamjernog ponašanja i karakteristika zlonamjernog softvera. Dok napadači mogu jednostavno promijeniti ili prikriti zlonamjerni kod, ponašanje objekata nije moguće tako lako promijeniti i ESET-ova otkrivanja DNA izrađena su tako da rabe taj princip.

Provodimo dubinske analize koda i izdvajamo „gene“ koji su odgovorni za njegovo ponašanje te gradimo ESET-ova otkrivanja DNA koja se upotrebljavaju za procjenu potencijalno sumnjivih kodova koji su pronađeni na disku ili u memoriji procesa koji se izvršava. Otkrivanja DNA mogu identificirati uzorce specifičnih poznatih zlonamjernih softvera, nove varijante poznate obitelji zlonamjernog softvera ili čak prethodno neviđeni ili nepoznati zlonamjerni softver koji sadrži gene koji upućuju na zlonamjerno ponašanje.

ESET LiveGrid®

ESET LiveGrid® (konstruiran na temelju naprednog sustava ranog upozorenja ESET ThreatSense.Net) prikuplja podatke koje šalju korisnici ESET-ovih programa diljem svijeta i prosljeđuje ih u Laboratorij za istraživanje tvrtke ESET. Pružanjem sumnjivih uzoraka i metapodataka "from the wild" (iz opće upotrebe) ESET LiveGrid® omogućuje nam da brzo reagiramo na potrebe svojih korisnika i da održimo ESET-ovu sposobnost reagiranja na najnovije prijetnje.

ESET-ovi istraživači zlonamjernih programa upotrebljavaju te informacije za stvaranje točne snimke stanja i opsega globalnih prijetnji, koja nam pomaže da se usmjerimo na prave ciljeve. Podaci sustava ESET LiveGrid® imaju važnu ulogu u postavljanju prioriteta u našoj automatiziranoj obradi.

Osim toga, implementira se i sustav reputacije koji doprinosi poboljšanju ukupne učinkovitosti naših rješenja za zaštitu od zlonamjernih programa. Korisnik može provjeriti reputaciju [pokrenutih procesa](#) i datoteka izravno iz sučelja programa ili kontekstnog izbornika s pomoću dodatnih informacija koje su dostupne u sustavu ESET LiveGrid®. Kada se u korisnikovom sustavu pregledava izvršna datoteka ili arhiv, njegova se oznaka najprije uspoređuje s bazom podataka pouzdanih i nepoželjnih stavki. Ako se nalazi na popisu pouzdanih stavki, pregledana datoteka smatra se čistom i označava se da bi se izuzela iz budućih skeniranja. Ako se nalazi na popisu nepoželjnih stavki, poduzimaju se odgovarajuće radnje na temelju svojstava prijetnje. Ako nema podudaranja, datoteka se temeljito skenira. Ovisno o rezultatima ovog skeniranja, datoteke se kategoriziraju kao prijeteće ili neprijeteće. Ovaj pristup ima značajan pozitivan utjecaj na performanse skeniranja. Ovaj sustav reputacije omogućuje učinkovito otkrivanje uzoraka zlonamjernih programa čak i prije nego što se njihovi potpisi isporuče na korisnikovo računalo putem nadograđene baze podataka virusa (što se događa nekoliko puta dnevno).

Uz sustav reputacije ESET LiveGrid®, sustav za povratne informacije ESET LiveGrid® prikupljaće informacije o vašem računalu koje se odnose na nove pronađene prijetnje. Te informacije mogu obuhvaćati uzorak ili kopiju datoteke u kojoj se pojavila prijetnja, put do te datoteke, naziv datoteke, datum i vrijeme, proces u kojem se prijetnja pojavila na računalu i informacije o operacijskom sustavu računala.

ESET LiveGrid® serveri

 Naši ESET LiveGrid® serveri se nalaze u Bratislavi, Beču i San Diegu, no to su samo serveri koji odgovaraju na zahtjeve klijentata. Poslani uzorci se obrađuju u Bratislavi u Slovačkoj.

Aktivacija ili deaktivacija sustava ESET LiveGrid® u ESET-ovim programima

 Detaljnije i ilustrirane upute o tome kako aktivirati ili deaktivirati sustav ESET LiveGrid® u ESET-ovim programima potražite u [članku ESET-ove baze znanja](#).

Sprječavanje ranjivosti

Sprječavanje ranjivosti osmišljeno je za ojačavanje zaštite često zloupotrebljavnih vrsta aplikacija kao što su web preglednici, PDF čitači, klijenti e-pošte i komponente sustava Microsoft Office i zaštitu od [ROP napada](#).

