ESET Glossary

Používateľská príručka

Pre zobrazenie tohto dokumentu v online verzii kliknite sem

Digital Security
Progress. Protected.

ESET Glossary bol vyvinutý spoločnosťou ESET, spol. s r. o.

Viac informácií nájdete na webovej stránke www.eset.sk.

Kontaktný formulár: https://www.eset.com/sk/podpora/kontakt/

REV. 12.4.2024

Vitajte v slovníku pojmov spoločnosti ESET

Náš slovník pojmov poskytuje komplexný prehľad súčasných hrozieb a technológií ESET, ktoré vás pred nimi chránia.

Témy sú rozdelené do nasledujúcich kapitol, ktoré popisujú:

- Detekcie – počítačový vírus, červ, trójsky kôň, potenciálne nechcené aplikácie atď.
- Vzdialené útoky – hrozby, ktoré sa vyskytujú v lokálnych sieťach alebo na internete.
- E-mailové hrozby – hoax, phishing, scam atď.
- Technológie ESET – ide o funkcie, ktoré sú súčasťou bezpečnostných riešení ESET.

Advér

Advér (adware) je skratka od „advertising‑supported software“. Do tejto kategórie patria programy, ktorých úlohou je zobrazovať reklamu. Advér zvyčajne sám otvorí nové okno (tzv. pop‑up okno) s reklamou v internetovom prehliadači alebo zmení nastavenie domovskej stránky prehliadača. Používajú ho často výrobcovia voľne šíriteľných (bezplatných) programov, aby si finančne zabezpečili ďalší vývoj svojej vlastnej, mnohokrát užitočnej aplikácie.

Samotný advér sám osebe nebýva škodlivý, len používateľa obťažuje. Nebezpečenstvo spočíva v tom, že môže vykonávať aj sledovanie (ako spyvér).

Ak sa používateľ rozhodne pre voľne šíriteľný softvér, odporúča sa venovať procesu inštalácie zvýšenú pozornosť. Inštalátor totiž zvyčajne upozorňuje, že sa popri zvolenom programe nainštaluje aj advér. V mnohých prípadoch môže používateľ zakázať jeho inštaláciu.

Na druhej strane niektoré programy sa bez prídavného advéru odmietnu nainštalovať, prípadne budú mať obmedzenú funkčnosť. Z toho vyplýva, že advér sa môže dostať do systému „legálnou“ cestou, pretože používateľ s tým súhlasí. Pozornosť je teda namieste. Ak sa nájde na vašom počítači súbor, ktorý je detegovaný ako advér, odporúčanou akciou je zmazanie, keďže je veľká pravdepodobnosť, že súbor obsahuje nebezpečný kód.

Botnet

Bot alebo webový robot je škodlivý program, ktorý prechádza sieťové adresy a infikuje zraniteľné počítače. Hackeri takto môžu prevziať kontrolu nad viacerými počítačmi naraz a zmeniť ich na boty (tiež známe ako zombie). Hackeri väčšinou používajú boty na infikovanie veľkej skupiny počítačov, ktoré spolu vytvoria sieť alebo tiež botnet. Akonáhle je váš počítač v sieti botnet, môže byť použitý na šírenie DDoS útokov, proxy a tiež na vykonávanie automatizovaných úloh cez internet bez toho, aby ste o tom vedeli (napríklad na posielanie nevyžiadanej pošty či vírusov alebo na ukradnutie súkromných informácií, ako sú prihlasovacie údaje do internet bankingu alebo čísla kreditných kariet).

Falošný poplach (FP)

V reálnom prostredí nie je možné zaručiť 100 % úspešnosť detekcie a rovnako ani 0 % možnosť nesprávneho vyhodnotenia a zaradenia bezpečných objektov medzi skutočné detekcie.

Falošný poplach (FP) predstavuje bezpečný súbor alebo aplikáciu, ktorá bola nesprávne klasifikovaná ako malvér alebo PUA (potenciálne nechcená aplikácia).

Packer

Packer je spustiteľný samorozbaľovací súbor, ktorý v sebe obsahuje niekoľko druhov malvéru v jednom balíku.

Najznámejšie packery sú napr. UPX, PE_Compact, PKLite a ASPack. Jeden malvér môže byť detegovaný viacerými spôsobmi, pretože môže byť komprimovaný vždy pomocou iného packera. Packery majú schopnosť mutácie vlastných „signatúr“, preto je takýto malvér ťažšie odhaliť a odstrániť.

Potenciálne nebezpečné aplikácie

Existuje množstvo programov, ktoré v bežných podmienkach slúžia používateľom k uľahčeniu činnosti, administrácii počítačových sietí a pod. V nesprávnych rukách však môže dôjsť k ich zneužitiu na nekalé účely. ESET ponúka možnosť detekcie takýchto aplikácií.

Potenciálne nebezpečné aplikácie predstavujú klasifikáciu používanú pre komerčný a legitímny softvér, ako napríklad nástroje vzdialeného prístupu, nástroje na prelomenie hesiel a keyloggery (programy zaznamenávajúce každé stlačenie klávesu používateľom).

V prípade, že používateľ zistí prítomnosť potenciálne nebezpečnej aplikácie, ktorá sa nachádza v systéme bez jeho vedomia, resp. bez vedomia správcu siete, danú aplikáciu odporúčame odstrániť.

Potenciálne nechcené aplikácie

Grayware alebo tiež potenciálne nechcená aplikácia (PUA) je označenie pre širokú škálu softvéru, ktorý nie je jednoznačne škodlivý ako iné druhy malvéru, napríklad vírusy alebo trójske kone. Môže však na váš počítač nainštalovať ďalší nežiaduci softvér, zmeniť správanie zariadenia, vykonávať neočakávané operácie, prípadne akcie bez súhlasu používateľa.

Kategórie softvéru, ktoré môžu byť považované za grayware, zahŕňajú: softvér zobrazujúci reklamy, softvér sťahujúci popri želanom obsahu aj neželaný softvér (tzv. download wrappers), rôzne panely nástrojov pre webové prehliadače, softvér so zavádzajúcim správaním, softvér inštalujúci ďalší neželaný softvér (tzv. bundleware), softvér na sledovanie (tzv. trackware), aplikácie na zdieľanie internetového pripojenia (tzv. proxyware), aplikácie na ťaženie kryptomeny, nástroje na čistenie registrov (tzv. registry cleaners; len na operačných systémoch Windows) alebo akékoľvek iné druhy softvéru hraničiace so škodlivými programami, prípadne softvér, ktorý využíva nezákonné alebo prinajmenšom neetické obchodné praktiky (napriek tomu, že sa tvári ako legitímny softvér) a ktorý by koncový používateľ mohol považovať za nežiaduci v prípade, že by vedel o všetkých následkoch jeho inštalácie.

Potenciálne nebezpečné aplikácie sú legitímnym (poprípade komerčným) softvérom, ktorý však môže byť útočníkmi zneužitý na nekalé účely. Detekciu týchto aplikácií môžete v nastaveniach produktu ESET kedykoľvek

zapnúť alebo vypnúť.

Vyskytujú sa situácie, keď sa používateľ rozhodne, že výhody, ktoré mu potenciálne nechcená aplikácia poskytuje, prevyšujú riziko spojené s jej používaním. Preto ich ESET radí do kategórie s nižším rizikom ako iné typy škodlivého softvéru, napr. trójske kone alebo červy.

- Upozornenie – Nájdená potenciálne nechcená aplikácia
- Nastavenia
- Softvérové „wrappery“
- Programy čistenia registrov
- Potenciálne nechcený obsah

> **Ilustrované inštrukcie**
> Ak chcete vedieť ako skontrolovať systém a odstrániť potenciálne nechcené aplikácie (PUA) pomocou našich produktov ESET pre domácnosti so systémom Windows, prečítajte si článok v Databáze znalostí spoločnosti ESET.

Upozornenie – Nájdená potenciálne nechcená aplikácia

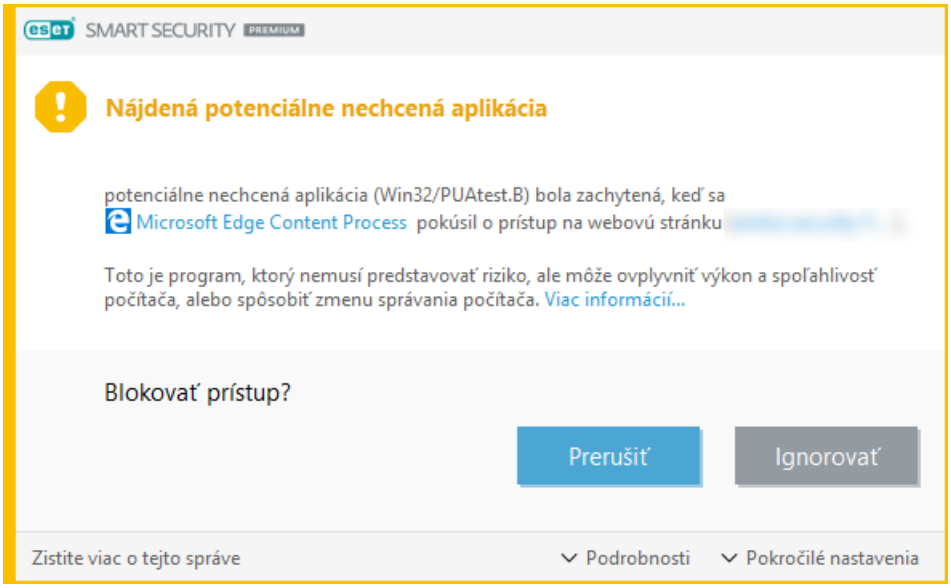
Keď sa nájde potenciálne nechcená aplikácia, budete môcť zvoliť akciu, ktorú má program vykonať:

1.**Vyliečiť/Prerušiť** – zvolením tejto možnosti zablokujete prístup potenciálne nechcenej aplikácie do vášho počítača.
Možnosť **Prerušiť** sa vám v upozornení o detekcii potenciálne nechcenej aplikácie zobrazí pri sťahovaní z webovej stránky a možnosť **Vyliečiť** v prípade súboru nachádzajúceho sa na disku počítača.

