

## ESET Glossary

### Felhasználói útmutató

[Ide kattintva megjelenítheti a dokumentum verzióját](#)

Copyright ©2024 – ESET, spol. s r.o.

Az ESET Glossary terméket az ESET, spol. s r.o. fejlesztette ki

További információkért látogasson el a <https://www.eset.com> oldalra.

Minden jog fenntartva. A szerző írásos engedélye nélkül a jelen dokumentáció egyetlen része sem reprodukálható, nem tárolható adatlekérő rendszerben, illetve nem továbbítható semmilyen formában és semmilyen módon, legyen az elektronikus, mechanikus, fénymásolási, rögzítési, szkennelési vagy más mód.

Az ESET, spol. s r.o. fenntartja magának a jogot, hogy az ismertetett alkalmazásszoftvert előzetes értesítés nélkül megváltoztassa.

Műszaki terméktámogatás: <https://support.eset.com>

REV. 2024.04.12.

<b>1 Bevezetés az ESET-szójegyzékbe</b>	<b>1</b>
<b>1.1 Reklámprogram</b>	<b>1</b>
<b>1.2 Botnet</b>	<b>1</b>
<b>1.3 Téves riasztás</b>	<b>2</b>
<b>1.4 Tömörítő</b>	<b>2</b>
<b>1.5 Veszélyes alkalmazások</b>	<b>2</b>
<b>1.6 Kéretlen alkalmazások</b>	<b>2</b>
<b>1.7 Zsarolóprogram</b>	<b>7</b>
<b>1.8 Rootkit</b>	<b>7</b>
<b>1.9 Visszatérés-orientált programozás</b>	<b>8</b>
<b>1.10 Kémprogramok</b>	<b>8</b>
<b>1.11 Trójai</b>	<b>8</b>
<b>1.12 Vírus</b>	<b>9</b>
<b>1.13 Féreg</b>	<b>9</b>
<b>1.14 Credential stuffing</b>	<b>10</b>
<b>1.15 DNS-mérgezés</b>	<b>10</b>
<b>1.16 Szolgáltatásmegtagadási támadások (DoS, DDoS)</b>	<b>10</b>
<b>1.17 ICMP-protokollon alapuló támadások</b>	<b>10</b>
<b>1.18 Portfigyelés</b>	<b>11</b>
<b>1.19 SMB-továbbítás</b>	<b>11</b>
<b>1.20 TCP-deszinkronizáció</b>	<b>11</b>
<b>1.21 Féregtámadás</b>	<b>12</b>
<b>1.22 ARP-gyorsítótármérgezés</b>	<b>12</b>
<b>2 E-mail útján terjedő kártevők</b>	<b>12</b>
<b>2.1 Reklámok</b>	<b>13</b>
<b>2.2 Megtévesztő üzenetek</b>	<b>13</b>
<b>2.3 Adathalászat</b>	<b>13</b>
<b>2.4 Levélszemét felismerése</b>	<b>14</b>
2.4 Szabályok	14
2.4 Engedélyezőlista	15
2.4 Tiltólista	15
2.4 Kivétel	15
2.4 Szerveroldali ellenőrzés	15
<b>2.5 Speciális memória-ellenőrzés</b>	<b>16</b>
<b>2.6 Netbank- és tranzakcióvédelem</b>	<b>16</b>
<b>2.7 Botnet elleni védelem</b>	<b>17</b>
<b>2.8 DNA-észlelések</b>	<b>17</b>
<b>2.9 ESET LiveGrid®</b>	<b>17</b>
<b>2.10 Exploit blokkoló</b>	<b>18</b>
<b>2.11 Java Exploit blokkoló</b>	<b>18</b>
<b>2.12 ESET LiveSense</b>	<b>18</b>
<b>2.13 Gépi tanulás</b>	<b>19</b>
<b>2.14 Hálózati támadások elleni védelem</b>	<b>20</b>
<b>2.15 Zsarolóprogram elleni védelem</b>	<b>20</b>
<b>2.16 Szekurit-alkapú támadások elleni védelem</b>	<b>20</b>
<b>2.17 Védett böngésző</b>	<b>20</b>
<b>2.18 UEFI Scanner</b>	<b>21</b>
<b>2.19 Kanári fájl</b>	<b>21</b>
<b>2.20 Holtpont</b>	<b>21</b>

# Bevezetés az ESET-szójegyzékbe

Az ESET-szójegyzék részletes áttekintést nyújt az aktuális kártevőkről és azokról az ESET-technológiákról, amelyek védelmet nyújtanak ellenük.