Sprječavanje ranjivosti dostupno je i aktivirano kao standardna postavka u svim ESET-ovim Windows programima za kućnu upotrebu, ESET-ovim programima za Windows Server i ESET-ovim sigurnosnim programima za Windows.

Funkcionira tako da nadzire procese s ciljem pronalaženja sumnjive aktivnosti koja bi mogla ukazivati na program koji iskorištava slabe točke sustava.

Kada zaštita od zloupotrebe prepozna sumnjivi proces, odmah zaustavlja proces te bilježi i šalje podatke o prijetnji ESET LiveGrid® cloud sustavu. Ove podatke obrađuje Laboratorij za istraživanje tvrtke ESET te se podaci upotrebljavaju da bi se svi korisnici bolje zaštitili od nepoznatih prijetnji i napada uslijed dosad nepoznate

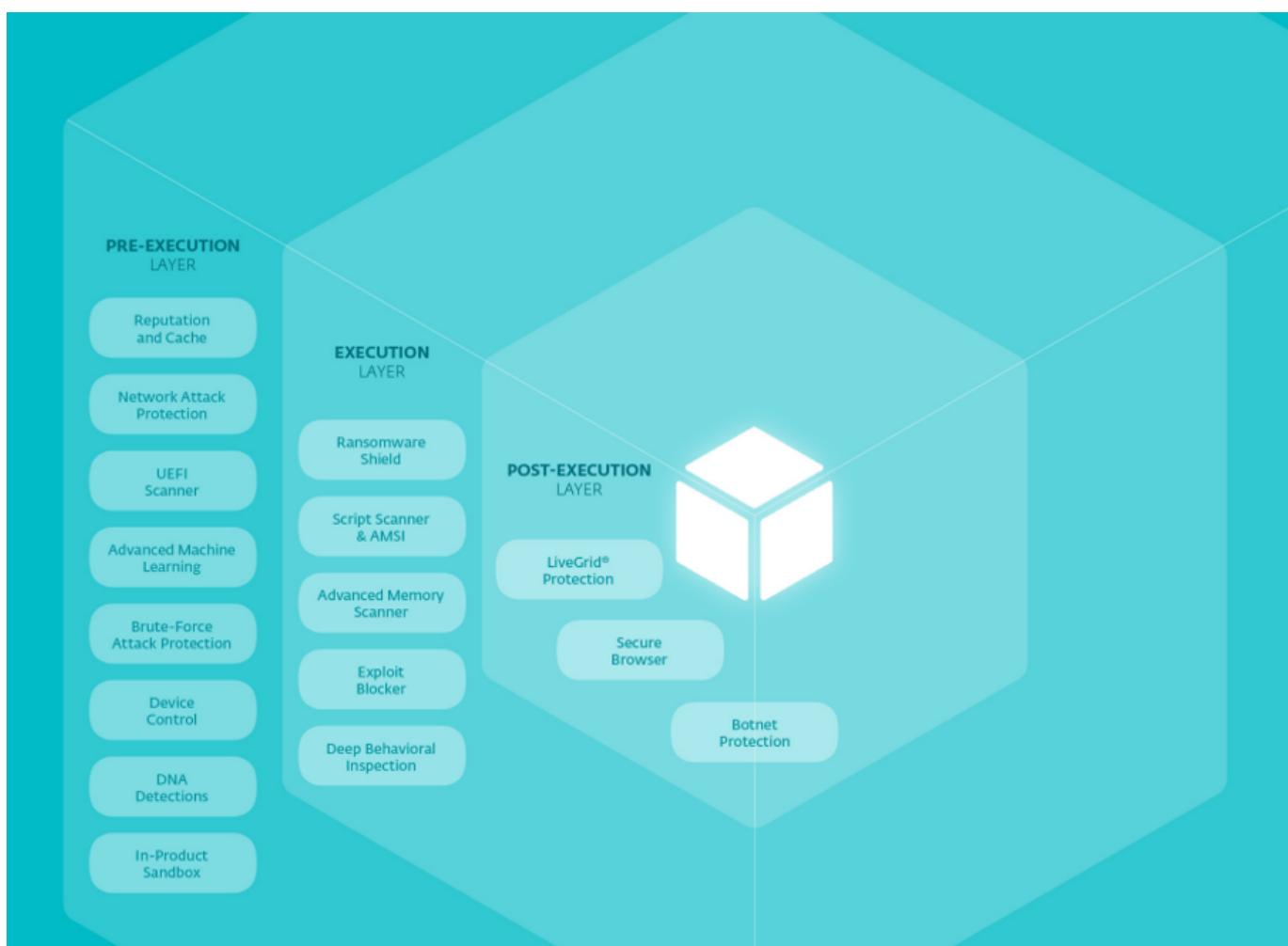
ranjivosti (tek izdani zlonamjerni programi za koje ne postoji konfiguirano rješenje).