2.**Ignorovať** – nevykoná sa žiadna akcia a potenciálne nechcenej aplikácii bude povolený prístup do vášho počítača.

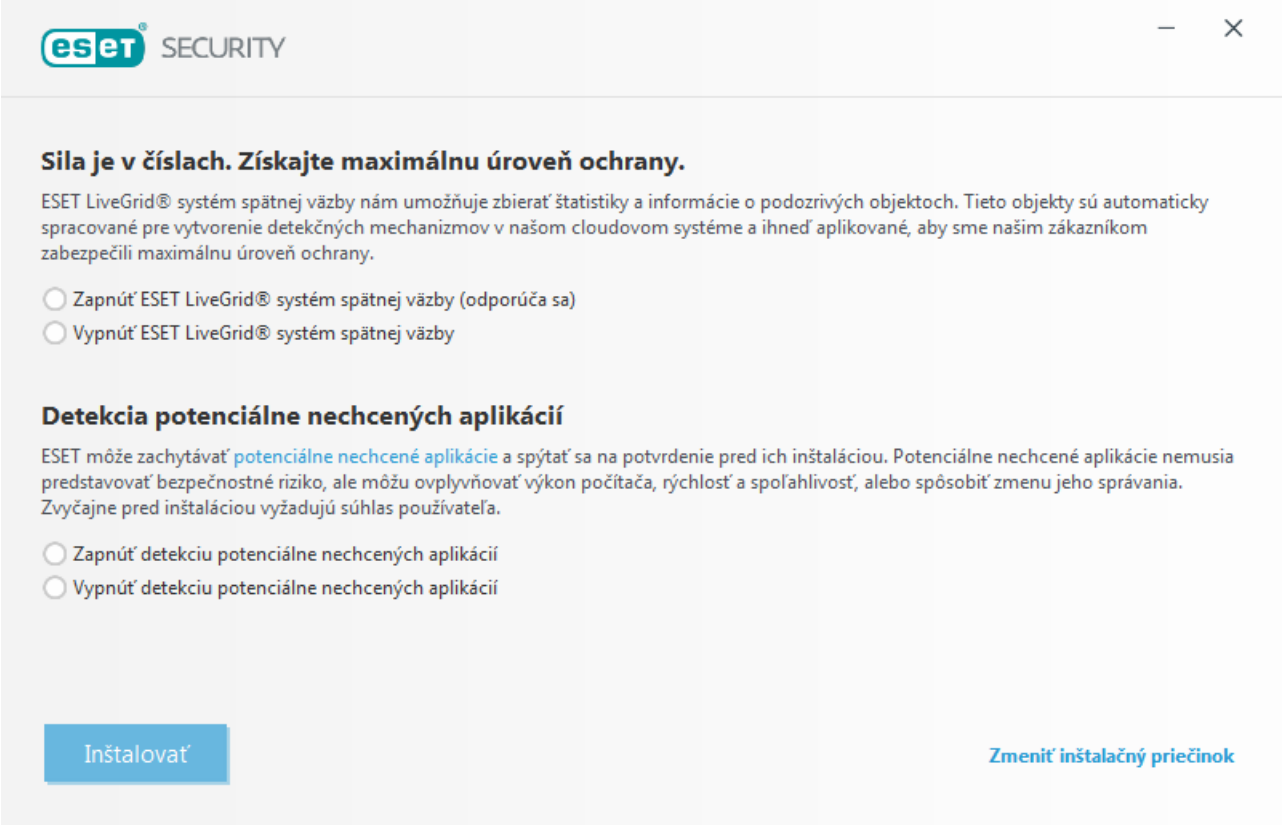
3.**Vylúčiť z detekcie** – ak si želáte, aby sa detegovaný súbor, ktorý už sa nachádza na vašom počítači, mohol v budúcnosti spúšťať bez ďalších upozornení a prerušení, kliknite na **Pokročilé nastavenia**, označte možnosť Vylúčiť z detekcie a nakoniec kliknite na tlačidlo **Ignorovať**.

4.**Vylúčiť signatúru z detekcie** – ak chcete povoliť, aby sa v budúcnosti mohli na vašom počítači bez ďalších upozornení a prerušení spúšťať všetky súbory (či už spomedzi existujúcich súborov alebo pri sťahovaní z internetu), ktoré program ESET deteguje pod daným názvom (signatúrou), kliknite na **Pokročilé nastavenia**, označte možnosť **Vylúčiť signatúru z detekcie** a nakoniec kliknite na tlačidlo **Ignorovať**. Ak sa hneď zobrazia ďalšie okná upozornení s názvom (signatúrou) rovnakej detekcie, kliknite na Ignorovať, čím ich zatvoríte (akékoľvek ďalšie okno, ktoré sa zobrazilo, sa týka detekcie, ktorá prebehla ešte pred tým, ako ste signatúru vylúčili z budúcich detekcií).



Nastavenia

Počas inštalácie svojho produktu ESET sa môžete rozhodnúť, či chcete zapnúť detekciu potenciálne nechcených aplikácií, ako to môžete vidieť na nasledujúcom obrázku:



Upozornenie

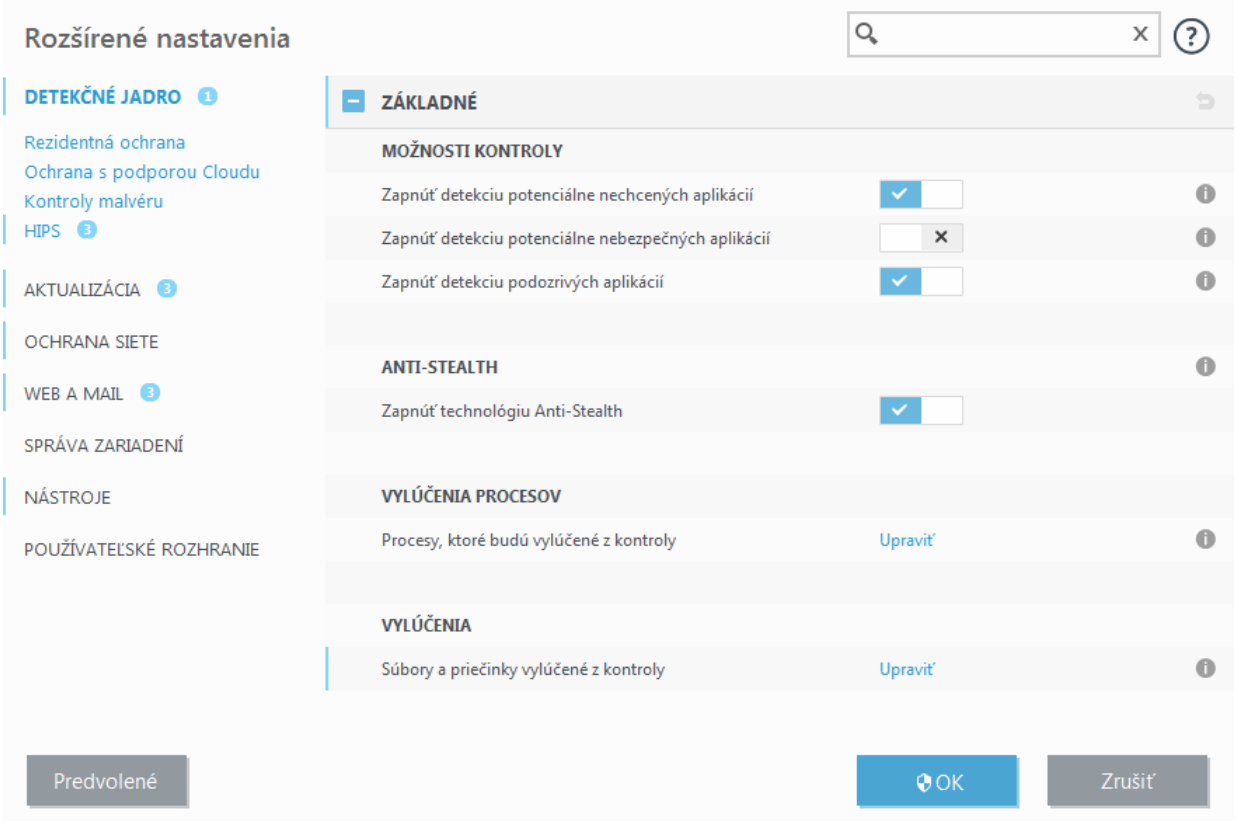
Potenciálne nechcené aplikácie môžu so sebou niesť riziko inštalácie advéru (t. j. reklamného softvéru) a panelov nástrojov alebo obsahovať iné nechcené či nebezpečné programové súčasti.

Toto nastavenie môžete kedykoľvek zmeniť v nastaveniach programu. Pre zapnutie alebo vypnutie detekcie potenciálne nechcených, nebezpečných alebo podozrivých aplikácií postupujte podľa týchto pokynov:

1. Otvorte svoj produkt ESET.

2. Stlačte kláves **F5** pre otvorenie okna **Rozšírené nastavenia**.

3. Prejdite do sekcie **Detekčné jadro** (v prechádzajúcich verziách programu išlo o sekcie **Antivírus** alebo **Počítač**) a povoľte alebo zakážte možnosti **Zapnúť detekciu potenciálne nechcených aplikácií**, **Zapnúť detekciu potenciálne nebezpečných aplikácií** a **Zapnúť detekciu podozrivých aplikácií** podľa vašich preferencií. Kliknite na **OK** pre uloženie nastavení.