A különböző témakörök a következő fejezetekben kapnak helyet:

- [Kártevők](#) – Számítógépes vírus, féreg, trójai, kéretlen alkalmazás stb.
- [Távoli támadások](#) – Helyi hálózatokon és az interneten végrehajtott támadások
- [E-mail útján terjedő kártevők](#) – Megtévesztő üzenetek, adathalászat, csalások stb.
- [ESET-technológiák](#) – Az ESET biztonsági megoldásaiban megtalálható termékfunkciók

## Reklámprogram

A reklámprogramok a hirdetések terjesztésére szolgáló szoftverek. Ebbe a kategóriába a reklámanyagokat megjelenítő programok tartoznak. A reklámprogramok gyakran automatikusan megnyitnak egy reklámot tartalmazó előugró ablakot a böngészőben, vagy módosítják a kezdőlapot. Gyakran szabadszoftverekkel („freeware” programokkal) vannak egybe csomagolva, mert ezek fejlesztői így próbálják meg csökkenteni az (általában hasznos) alkalmazásaik költségeit.

A reklámprogram önmagában nem veszélyes, de a hirdetések zavarhatják a felhasználókat. A veszélyt az jelenti, hogy az ilyen programok (a kémprogramokhoz hasonlóan) nyomkövetést is végezhetnek.

Ha freeware szoftver használata mellett dönt, szenteljen különleges figyelmet a telepítőprogramnak. A legtöbb telepítő valószínűleg értesítést küld a reklámprogramok telepítéséről. Gyakran lehetőség van a szoftver reklámprogram nélküli telepítésére.

Egyes szoftverek nem telepíthetők reklámprogram nélkül, vagy csak korlátozottan használhatók. Ez azt jelenti, hogy a reklámprogram gyakran „legálisan” tud hozzáférni a rendszerhez, mert a felhasználó engedélyt adott neki erre. Részesítse azonban előnyben a biztonságot, hiszen jobb félni, mint megijedni. Ha a számítógépen található valamelyik fájlról kiderül, hogy reklámprogram, ajánlatos törölni, mivel nagy valószínűséggel kártékony kódot tartalmaz.

## Botnet

A botok vagy webes robotok olyan automatizált kártékony programok, amelyek hálózati blokkokat ellenőriznek, és megtámadják a biztonsági résekkel rendelkező számítógépeket. Ez lehetővé teszi a hackereknek, hogy egyszerre számos számítógép felett átvegyék az irányítást, és botokká (más néven zombikká) alakítsák őket. A hackerek általában botok segítségével fertőznek meg sok számítógépet, amelyek egy hálózatot vagy botnetet alkotnak. Ha a botnet jelen van a számítógépen, felhasználható terjesztett szolgáltatásmegtagadásos (DDoS) támadásokban, proxykban, valamint a segítségével automatizált feladatok is végrehajthatók az Ön tudta nélkül az interneten keresztül (például levélszemét vagy vírus küldhető, illetve eltulajdoníthatók személyes és bizalmas adatok, többek között banki hitelesítő adatok vagy hitelkártyaszámok).

# Téves riasztás

A valóságban nincs garancia a 100%-os észlelési arányra, illetve nincs 0%-os esélye a tiszta objektumok kártevőként való téves kategorizálásának.

A téves riasztás egy olyan tiszta fájl/alkalmazás, amely tévesen kártevőnek vagy kóros alkalmazásnak lett osztályozva.

# Tömörítő

A tömörítők futásidejű önkicsomagoló végrehajtható fájlok, amelyek egyetlen csomagba tömörítenek számos kártevőtípust.