Zaštita od zloupotrebe Java

Zaštita od zloupotrebe Java je proširenje postojeće [tehnologije zaštite od zloupotrebe](#). Ova tehnologija nadzire Javu i traži ponašanje koje je nalik zloupotrebi. Blokirani uzorci se mogu prijaviti analitičarima zlonamjernih programa tako da oni mogu stvoriti potpise da bi se uzorci blokirali na različitim slojevima (blokiranje URL-a, preuzimanje datoteka itd.).

ESET LiveSense

ESET koristi razne jedinstvene, vlasničke tehnologije slojevite zaštite koje zajednički funkcioniraju kao ESET LiveSense. Slika u nastavku prikazuje neke od ESET-ovih osnovnih tehnologija te pokazuje otprilike kada i gdje mogu otkriti i naposljetku blokirati prijetnju tijekom životnog ciklusa u sustavu.



Strojno učenje

ESET od 1990. radi s algoritmima strojnog učenja radi otkrivanja i blokiranja prijetnji. Neuronske mreže dodane su modulu detekcije ESET-ovih programa 1998. godine.

Strojno učenje uključuje [otkrivanje DNK](#), koje se služi modelima na bazi strojnog učenja radi učinkovitog rada uz

vezu s cloudom ili bez nje. Algoritmi strojnog učenja također su ključan dio početnog razvrstavanja i klasifikacije ulaznih uzoraka, kao i njihova stavljanja na zamišljenu „kartu sigurnosti na mreži”.

ESET je razvio vlastiti modul strojnog učenja, koji se temelji na kombinaciji neuronskih mreža (kao što je duboko učenje ili duga kratkoročna memorija) i posebno odabranoj skupini od šest klasifikacijskih algoritama. Time se omogućuje generiranje konsolidiranih izlaznih informacija i ispravno označivanje ulaznog uzorka kao čistog, potencijalno nepoželjnog ili zlonamjernog.

ESET-ov modul strojnog učenja precizno je prilagođen kako bi mogao raditi zajedno s ostalim tehnologijama zaštite, kao što su DNK, testno okruženje ili [analiza memorije](#), kao i izdvajanje funkcija ponašanja, a sve u cilju pružanja najbolje stope otkrivanja prijetnji i najmanjeg mogućeg broja [lažno pozitivnih rezultata](#).

Konfiguracija skenera u odjeljku "Napredno podešavanje" ESET-ovih programa

- [ESET-ovi Windows programi za kućnu upotrebu](#) (od verzije 13.1)
- [ESET-ovi Windows sigurnosni programi](#) (od verzije 7.2)

Zaštita od mrežnog napada

Zaštita od mrežnog napada proširenje je firewalla koje poboljšava otkrivanje zloupornab poznatih slabih točaka na mrežnoj razini. Implementiranjem otkrivanja najčešćih zloupornab u protokolima koji se najčešće koriste kao što su SMB, RPC i RDP, zaštita od mrežnog napada predstavlja još jedan važan sloj zaštite od širenja zlonamjernog softvera, mrežnih napada i iskorištavanja slabih točaka za koje zakrpa još nije izdana ili primjenjena.

Zaštita od ransomwarea

Zaštita od ransomwarea je metoda otkrivanja prijetnji na temelju ponašanja koja nadzire ponašanje aplikacija i procesa koji pokušavaju mijenjati datoteke na sličan način kao i [ransomware ili koderi datoteka](#). Ako se smatra da se aplikacija ponaša zlonamjerno ili ako se prilikom skeniranja na temelju reputacije pokaže da je aplikacija sumnjiva, ona će se blokirati i proces se zaustavlja ili će se od korisnika tražiti da je blokira ili dopusti.

ESET LiveGrid® mora biti aktiviran kako bi Zaštita od ransomwarea ispravno radila. Pogledajte naš članak iz [ESET-ove baze znanja](#) kako biste osigurali da je ESET LiveGrid® aktiviran i da funkcioniра u vašem ESET-ovu programu.

Zaštita od napada na temelju skripti

Zaštita od napada na temelju skripti sastoji se od zaštite od javascripta u web preglednicima i zaštite programa Antimalware Scan Interface (AMSI) od skripti u PowerShellu.



HIPS

HIPS mora biti [aktiviran](#) da bi ova značajka radila.

Zaštita od napada na temelju skripti podržava sljedeće web-preglednike:

- Mozilla Firefox
- Google Chrome

- Internet Explorer
- Microsoft Edge

Uporaba podržanog web preglednika

i Minimalne podržane verzije web preglednika mogu se razlikovati jer se potpis datoteke preglednika prilično često mijenja. Međutim, najnovija verzija web preglednika uvijek je podržana.