Ilustrované inštrukcie

Podrobnejšie informácie o tom, ako nakonfigurovať produkty ESET, aby zachytávali alebo naopak ignorovali potenciálne nechcené aplikácie (PUA), nájdete v nasledujúcich článkoch Databázy znalostí spoločnosti ESET:

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

Softvérové „wrappery“

Softvérový „wrapper“ (z angl. baliť, obaľovať) je špeciálny softvér na zmenu aplikácií, ktorý využívajú napríklad niektoré internetové stránky ponúkajúce rozličné súbory na stiahnutie. Wrapper je aplikácia tretej strany, ktorá vám nainštaluje program, ktorý si chcete stiahnuť, ale súbežne s ním nainštaluje aj ďalší softvér, ako napríklad panely s nástrojmi do internetového prehliadača alebo advér. Tento prídavný softvér tiež môže zmeniť nastavenia domácej stránky či nastavenia vyhľadávania vo vašom prehliadači. Mnohé internetové stránky poskytujúce služby ukladania/sťahovania súborov (file hosting) často neupozornia predajcov softvéru ani používateľov na zmenu v sťahovaných súboroch a neuľahčujú možné vynechanie už spomínaných potenciálne nechcených sprievodných

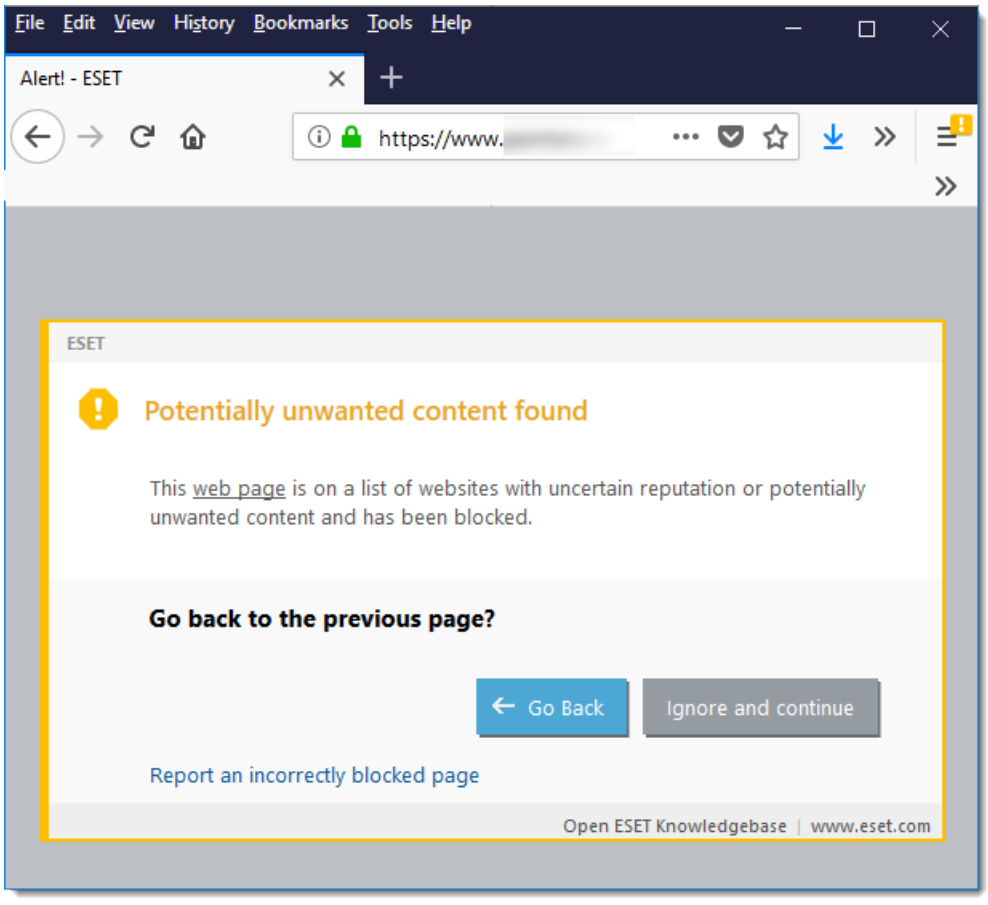
dodatkov pri inštalácii. Z týchto dôvodov ESET klasifikuje softvérový „wrapper“ ako jeden z typov potenciálne nechcených aplikácií, aby tak mali používatelia možnosť výberu, či chcú sťahovaný súbor prijať alebo sťahovanie odmietnuť.

Programy čistenia registrov

Nástroje na čistenie registrov (tzv. „registry cleaners“) sú programy, ktoré môžu naznačovať, že databáza Registry systému Windows vyžaduje pravidelnú údržbu alebo čistenie. Použitie takéhoto programu však môže pre systém vášho počítača predstavovať aj určité riziká. Niektoré nástroje na čistenie registrov navyše prezentujú neodborné, neoveriteľné či nepodložené tvrdenia o svojich výhodách a/alebo na základe výsledkov „bezplatnej kontroly“ generujú zavádzajúce správy o počítačovom systéme. Cieľom týchto zavádzajúcich tvrdení a správ je presvedčiť vás, aby ste si zakúpili plnú verziu alebo si program predplatili, pričom zvyčajne nemáte možnosť si program pred platbou plnohodnotne vyskúšať a zhodnotiť. Z uvedených dôvodov ESET klasifikuje takéto programy ako potenciálne nechcené aplikácie (PUA) a poskytuje vám možnosť ich povoliť alebo blokovať.

Potenciálne nechcený obsah

Ak je povolená detekcia potenciálne nechcených aplikácií vo vašom produkte ESET, ako potenciálne nechcený obsah budú blokované tie webové stránky, ktoré majú reputáciu šírenia potenciálne nechcených aplikácií alebo zavádzania používateľov k vykonaniu takých krokov, ktoré môžu mať negatívny vplyv na prehliadanie webu či systém počítača. Ak sa zobrazí upozornenie, že stránka, ktorú sa pokúšate navštíviť, je klasifikovaná ako potenciálne nechcený obsah, môžete kliknúť na možnosť **Prejsť naspäť**, čím sa dostanete o krok späť od zablokovanej webovej stránky, alebo možnosť **Ignorovať alebo pokračovať**, čím povolíte načítanie stránky.



Podrobnejšie informácie o tejto téme nájdete v tomto článku Databázy znalostí spoločnosti ESET.

Ransomvér

Ransomvér (tiež známy ako filecoder) je typ malvéru, ktorý uzamkne vaše zariadenie, prípadne zašifruje obsah, ktorý je na ňom uložený. Jeho cieľom je vymáhať od vás peniaze s prísľubom obnovenia prístupu k vášmu obsahu po zaplatení požadovanej sumy. Súčasťou tohto malvéru môže byť aj časovač s vopred naprogramovanou lehotou splatnosti, ktorá musí byť dodržaná. Ak sa táto lehota nedodrží, cena sa zvýši, prípadne sa zariadenie stane natrvalo neprístupným.

Keď sa zariadenie infikuje, filecoder sa môže pokúsiť zašifrovať zdieľané disky. Môže to vyzerať tak, že sa malvér šíri po sieti, v skutočnosti k tomu však nedochádza. Takáto situácia nastáva v prípade, ak je zdieľaný disk na súborovom serveri zašifrovaný, avšak samotný server malvérom napadnutý nie je (pokiaľ nejde o terminálový server).

Autori ransomvéru vygenerujú kľúčový pár: verejný a súkromný kľúč, pričom verejný kľúč vložia do malvéru. Samotný ransomvér môže byť súčasťou trójskeho koňa, prípadne môže mať podobu súboru alebo obrázka, ku ktorému sa môžete dostať prostredníctvom e-mailu, sociálnych sietí alebo nástrojov na okamžité posielanie správ (instant messenger). Po infiltrácii počítača malvér vygeneruje náhodný symetrický kľúč a zašifruje dáta na zariadení. Na zašifrovanie symetrického kľúča použije verejný kľúč nachádzajúci sa v malvéri. Ransomvér potom za dešifrovanie dát požaduje od používateľa zaplatenie určitej sumy peňazí. Správa obsahujúca výzvu na zaplatenie, ktorá sa zobrazí na zariadení, môže byť falošným varovaním, ktoré hovorí o tom, že váš systém bol použitý na nelegálne aktivity alebo obsahuje nelegálny obsah. Od obete ransomvéru sa požaduje platba pomocou rôznych platobných metód. Možnosti platby sú zvyčajne tie, ktoré sú ťažko vystopovateľné, napríklad digitálne (krypto) meny, SMS správy s nadmernými poplatkami, predplatené kupóny atď. Po prijatí platby sa od autorov ransomvéru očakáva, že použijú svoj súkromný kľúč na dešifrovanie symetrického kľúča a dešifrujú tak dáta obete. Bohužiaľ, táto operácia nie je zaručená.

> **Viac informácií o ochrane pred ransomvérom**
>
> Produkty ESET používajú viacvrstvovú technológiu, ktorá zariadenia chráni pred ransomvérom. Prečítajte si náš článok Databázy znalostí spoločnosti ESET, v ktorom nájdete osvedčené postupy na ochranu vášho systému pred ransomvérom.

Rootkit

Rootkit je kategóriou škodlivého softvéru, ktorý zabezpečí útočníkovi prienik do systému, pričom utají svoju prítomnosť. Ide o program, ktorý po preniknutí do systému (zvyčajne využitím bezpečnostnej diery) po sebe zahladí všetky stopy – prítomnosť súborov, spustené procesy, zápisy v registroch Windows atď. Vzhľadom na to je v podstate neodhaliteľný bežnou kontrolou.