A leggyakoribb tömörítők a UPX, a PE\_Compact, a PKLite és az ASPack. Ugyanaz a kártevő eltérően is észlelhető, ha másik tömörítővel van tömörítve. A tömörítők képesek „aláírásaikat” megváltoztatni, így nehezebb felismerni és eltávolítani a kártevőt.

# Veszélyes alkalmazások

Számtalan törvényesen használható alkalmazás van, amely leegyszerűsíti a hálózati számítógépek felügyeletét. Nem megfelelő kezekben azonban kártékony célokra is használhatók. Az ESET az ilyen alkalmazások felismerésére nyújt megoldást.

A **veszélyes alkalmazások** csoportjába a kereskedelembe kapható, törvényes szoftverek tartoznak, többek között a távoli hozzáférést biztosító eszközök, a jelszófeltörő alkalmazások, valamint a billentyűzetfigyelők (a felhasználó minden billentyűleütését rögzítő programok).

Ha észreveszi, hogy egy veszélyes alkalmazás van jelen a számítógépen és fut (de nem Ön telepítette), kérjen tanácsot a hálózati rendszergazdától, vagy távolítsa el az alkalmazást.

# Kéretlen alkalmazások

A „grayware” vagy kéretlen alkalmazás (PUA) kategória számos különböző szoftvert foglal magában. Az ilyen szoftverek nem annyira kártékonyak, mint a többi kártevő, például a vírusok és a trójaiak. További nemkívánatos szoftvereket telepíthetnek azonban, megváltoztathatják a digitális készülék viselkedését, illetve olyan tevékenységeket végezhetnek, amelyeket a felhasználó nem hagyott jóvá, vagy nem várt.

A grayware közé a következő kategóriák tartoznak: hirdetést megjelenítő szoftverek, letöltési burkolók, különféle böngészőeszköztárak, megtévesztő viselkedésű szoftverek, egybecsomagolt és nyomkövető programok, proxytelepítő programok (internetmegosztó alkalmazások), kriptobányászók, beállításjegyzék-tisztítók (csak Windows operációs rendszerek esetén), illetve minden olyan szoftver, amely tiltott vagy legalábbis etikátlan eljárásokat alkalmaz (annak ellenére, hogy jogszerűnek tűnik), és amelyet elutasítana az a végfelhasználó, akinek a tudomására jutna, hogy mi a szoftver rendeltetése.

A [veszélyes alkalmazás](#) jogszerű (akár kereskedelmi) szoftver, de a támadók visszaélhetnek vele. Az ilyen típusú alkalmazások észlelését az ESET szoftverek felhasználói aktiválni tudják, illetve le tudják tiltani.

Bizonyos esetekben a felhasználók úgy vélhetik, hogy a kéretlen alkalmazásoknak nagyobbak az előnyei, mint a

kockázatai. Emiatt az ESET az ilyen alkalmazásokat alacsony kockázatú kategóriába sorolja a kártevő szoftverek egyéb típusaival (például trójaiakkal vagy férgekkel) szemben.

- [Figyelem – A program kéréstlen alkalmazást talált](#)
- [Beállítások](#)
- [Szoftvercsomagolók](#)
- [Beállításjegyzék-tisztítók](#)
- [Nemkívánatos tartalom](#)

### Ábrákkal ellátott útmutató



A kéréstlen alkalmazások ESET Windows otthoni termékekben való ellenőrzéséhez és eltávolításához olvassa el az [ESET tudásbáziscikkét](#).