Zaštićeni preglednik

Zaštićeni preglednik dodatan je sloj zaštite osmišljen za zaštitu vaših osjetljivih podataka tijekom pregledavanja na mreži (na primjer, finansijskih podataka tijekom mrežnih transakcija).

ESET Endpoint Security 8 i njegove novije verzije sadrže ugrađeni popis web stranica koje će pokrenuti otvaranje zaštićenog preglednika. U odjeljku konfiguracije programa možete dodati web stranicu ili urediti popis web stranica. Zaštićeni preglednik je standardno deaktiviran nakon instalacije.

Više informacija o toj značajci pročitajte u ovom [članku ESET-ove baze znanja](#).

Za sigurno pregledavanje weba nužna je upotreba šifrirane HTTPS komunikacije. Da biste se mogli koristiti Zaštićenim preglednikom, vaš internetski preglednik mora zadovoljavati minimalne zahtjeve navedene u nastavku:

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

i Na uređajima s ARM procesorima podržani su samo Firefox i Microsoft Edge.

Otvorite ESET-ov zaštićeni preglednik u željenom web pregledniku

Kada otvorite ESET-ov zaštićeni preglednik izravno s kartice **Alati** u izborniku programa, otvara se u web pregledniku koji ste postavili kao standardni. U suprotnom, kada otvorite željeni web preglednik (ne iz izbornika programa), ESET-ov interni popis će se preusmjeriti na istu vrstu web preglednika koju štiti ESET.

Skener za UEFI

Skener za jedinstveno sučelje za proširivi firmware (UEFI) dio je sustava za sprečavanje upada utemeljenog na serveru (HIPS-a) koji štiti UEFI firmware na vašem računalu. UEFI firmware učitava se u memoriju na početku pokretanja sustava. Kod se nalazi na čipu flash memorije zalemljenom na matičnoj ploči. Njegovom zarazom napadači mogu instalirati zlonamjerni program koji preživljava ponovne instalacije i ponovna pokretanja sustava. Također se lako može dogoditi da rješenja protiv zlonamjernih programa ne primijete zlonamjerni program jer većina njih ne skenira taj sloj.

Skener za UEFI automatski je aktiviran. Također možete ručno pokrenuti skeniranje računala u glavnom prozoru programa tako da kliknete **Skeniranje računala > Napredna skeniranja > Prilagođeno skeniranje** i odaberete

Ako je vaše računalo već zaraženo zlonamjernim softverom za UEFI, pročitajte sljedeći članak u ESET-ovoј bazi znanja:
[Moje računalo zaraženo je zlonamjernim softverom UEFI, što trebam učiniti?](#)

Lažna datoteka

Lažna datoteka je lažni računalni dokument umetnut među stvarne dokumente koji pomaže u ranoj detekciji neovlaštenog pristupa podacima, njihova kopiranja ili izmjene.

Mrtva petlja

Mrtva petlja je situacija u kojoj svaki računalni proces čeka resurs koji je dodijeljen drugom procesu. U takvoj situaciji nijedan proces se ne izvršava jer resurs koji mu je potreban zadržava drugi proces koji isto tako čeka da se oslobodi drugi resurs. Važno je spriječiti mrtvu petlju prije nego što do nje dođe. Planer resursa može otkriti pojavu mrtve petlje, što pomaže operativnom sustavu da prati sve resurse dodijeljene različitim procesima. Mrtva petlja se može dogoditi ako se sljedeća četiri uvjeta istovremeno:

- **Nema preventivne radnje** – resurs može osloboditi proces koji ga zadržava samo dobrovoljno nakon što taj proces završi svoj zadatak.
- **Uzajamni izuzetak** – posebna vrsta binarnog semafora koji se upotrebljava za kontrolu pristupa zajedničkom resursu. Omogućuje da se trenutačni zadaci višeg prioriteta blokiraju tijekom što kraćeg razdoblja.
- **Zadržavanje i čekanje** – u ovom uvjetu potrebno je spriječiti procese da zadržavaju jedan resurs ili nekoliko resursa dok istovremeno čekaju jedan ili više drugih resursa.
- **Kružno čekanje** – nameće stvaranje ukupnog redoslijeda svih vrsta resursa. Kružno čekanje isto tako zahtijeva da svaki proces zahtijeva resurse od manjeg prema većem prebrojavanju.

Postoje tri načina za rješavanje mrtve petlje:

- Nemojte dopustiti sustavu da uđe u stanje mrtve petlje.
- Pustite da dođe do mrtve petlje, a zatim poduzmite preventivnu radnju kako biste je riješili.
- Ako dođe do mrtve petlje, ponovno pokrenite sustav.