Pri prevencii je potrebné vziať na vedomie fakt, že s rootkitom je možné prísť do kontaktu na dvoch úrovniach:

1. V momente, keď sa snaží preniknúť do systému. V tomto prípade sa ešte nenachádza v systéme, teda ešte nie je aktívny. Antivírusový systém si s ním poradí (za predpokladu, že rozpozná, že ide o infiltráciu).

2. Keď je už zavedený v systéme a nedetegovateľný štandardným spôsobom kontroly. Používatelia produktov ESET majú výhodu v tom, že naše produkty používajú technológiu Anti-Stealth a dokážu aktívne rootkity odhaliť a eliminovať.

Návratovo orientované programovanie

Návratovo orientované programovanie (ang. return‑oriented programming; ROP) je typickým útokom zneužívajúcim kód, pri ktorom útočník so škodlivým úmyslom ovláda tok riadenia softvéru prostredníctvom existujúceho kódu. Útok ROP je pokročilou verziou pretečenia zásobníka (tzv. stack‑smashing). K pretečeniu zásobníka dochádza vtedy, keď program zapisuje na pamäťovú adresu mimo určenej dátovej štruktúry zásobníka volaní programu, zvyčajne s vyrovnávacou pamäťou pevnej dĺžky.

ROP je technika zneužitia, ktorá umožňuje spúšťanie kódu v cieľovom systéme. Získaním kontroly nad zásobníkom volaní útočník ovláda procesy existujúceho dôveryhodného softvéru bežiaceho v počítači a manipuluje s ním tak, aby vykonal inú ako zamýšľanú úlohu.

Spyvér

Kategória spyvéru zahŕňa aplikácie, ktoré posielajú súkromné informácie bez súhlasu používateľa. Predmetom odosielania sú rôzne štatistické informácie, ako napríklad zoznam navštevovaných internetových stránok, zoznam e‑mailových adries v adresári alebo klávesy stlačené používateľom.

Tvorcovia takýchto programov argumentujú, že ide len o snahu zistiť potreby alebo záujmy používateľa a zásobovať ho lepšie cielenou reklamou. Hranica medzi užitočnými a škodlivými aplikáciami je však v tomto prípade veľmi nejasná a nemožno zaručiť, že získané informácie nebudú v budúcnosti zneužité. Údaje získané metódami spyvéru totiž môžu obsahovať aj rôzne bezpečnostné kódy, čísla bankových účtov, PIN kódy atď. Spyvér je často súčasťou bezplatných verzií programov, aby autor nadobudol zisk, resp. presvedčil používateľa ku kúpe programu. Používatelia sú často informovaní o prítomnosti spyvéru počas inštalácie programu, aby zvážili zakúpenie plnej verzie, ktorá spyvér neobsahuje.

Príkladom voľne šíriteľného softvéru obsahujúceho spyvér sú hlavne klientske aplikácie P2P (peer‑to‑peer) sietí. Zvláštnou podkategóriou sú programy vydávajúce sa za antispyvér, pričom samé spyvér obsahujú – napr. Spyfalcon, Spy Sheriff.

Ak bol na vašom počítači detegovaný spyvér, odporúčame vám súbor zmazať, pretože je vysoko pravdepodobné, že obsahuje škodlivý kód.

Keyloggery sú podkategóriou spyvéru. Existujú hardvérové a softvérové keyloggery. Softvérové keyloggery môžu zbierať iba informácie zadané na jednej webovej stránke alebo v jednej aplikácii. Sofistikovanejšie keyloggery dokážu zaznamenávať všetok napísaný text vrátane informácií, ktoré sú skopírované alebo vložené. Niektoré keyloggery zamerané na mobilné zariadenia môžu zaznamenávať hovory, informácie z aplikácií na odosielanie a prijímanie správ, polohu či dokonca záznamy z mikrofónu a kamery.

Trójsky kôň

Počítačové trójske kone sú infiltrácie, ktoré sa snažia zamaskovať sa za užitočné programy a zabezpečiť tým svoje spustenie.

Trójsky kôň je v súčasnosti všeobecný pojem, ide o pomerne širokú kategóriu aplikácií, z ktorých najznámejšie sú:

- Downloader – škodlivý kód, ktorého úlohou je sťahovať do systému ďalšie infiltrácie z internetu.
- Dropper – škodlivý kód, tzv. nosič. Prenáša v sebe ukrytý ďalší škodlivý softvér a sťažuje tým jeho detekciu

pomocou antivírusových programov.

• Backdoor – škodlivý kód umožňujúci komunikáciu so vzdialeným útočníkom, ktorý tak môže získať prístup a kontrolu nad napadnutým systémom.

• Keylogger (keystroke logger) – program, ktorý sleduje, aké klávesy používateľ stláča a informácie zasiela vzdialenému útočníkovi.

• Dialer – pripája sa na zahraničné čísla, ktoré sú spoplatnené vysokými čiastkami. Používateľ si prakticky nemá šancu všimnúť odpojenie od miestneho poskytovateľa pripojenia a vytvorenie nového pripojenia do zahraničia. Reálnu škodu môžu spôsobiť iba používateľom so starším vytáčaným pripojením (tzv. dial-up).

Súbor trójskeho koňa neobsahuje v zásade nič iné okrem samotného škodlivého kódu, preto odporúčanou akciou v prípade infekcie je zmazanie.

Vírus

Tento druh infiltrácií napáda zvyčajne už existujúce súbory na disku. Označenie dostal podľa biologického vírusu, pretože sa podobným spôsobom šíri z miesta na miesto. Slovo vírus sa často nesprávne používa na pomenovanie všetkých typov bezpečnostných hrozieb. V súčasnosti sa začína používať presnejšie pomenovanie – malvér alebo škodlivý softvér.

Počítačové vírusy najčastejšie napádajú spustiteľné súbory a dokumenty. Fungujú zhruba takto: po spustení napadnutého súboru dôjde najprv k spusteniu škodlivého kódu. Ten vykoná akciu, ktorú má v sebe naprogramovanú, a až nakoniec sa k slovu dostane pôvodná aplikácia. Vírus môže infikovať všetky súbory, ku ktorým má používateľ povolenia na zápis.

Samotná činnosť aktivovaného vírusu môže mať mnoho podôb. Niektoré vírusy sú krajne nebezpečné, pretože dokážu cielene zmazať súbory z disku. Ostatné len majú poukázať na zručnosť tvorcov a používateľa skôr iba obťažujú, než by mali spôsobiť reálnu škodu.

Ak je váš počítač nakazený vírusom a liečenie nie je možné, pošlite vzorku na analýzu do výskumného laboratória spoločnosti ESET. V prípade infekcie vírusom môžu byť súbory natoľko modifikované, že nie je možné ich vyliečenie a musia byť nahradené ich zálohovanou kópiou.

Červ

Počítačový červ je program so škodlivým kódom, ktorý napáda hostiteľské počítače a cez sieť sa šíri ďalej. Základný rozdiel medzi vírusom a červom je ten, že červ sa dokáže šíriť sám a nie je závislý na hostiteľskom súbore (alebo zavádzacom sektore). Červ využíva na šírenie hlavne elektronickú poštu a bezpečnostné diery v sieťových aplikáciách.

Má preto omnoho dlhšiu životnosť ako vírusy. Vďaka rozšírenosti internetu sa dokáže dostať do celého sveta v priebehu niekoľkých hodín od vydania, niekedy dokonca v priebehu niekoľkých minút. Schopnosť samostatne a rýchlo sa replikovať ich robí nebezpečnejšími ako ostatné typy malvéru.

Červ aktivovaný v systéme dokáže spôsobiť celý rad nepríjemností: môže mazať súbory, značne spomaľuje činnosti PC, deaktivuje niektoré programy. Často sa využíva ako prostriedok na distribúciu iných druhov infiltrácií.

V prípade infekcie červom sa odporúča škodlivý súbor zmazať, pretože obsahuje len škodlivý kód.

Credential stuffing

Credential stuffing je typ kybernetického útoku, pri ktorom sa zneužívajú prihlasovacie údaje z uniknutých databáz. Útočníci používajú botov a iné automatizačné metódy s cieľom prihlásiť sa do účtov na viacerých webových stránkach prostredníctvom uniknutých údajov. Zameriavajú sa na tých používateľov, ktorí recyklujú svoje prihlasovacie údaje na viacerých webových stránkach a službách. Pri úspešnom útoku môžu útočníci získať úplný prístup k účtu a k údajom, ktoré má používateľ v tomto účte uložené. Prístup môžu využiť na odcudzenie osobných údajov s vidinou krádeže identity, podvodné transakcie, šírenie spamu a iné škodlivé aktivity.

DNS Poisoning

Použitím metódy DNS (Domain Name Server) poisoning môžu hackeri oklamať DNS server ľubovoľného počítača, aby považoval podsunuté falošné dáta za legitímne a overené. Tieto falošné informácie sú uložené vo vyrovnávacej pamäti (cache) po určitú dobu, čím umožňujú útočníkom prepísať DNS odpovede z IP adries. Výsledkom je, že používatelia, ktorí chcú pristupovať na webové stránky, sťahujú počítačové vírusy alebo červy namiesto originálneho obsahu.

DoS útok

DoS, čiže Denial of Service, je pokus útočníka zamedziť používateľom prístup k počítaču alebo sieti. Komunikácia medzi používateľmi je natoľko preťažená, že nemôže adekvátne prebiehať. Napadnutý počítač je zvyčajne potrebné reštartovať, aby mohol poskytovať plnohodnotné služby.

Cieľom sa najčastejšie stávajú webové servery a účelom útoku je vyradiť ich na určitú dobu z činnosti.

Útok cez protokol ICMP

Protokol ICMP (Internet Control Message Protocol) je jedným z hlavných internetových protokolov. Slúži na odosielanie rôznych chybových hlásení a na tento účel ho využívajú hlavne počítače v sieti.