## Figyelem – A program kéréstlen alkalmazást talált

Ha a víruskereső kéréstlen alkalmazást észlelt, eldöntheti, hogy milyen műveletet végezzen el:

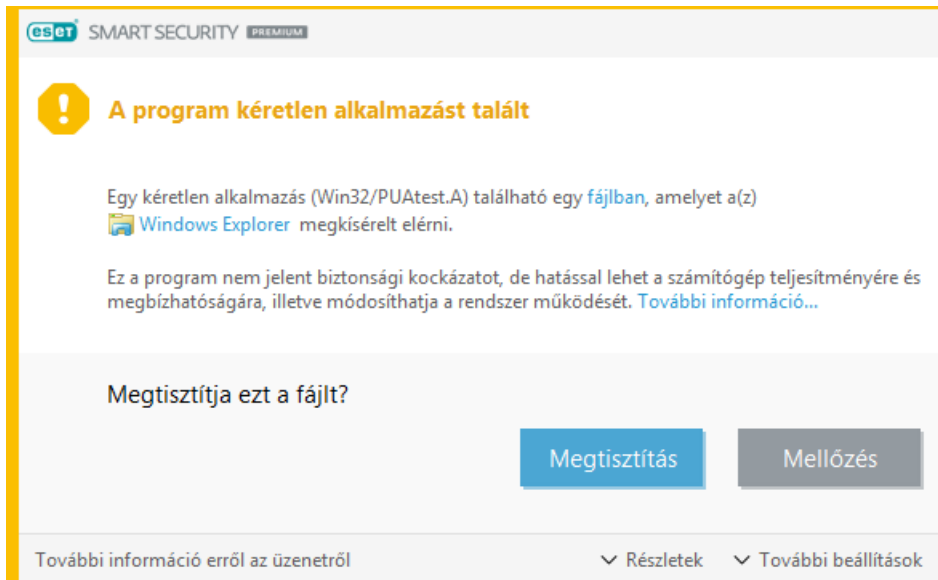
**1.Megtisztítás/Leválasztás:** Ez a beállítás megszakítja a műveletet, és megakadályozza, hogy a kéréstlen alkalmazás bejusson a rendszerbe.

Webhelyről való letöltés során a **Kapcsolat bontása** lehetőség fog rendelkezésre állni a kéréstlen alkalmazásokról szóló értesítések esetén, lemezen található fájl esetén pedig a **Megtisztítás** lehetőség.