Útoky vedené cez protokol ICMP zneužívajú jeho slabé miesta. ICMP je využívaný na zasielanie jednosmerných odkazov, pričom nie je používaná žiadna autentifikácia. Toto umožňuje vzdialeným útočníkom spúšťať útoky typu DoS (Denial of Service) alebo útoky, ktoré dávajú neoprávneným osobám prístup k prichádzajúcim a odchádzajúcim paketom.

Typickými príkladmi ICMP útokov sú ping flood, ICMP_ECHO flood alebo smurf attack. Medzi symptómy patrí značné spomalenie internetových aplikácií, prípadne krátkodobé alebo aj dlhodobé odpojenie od internetu.

Skenovanie portov

Skenovanie portov je činnosť, ktorou sa systematicky overuje prístupnosť počítačových portov. Skener portov je špeciálny softvér, ktorý dokáže zistiť v sieti prípadné otvorené porty.

Počítačový port je miesto, ktorým prechádzajú informácie z/do počítača, takže ide z hľadiska bezpečnosti o kritickú záležitosť. Vo veľkých sieťach má skenovanie portov svoje legitímne opodstatnenie, pretože je to rýchly spôsob odhalenia prípadných bezpečnostných dier.

Skenovanie portov je však aj častá technika používaná hackermi. Prvým krokom je zvyčajne zaslanie paketov na každý port. Na základe odpovede sa dá zistiť, či je port používaný. Samotné skenovanie samo osebe nespôsobuje žiadne škody. Táto technika však umožňuje odhaliť potenciálne zraniteľnosti a získať tak kontrolu nad vzdialeným počítačom.

Sieťovým administrátorom sa odporúča, aby blokovali všetky nepoužívané porty a chránili používané porty pred neovereným prístupom.

SMB Relay

SMB Relay a SMB Relay 2 sú špeciálne programy, ktoré dokážu vykonať útok na vzdialený počítač. Program využíva protokol pre zdieľanie súborov Server Message Block previazaný s NetBIOSom. Ak používateľ zdieľa adresár alebo disk v rámci lokálnej siete, využíva s najväčšou pravdepodobnosťou tento spôsob zdieľania.

V rámci komunikácie v sieti potom dochádza k odosielaniu kontrolných súčtov, „hashov“ používateľských hesiel.

SMB Relay zachytí komunikáciu na UDP porte 139 a 445, presmeruje pakety medzi klientom a serverom danej stanice a modifikuje ich. Po pripojení sa a autentifikácii je klientska stanica odpojená a SMB Relay vytvorí novú virtuálnu IP adresu. K tejto adrese sa potom dá pripojiť pomocou príkazu „net use \\192.168.1.1“ a adresa môže byť využívaná všetkými vstavanými sieťovými funkciami vo Windows. Program prenáša všetku SMB komunikáciu okrem negociácie a autentifikácie. Pokiaľ je vzdialený počítač pripojený, útočník sa na danú IP adresu môže kedykoľvek pripojiť.

Program SMB Relay 2 pracuje na rovnakom princípe, namiesto IP adries ale používa mená z NetBIOS. Oba programy umožňujú útoky typu „man-in-the-middle“ (človek uprostred) – teda útoky, kde útočník dokáže čítať, vkladať a meniť odkazy medzi dvomi stranami bez toho, aby ktorákoľvek zo strán o tom vedela. Najčastejším príznakom je, že systém prestane reagovať, alebo dôjde k náhlemu reštartu.

Odporúčanou ochranou proti týmto útokom je zvýšenie kvality autentifikácie pomocou hesiel alebo kľúčov.

Desynchronizácia TCP

Desynchronizácia TCP je technika používaná pri útokoch typu TCP Hijacking. Je spúšťaná procesom, počas ktorého sa poradové číslo prichádzajúcich paketov líši od očakávaného poradového čísla. Pakety s neočakávaným poradovým číslom sú zamietnuté (alebo uložené vo vyrovnávacej pamäti, ak sú prítomné v aktuálnom komunikačnom okne).

V stave desynchronizácie si obe strany v komunikácii navzájom zahadzujú pakety. Do toho môže vstúpiť útočník (sledujúci danú komunikáciu) a dodať pakety so správnym sekvenčným číslom. Útočník môže prípadne ďalej pridávať do komunikácie príkazy, alebo ju inak modifikovať.

Cieľom útoku je narušiť spojenie na úrovni klient□server alebo peer-to-peer komunikáciu. Brániť sa je možné používaním autentifikácie jednotlivých segmentov TCP. Odporúča sa tiež dodržiavať odporúčané nastavenia pre sieťové zariadenia.

Útoky počítačových červov

Počítačový červ je program so škodlivým kódom, ktorý napáda hostiteľské počítače a cez sieť sa šíri ďalej. Tzv. sieťové červy zneužívajú rôzne bezpečnostné chyby v aplikáciách. Vďaka rozšírenosti internetu sa dokáže dostať

do celého sveta v priebehu niekoľkých hodín od vytvorenia.

Najrozšírenejšie typy útokov (Sasser, SqlSlammer) je možné blokovať štandardnými nastaveniami firewallu, prípadne blokovaním nepoužívaných portov či zabezpečením tých používaných. Dôležitá je tiež inštalácia bezpečnostných záplat a aktualizácií pre operačný systém.

Útok DNS Cache Poisoning

Protokol ARP (Address Resolution Protocol) zabezpečuje preklad adries medzi linkovou vrstvou (MAC adresy) a sieťovou vrstvou (IP adresy). Pri útoku ARP Cache Poisoning dochádza k poškodeniu tabuliek ARP (prekladových tabuliek pre mapovanie MAC adresy na IP adresu zariadenia), čo umožňuje útočníkom zachytiť komunikáciu medzi sieťovými zariadeniami.

Útočník odošle na predvolenú sieťovú bránu falošnú správu s odpoveďou ARP, ktorá uvádza, že daná MAC adresa je prepojená s IP adresou iného cieľa. Keď predvolená brána prijme túto správu a rozošle zmeny všetkým ostatným zariadeniam v sieti, všetka komunikácia cieľa na akékoľvek iné sieťové zariadenie prechádza cez počítač útočníka. Táto akcia umožňuje útočníkovi kontrolovať alebo upravovať komunikáciu pred jej preposlaním na zamýšľaný cieľ.

E-mailové hrozby

E-mail prináša ako forma komunikácie veľa výhod.

Bohužiaľ, s vysokou mierou anonymity vytvára e-mail a internet priestor aj pre ilegálne aktivity, ako je napríklad spamovanie. Spam zahŕňa nevyžiadanú reklamu, falošné správy (hoaxy) a rozširovanie škodlivého softvéru – malvéru. Nebezpečenstvo spamu umocňuje fakt, že náklady na rozposielanie sú v podstate nulové a tvorcovia majú k dispozícii veľa nástrojov a zdrojov na zistenie e□mailových adries. Navyše, objem a rôznorodosť spamu ho robí len ťažko regulovateľným. Čím dlhšie používate svoju e□mailovú adresu, tým pravdepodobnejšie sa ocitnete v databáze spamového mechanizmu.

Zopár tipov na prevenciu:

- Pokiaľ je to možné, nezverejňovať svoju adresu na internete.
- Poskytovať svoju adresu len dôveryhodným osobám.
- Používať nie úplne bežné aliasy – zložitejšie sú ťažšie zistiteľné technikami používanými pri rozosielaní nevyžiadanej pošty.
- Neodpovedať na spam, ktorý ste už dostali do svojej schránky.
- Byť obozretný pri prípadnom vypĺňaní formulárov na internete, najmä pri položkách typu „chcem na e□mail dostávať informácie“.
- Používať viacero „špecializovaných“ e□mailových adries – napr. pracovný e□mail, e□mail pre komunikáciu s priateľmi atď.
- Raz za čas zmeniť e□mailovú adresu.
- Používať antispamové riešenie.

Reklamy

Reklama na internete patrí medzi najrýchlejšie sa šíriace formy reklamy. Jej hlavnou výhodou sú takmer nulové náklady, veľmi vysoká adresnosť, okamžité doručenie odkazu adresátovi a vysoká výnosnosť. Spoločnosti sa snažia týmto spôsobom udržiavať kontakt so svojimi súčasnými klientami, prípadne získať si nových.

Reklama zasielaná e-mailom je sama osebe legitímna. Používateľ môže mať záujem získavať reklamné informácie z určitej oblasti. Často si však nepraje, aby mu bola reklama zasielaná, no napriek tomu sa tak deje. V takomto prípade sa reklamný e-mail stáva zároveň nevyžiadanou poštou – spamom.

Objem nevyžiadaných správ sa stal problémom a nejaví známky spomaľovania. Autori nevyžiadanej pošty sa snažia spam zamaskovať ako legitímne správy.

Falošné správy (hoaxy)

Hoax je mylná informácia, ktorá je hromadne šírená internetom. Najčastejším médiom je e-mail, prípadne komunikačné nástroje typu ICQ a Skype. Ide buď o falošnú poplašnú správu, žart, alebo mystifikáciu – správa sama osebe sa jednoducho nezakladá na pravde.

Hoaxy o počítačových vírusoch majú za cieľ vyvolať strach a neistotu, pričom sa snažia dosiahnuť, aby používatelia uverili, že sa momentálne šíri „neodhaliteľný vírus“, ktorý maže súbory a kradne heslá alebo spôsobuje iný typ škody.

Niektoré hoaxy fungujú spôsobom, že žiadajú od príjemcov, aby boli preposielané ďalej, čím sa hoax šíri. Existujú hoaxy pre mobilné telefóny, žiadosti o pomoc, ľudia zo zahraničia, ktorí vám ponúkajú peniaze atď. Je obvykle nemožné zistiť úmysel autora hoaxu.

Ak uvidíte správu, ktorá vás vyzýva na preposlanie každému, koho poznáte, jedná sa pravdepodobne o hoax. Existuje veľa stránok na internete, ktoré vám môžu pomôcť rozoznať hoax. Ak máte podozrenie, že sa jedná o hoax, uistite sa pred preposlaním správy vyhľadaním na internete.

Phishing

Pojmom phishing sa označuje kriminálna činnosť využívajúca tzv. sociálne inžinierstvo (manipulačné techniky na získanie dôverných informácií). Cieľom je získať citlivé údaje, ako napríklad heslá k bankovým účtom, PIN kódy a iné.

Phishingom označujeme falošný e-mail, ktorý sa snaží pôsobiť dôveryhodne a vzbudiť dojem, že jeho odosielateľom je inštitúcia – banka, poisťovňa. Grafický výzor správy alebo stránka, na ktorú správa odkazuje, sú na prvý pohľad nerozpoznateľné od originálov používaných existujúcimi inštitúciami. Pod rôznymi zámienkami, napríklad overením si prístupových údajov či zaslania sumy peňazí na účet, sú od používateľov získavané osobné údaje (napr. čísla bankových účtov, prihlasovacie mená a heslá). Poskytnuté údaje môžu byť následne ľahko zneužité.

Najlepšou obranou proti phishingu je naň vôbec neodpovedať. Nepatrí totiž medzi bežnú prax finančných (a iných) inštitúcií, aby prostredníctvom e-mailu žiadali od svojich zákazníkov zadanie citlivých prístupových údajov.

Rozpoznávanie spamových podvodov

Existuje niekoľko znakov, podľa ktorých sa dá rozpoznať, či je e-mailová správa vo vašej schránke nevyžiadanou poštou. Ak daná správa spĺňa niektorú z nasledovných podmienok, ide pravdepodobne o nevyžiadanú poštu – spam.

- Adresa odosielateľa nepatrí do vášho zoznamu kontaktov.
- Dostanete výhodnú finančnú ponuku, no žiada sa od vás vstupný poplatok.
- Pod rôznymi zámienkami, napríklad overením si prístupových údajov, zaslania sumy peňazí na účet a podobne, sú od vás požadované citlivé osobné údaje (napr. číslo bankového účtu, heslo do internetového bankovníctva).
- Správa je napísaná v cudzom jazyku.
- Správa ponúka produkt, o ktorý sa nezaujímate. Ak máte predsa len o produkt záujem, je vhodné si overiť priamo u výrobcu, či odosielateľ správy patrí medzi dôveryhodných distribútorov.
- Správa obsahuje skomolené slová, aby sa oklamali filtre pre nevyžiadanú poštu. Napríklad namiesto „viagra“ bude „vaigra“.

Pravidlá

Pravidlá v prostredí antispamového programu, prípadne e-mailového klienta, pomáhajú pri spracúvaní e-mailových správ. Pravidlo sa skladá z dvoch logických častí:

1. Podmienka (napr. správa prichádzajúca z určitej adresy alebo s určitým predmetom)
2. Akcia (napr. zmazanie správy alebo jej presunutie do vopred určeného priečinka)

Množstvo a kombinácia pravidiel závisí od konkrétneho antispamového riešenia. Pravidlá slúžia ako opatrenia proti nevyžiadanej pošte (spamu). Typické príklady:

1. Podmienka: Prichádzajúca správa obsahuje slovo typické pre nevyžiadanú poštu.
2. Akcia: Zmaž správu.

1. Podmienka: Prichádzajúca správa obsahuje ako prílohu súbor s príponou .exe.
2. Akcia: Zmaž prílohu a správu ulož do schránky.

1. Podmienka: Prijatá správa prišla z domény vášho zamestnávateľa.
2. Akcia: Presuň správu do priečinka „Pracovné“.

Na jednoduchšiu prácu s e-mailmi a efektívnejšie filtrovanie spamu odporúčame používať v antispamových programoch kombináciu rôznych pravidiel.

Whitelist

Whitelist je vo všeobecnosti zoznam položiek, prípadne osôb, ktoré sú akceptované alebo majú niekam zabezpečený prístup. Pojmom e□mailový whitelist (povolené adresy) sa označuje zoznam kontaktov, ktoré majú povolenie doručovať správy do používateľovej schránky. Zoznamy možno vytvárať na základe kľúčových slov, ktoré sú potom vyhľadávané v e□mailových adresách, názvoch domén alebo IP adresách.

Ak je whitelist nastavený do režimu exkluzivity, správy z iných adries, domén či IP adries sa do doručenej pošty nedostanú. Ak sa whitelist síce používa, nie však v režime exkluzivity, tak sa takéto správy nevymažú, ale zvyčajne sa vyfiltrujú a presunú do špeciálneho priečinka.

Whitelist je založený na opačnom princípe ako blacklist. Výhodou whitelistu je, že nie je natoľko náročný na udržiavanie ako blacklist. Obe metódy je možné vhodne skombinovať a dosiahnuť tak účinné filtrovanie nevyžiadanej pošty.

Blacklist

Všeobecne je to zoznam blokovaných adries, súborov alebo ľudí. Vo virtuálnom svete predstavuje mechanizmus, ktorý povoľuje prijímanie elektronickej pošty od všetkých odosielateľov, ktorí sa na zozname blokovaných adries nenachádzajú.

Blacklisty sa vyskytujú na dvoch úrovniach. Používateľ si sám vo svojom antispamovom programe môže definovať vlastný zoznam. Existuje však možnosť používať pravidelne aktualizované, profesionálne blacklisty od rôznych inštitúcií, ktorých sa na internete nachádza veľké množstvo.

Blacklist je však aj náročný na udržiavanie, pretože nové adresy, ktoré je potrebné pridať do zoznamu, sa objavujú každý deň. Na docielenie efektívneho filtrovania nevyžiadanej pošty (spamu) odporúčame použiť kombináciu whitelistu a blacklistu.

Výnimka

Zoznam výnimiek zvyčajne obsahuje e□mailové adresy, ktoré môžu byť zneužité na rozposielanie spamu. Správy prijaté z týchto adries budú vždy skontrolované na prítomnosť spamu. Štandardne obsahuje zoznam výnimiek všetky adresy z e□mailových účtov používateľa.

Kontrola na serveri

Kontrola na serveri je technika odhaľovania hromadných nevyžiadaných správ na základe ich počtu a používateľskej reakcie. Na základe obsahu hlavnej časti správy sa vypočíta digitálny „odtlačok“. Číselná hodnota nedáva žiadnu informáciu o obsahu správy. Dve rovnaké správy budú mať rovnaký odtlačok, zatiaľ čo dve rôzne správy budú mať odlišný odtlačok.

Ak používateľ označí danú správu ako nevyžiadanú poštu, odošle sa na server jej odtlačok. Po určitom počte odoslaní rovnakého odtlačku ho server uloží do svojej databázy odtlačkov nevyžiadanej pošty. Pri kontrole doručenej pošty program posiela na server odtlačky prijatých správ. Server vráti informáciu, ktoré odtlačky zodpovedajú pošte, ktorú iní používatelia označili ako „nevyžiadanú“.

Pokročilá kontrola pamäte

Pokročilá kontrola pamäte pracuje spolu s funkciou Exploit Blocker na zvýšení ochrany proti malvéru, ktorý bol navrhnutý tak, aby sa vyhol detekcii bezpečnostných produktov maskovaním a/alebo šifrovaním. V prípadoch, kde bežná emulácia ani heuristika neodhalia hrozbu, pokročilá kontrola pamäte identifikuje podozrivé správanie a deteguje hrozby, ktoré sa spustia v pamäti systému. Toto riešenie je efektívne proti ťažko odhaliteľnému malvéru.

Na rozdiel od funkcie Exploit Blocker je Pokročilá kontrola pamäte metódou pracujúcou až po spustení malvéru. Znamená to, že existuje riziko prebehnutia určitej škodlivej aktivity skôr, ako dôjde k odhaleniu hrozby, avšak aj to len v prípade, že ostatné detekčné techniky zlyhali. Predstavuje preto akúsi dodatočnú vrstvu ochrany.

Ochrana online platieb

Ochrana online platieb predstavuje dodatočnú vrstvu ochrany, ktorej cieľom je chrániť vaše online transakcie a finančné údaje pred zneužitím.

ESET Smart Security Premium a ESET Internet Security obsahujú zoznam vopred zadefinovaných webových stránok, ktoré spúšťajú zabezpečený prehliadač. Webové stránky môžete pridávať do zoznamu a upravovať v nastaveniach programu.

Zabezpečiť všetky prehliadače – týmto nastavením povolíte spúšťanie podporovaných prehliadačov v zabezpečenom režime.

Pre podrobnejšie informácie o tejto funkcii si prečítajte nasledujúce články Databázy znalostí spoločnosti ESET:

- Ako používať ESET Ochranu online platieb?
- Ako pozastavím alebo vypnem Ochranu online platieb v produkte ESET pre domácnosti so systémom Windows?
- Ochrana online platieb – bežné chyby

Na chránené prehliadanie internetu je nevyhnutné použiť šifrovaný komunikačný protokol HTTPS. Ochrana online platieb je podporovaná v týchto prehliadačoch:

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

Otvorte Ochranu online platieb v preferovanom webovom prehliadači

Keď otvoríte Ochranu online platieb priamo z hlavného okna produktu zo záložky **Nástroje**, otvorí sa vo webovom prehliadači, ktorý ste v systéme Windows nastavili ako predvolený. V opačnom prípade pri bežnom spustení preferovaného prehliadača (nie z produktu) budete po prístupe na webovú stránku zo zoznamu chránených stránok presmerovaný na rovnaký typ webového prehliadača zabezpečeného spoločnosťou ESET.