**2.Mellőzés:** Ha ezt a beállítást választja, a kéréstlen alkalmazások bejuthatnak a rendszerbe.

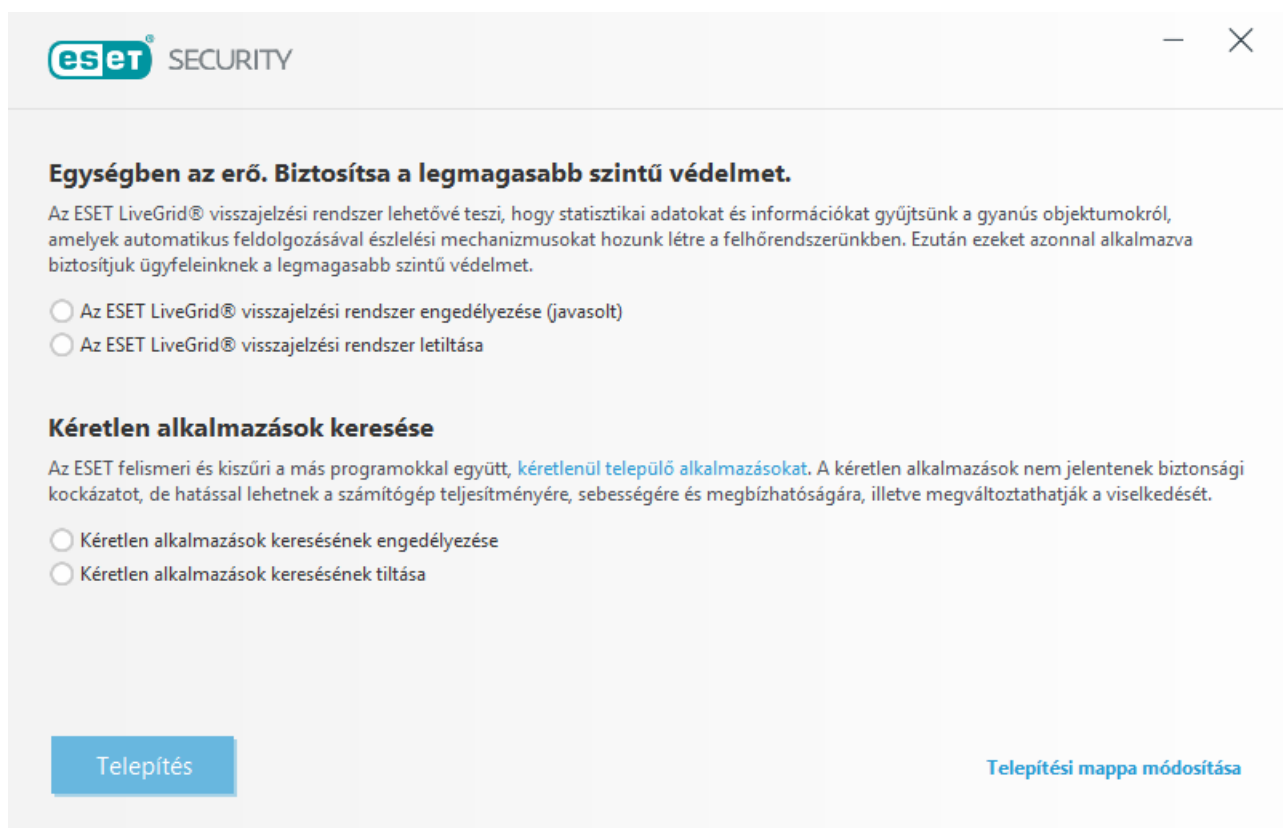
**3.Felvétel a kivételek közé:** Ha szeretné engedélyezni, hogy az észlelt fájl a jövőben megszakítás nélkül fusson a számítógépén, kattintson a **További beállítások** elemre, jelölje be a Felvétel a kivételek közé jelölőnégyzetet, majd kattintson a **Mellőzés** elemre.