Ochrana pred botnetmi

Ochrana pred botnetmi odhaľuje malvér pomocou analýzy komunikačných sieťových protokolov. Botnet malvér sa často mení na rozdiel od sieťových protokolov, ktoré sa v posledných rokoch nezmenili. Táto nová technológia pomáha spoločnosti ESET odhaľovať malvér, ktorého cieľom je pripojiť váš počítač k sieti botnet.

Detekcia na úrovni DNA

Typy detekcie sú rôzne, pohybujú sa od veľmi špecifických hashov až po detekcie na úrovni DNA, ktoré sú komplexnými definíciami škodlivého správania a charakteristík malvéru. Zatiaľ čo škodlivý kód môže byť útočníkmi ľahko upravený alebo maskovaný, správanie objektu sa tak jednoducho zmeniť nedá – detekcie na úrovni DNA sú navrhnuté tak, aby práve tento princíp využívali.

Vykonávame hĺbkovú analýzu kódu a extrahujeme tzv. gény zodpovedné za správanie kódu. Na základe týchto behaviorálnych génov vytvárame detekcie na úrovni DNA, ktoré sa používajú na posúdenie potenciálne podozrivého kódu, či už sa nachádza na disku alebo v pamäti prebiehajúceho procesu. Detekcia na úrovni DNA dokáže identifikovať konkrétne známe vzorky malvéru, nové varianty známej rodiny malvéru, ale dokonca aj doposiaľ nezistený alebo neznámy malvér, ktorý obsahuje gény indikujúce škodlivé správanie.

ESET LiveGrid®

ESET LiveGrid® (založený na pokročilom systéme včasného varovania ThreatSense.Net) pracuje s dátami získanými od používateľov bezpečnostných produktov ESET z celého sveta a tieto dáta zasiela do výskumného laboratória spoločnosti ESET. Vďaka prijatým vzorkám podozrivého softvéru a príslušným metadátam nám ESET LiveGrid® umožňuje okamžite reagovať na najnovšie hrozby, ako aj na požiadavky našich zákazníkov.

Z prijatých údajov pracovníci výskumných laboratórií spoločnosti ESET vytvoria čo najpresnejší obraz o pôvode a rozsahu hrozby, vďaka čomu sa dokážeme zamerať na správne ciele. Dáta zo systému ESET LiveGrid® zohrávajú dôležitú úlohu pri určovaní priorít v rámci nášho automatického spracovávania.

Okrem toho obsahuje aj systém reputácie, ktorý pomáha zlepšiť celkovú efektivitu našich antimalvérových riešení. Používateľ môže skontrolovať reputáciu súborov a spustených procesov priamo z používateľského prostredia programu alebo z kontextového menu, cez ktoré je možné získať podrobnejšie informácie zo systému ESET LiveGrid®. Ak je na systéme používateľa kontrolovaný archív alebo spustiteľný súbor, najskôr bude porovnaný voči databáze povolených a blokovaných objektov. Ak sa nachádza na whiteliste, teda na zozname povolených objektov, bude označený príznakom bezpečný a zároveň bude vylúčený z budúcich kontrol. Ak sa súbor nachádza na blackliste, teda na zozname blokovaných súborov, budú vykonané akcie zodpovedajúce typu danej hrozby. Ak sa v databáze nenájde zhoda, súbor bude dôkladne skontrolovaný. Na základe výsledkov kontroly sú súbory zaradené do kategórií ako škodlivé alebo neškodné. Takýto postup výrazne zlepšuje výkon samotnej kontroly. Systém kontroly súborov podľa reputácie umožňuje efektívne odhaliť malvér ešte predtým, ako sú jeho signatúry zaradené do novej aktualizácie detekčného jadra (čo sa deje niekoľkokrát za deň).

Na rozdiel od reputačného systému ESET LiveGrid®, systém spätnej väzby ESET LiveGrid® zozbiera z vášho počítača len tie informácie, ktoré sa týkajú novej hrozby. Môže ísť o vzorku alebo kópiu súboru, v ktorom sa infiltrácia objavila, cestu k danému súboru, názov súboru, informáciu o dátume a čase detekcie, spôsob, akým sa hrozba dostala do vášho počítača, a informáciu o operačnom systéme.

ESET LiveGrid® servery

Naše servery ESET LiveGrid® sa nachádzajú v Bratislave, Viedni a San Diegu, ide však len o servery, ktorých úlohou je reagovať na požiadavky od klientov. Samotné spracovávanie zasielaných vzoriek prebieha v Bratislave.

Zapnutie alebo vypnutie systému ESET LiveGrid® v produktoch ESET

Viac podrobností a názornú ukážku, ako zapnúť alebo vypnúť ESET LiveGrid® v produktoch ESET, nájdete v článku Databázy znalostí spoločnosti ESET.

Exploit Blocker

Exploit Blocker je navrhnutý na ochranu najčastejšie zneužívaných aplikácií, ako napríklad webových prehliadačov, prehliadačov PDF dokumentov, e-mailových klientov a súčastí balíka Microsoft Office, ako aj ochranu pred útokmi ROP. Exploit Blocker je dostupný a predvolene zapnutý vo všetkých produktoch ESET pre Windows určených pre domácnosti, produktoch ESET pre Windows Server a produktoch ESET pre Windows na ochranu koncových zariadení.

Funguje na princípe monitorovania správania procesov a zachytenia podozrivej aktivity, ktorá môže poukázať na exploit.

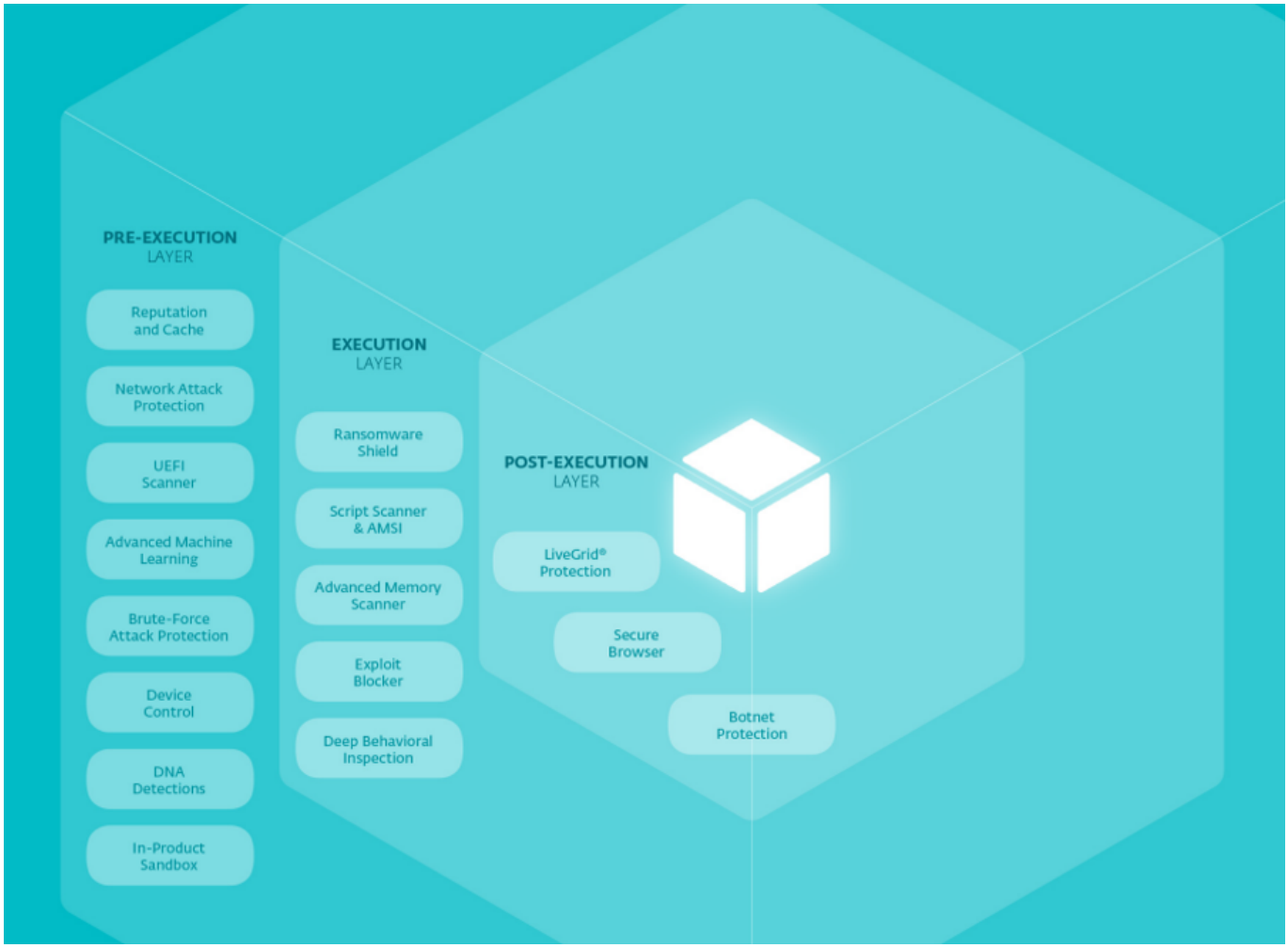
Ak Exploit Blocker identifikuje podozrivý proces, môže ho okamžite zastaviť a zaznamenať dáta o tejto hrozbe. Tieto dáta sú následne odoslané do cloudového systému ESET LiveGrid®. Následne sú spracované výskumným laboratóriom spoločnosti ESET a použité na lepšiu ochranu všetkých používateľov pred neznámymi hrozbami a tzv. zero-day útokmi (ide o nový malvér, pre ktorý zatiaľ nie sú vydané záplaty/opravy).

Java Exploit Blocker

Java Exploit Blocker je rozšírenie k už existujúcej technológii Exploit Blocker. Toto rozšírenie sleduje Javu a hľadá podozrivé správanie. Blokované vzorky môžu byť odoslané analytikom malvéru, ktorí následne vytvárajú signatúry a pomocou nich zabezpečujú blokovanie na rôznych vrstvách (blokovanie URL, sťahované súbory atď.).

ESET LiveSense

ESET LiveSense je kombináciou mnohých jedinečných technológií viacvrstvovej ochrany spoločnosti ESET, ktoré navzájom spolupracujú. Na nasledujúcom obrázku sú znázornené niektoré z kľúčových technológií spoločnosti ESET, ako aj to, kedy a kde približne môžu odhaliť a prípadne zablokovať hrozbu počas jej životného cyklu v systéme.



Strojové učenie

Spoločnosť ESET využíva algoritmy strojového učenia na detekciu a blokovanie hrozieb už od roku 1990. Neurónové siete sme do detekčného jadra našich produktov ESET pridali v roku 1998.

Strojové učenie úzko súvisí tiež s detekciami na úrovni DNA. Tie využívajú modely založené na strojovom učení, aby mohli efektívne pracovať s cloudovým pripojením aj bez neho. Algoritmy strojového učenia rovnako zohrávajú dôležitú úlohu pri počiatočnom triedení a klasifikácii prichádzajúcich vzoriek, ako aj ich umiestňovaní na pomyselnú „mapu kybernetickej bezpečnosti“.

Spoločnosť ESET vyvinula vlastné jadro strojového učenia. Využíva kombinované možnosti neurónových sietí (napríklad hĺbkové učenie a dlhú krátkodobú pamäť – LSTM) a šiestich manuálne vybratých klasifikačných algoritmov. Vďaka tomu dokáže generovať konsolidovaný výstup a pomáha správne označiť prichádzajúce vzorky ako čisté, potenciálne nechcené alebo škodlivé.

Jadro strojového učenia spoločnosti ESET je vyladené tak, aby spolupracovalo s ostatnými ochrannými technológiami, ako sú detekcie na úrovni DNA, sandbox a analýza pamäte, ako aj s extrakciou vzorcov správania, pričom cieľom je ponúknuť čo najvyššiu úspešnosť detekcie a čo najmenší počet falošných poplachov.

Konfigurácia ochrany v Rozšírených nastaveniach produktov ESET

- Produkty ESET pre domácnosti so systémom Windows (od verzie 13.1)
- Produkty ESET pre firemné koncové zariadenia so systémom Windows (od verzie 7.2)

Ochrana pred sieťovými útokmi

Ochrana pred sieťovými útokmi predstavuje rozšírenie firewallu, ktoré vylepšuje detekciu zneužití (tzv. exploitov) známych zraniteľností na úrovni siete. Implementácia detekcie bežných zneužití zraniteľností v rozšírených protokoloch ako SMB, RPC a RDP prináša ďalšiu dôležitú vrstvu ochrany pred malvérom, sieťovými útokmi a zneužitiami zraniteľností, pre ktoré zatiaľ nebola vydaná oprava.

Ransomware Shield

Ransomware Shield je detekčná technika monitorujúca správanie aplikácií a procesov, ktoré sa pokúšajú robiť zmeny v súboroch tak, ako je to typické pri malvéri typu ransomvér/filecoder. Ak správanie aplikácie možno považovať za škodlivé alebo ak kontrola na základe reputácie vyhodnotí aplikáciu ako podozrivú, dôjde k zablokovaniu danej aplikácie a zastaveniu procesu, prípadne môže byť používateľ vyzvaný, aby zvolil akciu blokovania alebo povolenia.

Aby mohla funkcia Ransomware Shield správne fungovať, musí byť systém ESET LiveGrid® povolený. Prečítajte si náš článok Databázy znalostí spoločnosti ESET, ktorý vám pomôže zistiť, či máte ESET LiveGrid® zapnutý a funkčný.

Ochrana proti skriptovým útokom

Ochrana proti skriptovým útokom pozostáva z ochrany pred JavaScriptom vo webových prehliadačoch a z ochrany Antimalware Scan Interface (AMSI) pred skriptami spúšťanými v prostredí PowerShell.

HIPS
Aby táto funkcia mohla fungovať, musí byť povolený systém HIPS.

Ochrana proti skriptovým útokom je podporovaná pre nasledujúce webové prehliadače:

- Mozilla Firefox
- Google Chrome
- Internet Explorer
- Microsoft Edge

Používajte podporovaný webový prehliadač
Minimálne podporované verzie webových prehliadačov sa môžu líšiť, pretože signatúry súborov prehliadačov sa pomerne často menia. Najnovšia verzia webového prehliadača je však podporovaná vždy.

Zabezpečený prehliadač

Zabezpečený prehliadač predstavuje dodatočnú vrstvu ochrany, ktorej cieľom je chrániť vaše citlivé údaje (napríklad online transakcie a finančné údaje) pred zneužitím.

ESET Endpoint Security vo verzii 8 a novších obsahuje zoznam vopred zadefinovaných webových stránok, ktoré spúšťajú zabezpečený prehliadač. Webové stránky môžete pridávať do zoznamu a upravovať v nastaveniach programu. Zabezpečený prehliadač je po inštalácii produktu predvolene vypnutý.

Podrobnejšie informácie o tejto funkcii nájdete v tomto článku Databázy znalostí spoločnosti ESET.

Použitie šifrovanej komunikácie HTTPS je nevyhnutné pre zabezpečené prehliadanie internetu. Na používanie Zabezpečeného prehliadača musí váš webový prehliadač spĺňať minimálne požiadavky popísané nižšie:

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

Na zariadeniach s procesorom ARM sú podporované len prehliadače Firefox a Microsoft Edge.

Otvorte zabezpečený prehliadač ESET v preferovanom webovom prehliadači

Keď otvoríte zabezpečený prehliadač ESET priamo z hlavného okna produktu zo záložky **Nástroje**, otvorí sa vo webovom prehliadači, ktorý ste nastavili ako predvolený. V opačnom prípade pri bežnom spustení preferovaného prehliadača (nie z produktu ESET) budete po prístupe na stránku uvedenú na internom zozname spoločnosti ESET presmerovaný na rovnaký typ webového prehliadača zabezpečený spoločnosťou ESET.

Kontrola UEFI

Kontrola UEFI (Unified Extensible Firmware Interface) je súčasťou systému HIPS (Host-based Intrusion Prevention System), ktorý chráni UEFI na vašom počítači. UEFI predstavuje firmvér, ktorý sa načíta do pamäte na začiatku procesu zavádzania systému pri štarte počítača. Kód je uložený na pamäťovom čipe, ktorý je pripevnený k základnej doske. UEFI môžu útočníci infikovať malvérom, ktorý je odolný aj voči preinštalovaniu a reštartu systému. Takýto malvér nemusia antivírusové programy zachytiť, keďže väčšina z nich túto vrstvu nekontroluje.

Kontrola UEFI je automaticky povolená. Kontrolu môžete spustiť aj manuálne z hlavného okna programu, a to kliknutím na **Kontrola počítača** > **Pokročilé kontroly** > **Vlastná kontrola** a zvolením položky **Zavádzacie sektory/UEFI** za cieľ kontroly.

Ak váš počítač už je napadnutý UEFI malvérom, prečítajte si nasledujúci článok Databázy znalostí spoločnosti ESET:
Čo mám robiť, ak je môj počítač napadnutý UEFI malvérom?

Nastražený súbor (tzv. canary file)

Canary file alebo nastražený súbor je falošný počítačový dokument umiestnený medzi skutočnými dokumentmi s cieľom pomôcť včas odhaliť neoprávnený prístup k údajom, ich kopírovanie alebo modifikáciu.

Zablokovanie (deadlock)

Zablokovanie (deadlock) predstavuje situáciu, keď počítačový proces čaká na uvoľnenie prostriedkov, ktoré sú priradené k inému procesu. V tejto situácii sa žiadny z procesov nespustí, pretože požadované prostriedky zadržiava proces, ktorý tiež čaká na uvoľnenie iných prostriedkov. Je dôležité zabrániť zablokovaniu skôr, ako k nemu vôbec dôjde. Výskyt zablokovania môže odhaliť plánovač prostriedkov, ktorý pomáha operačnému systému sledovať všetky prostriedky pridelené rôznym procesom. Zablokovanie môže nastať, ak sú súčasne splnené tieto štyri podmienky:

- **Zákaz preempcie** – prostriedky môže dobrovoľne uvoľniť len samotný proces, ktorý ich zadržiava, a to po dokončení svojej úlohy.

- **Vzájomné vylúčenie** – špeciálny typ binárneho semafora, ktorý sa používa na riadenie prístupu k zdieľaným prostriedkom. Umožňuje, aby boli aktuálne úlohy s vyššou prioritou blokované čo najkratší čas.

- **Zadržiavanie a čakanie** – v tomto prípade je potrebné zabrániť tomu, aby procesy zadržiavali jedny prostriedky a zároveň čakali na ďalšie.

- **Kruhové čakanie** – určuje celkové usporiadanie všetkých typov prostriedkov. Pri kruhovom čakaní sa takisto vyžaduje, aby každý proces žiadal o prostriedky vo vzostupnom poradí.

Existujú tri spôsoby, ako riešiť zablokovanie:

- Nedovoľte, aby sa systém dostal do zablokovaného stavu.
- Dovoľte, aby došlo k zablokovaniu, a keď sa tak stane, využite preempciu, teda odobratie zadržiavaných prostriedkov.
- Ak dôjde k zablokovaniu, reštartujte systém.