**4.Vírusdefiníciók kizárása az észlelésből:** Ha engedélyezni szeretné, hogy egy adott észlelési név (vírusdefiníció) által észlelt összes fájl megszakítás nélkül futhasson a számítógépén a jövőben (meglévő fájlok vagy webes letöltések), kattintson a **További beállítások** elemre, jelölje be a **Vírusdefiníciók kizárása az észlelésből** jelölőnégyzetet, majd kattintson a **Mellőzés** elemre. Ha azonnal megjelennek további észlelési ablakok azonos észlelési névvel, a Mellőzés elemre kattintva zárja be őket (az esetleges további ablakok olyan észlelésre vonatkoznak, amelyek azelőtt kerültek sorra, hogy kizárta volna a vírusdefiníciót az észlelésből).



## Beállítások

ESET-szoftvere telepítésekor eldöntheti, hogy az alább látható módon engedélyezi-e a kényszerű alkalmazások keresését:



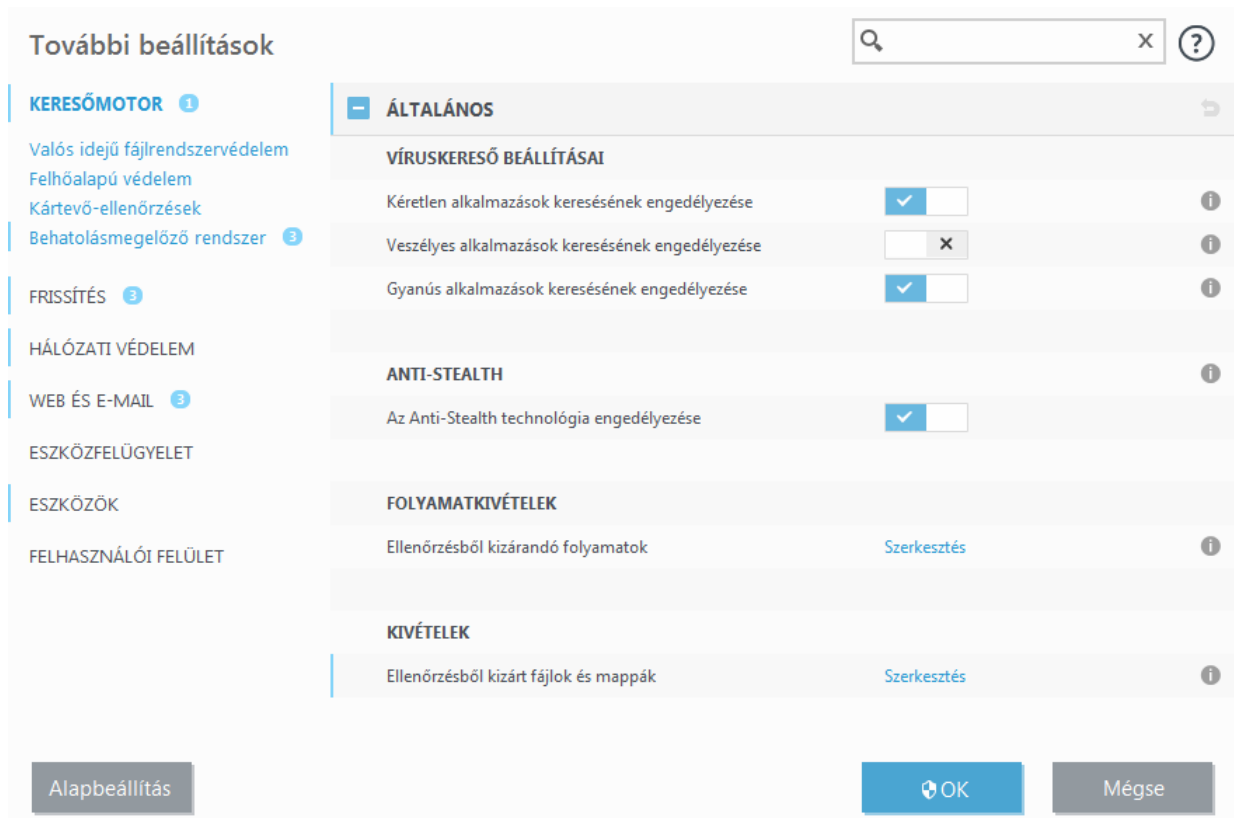
### Figyelmeztetés



A kényszerű alkalmazások reklámprogramokat és eszköztárakat telepíthetnek, illetve más kényszerű vagy veszélyes funkciókat tartalmazhatnak.

Ezek a beállítások bármikor módosíthatók a program beállításai között. Ha szeretné engedélyezni vagy letiltani a kényszerű, veszélyes vagy gyanús alkalmazásokat, kövesse az alábbi utasításokat:

1. [Nyissa meg az ESET-terméket.](#)
2. Nyomja le az **F5** billentyűt a **További beállítások** párbeszédpanel megnyitásához.
3. Kattintson a **Keresőmotor** elemre (korábbi verziókban **Vírusirtó** vagy **Számítógép**), és az igényeinek megfelelően engedélyezze vagy tiltsa le a **Kéretlen alkalmazások keresésének engedélyezése**, a **Veszélyes alkalmazások keresésének engedélyezése** és a **Gyanús alkalmazások keresésének engedélyezése** funkciót. Az **OK** gombra kattintva hagyja jóvá a műveletet.



### Ábrákkal ellátott útmutató

A ESET tudásbáziscikkeiből részletesen tájékozódhat arról, hogy hogyan konfigurálhatók a termékek úgy, hogy észleljék vagy mellőzzék a kéretlen alkalmazásokat:

- ✓ [ESET NOD32 Antivirus / ESET Internet Security / ESET Smart Security Premium](#)
- [ESET Cyber Security a macOS rendszerre/ESET Cyber Security Pro a macOS rendszerre](#)
- [ESET Endpoint Security / ESET Endpoint Antivirus for Windows](#)
- [ESET Mobile Security az Android rendszerre](#)

## Szoftvercsomagolók

A szoftvercsomagolók olyan speciális típusú alkalmazásmódosítások, amelyeket bizonyos fájlátoló webhelyek használnak. A csomagolók harmadik felek olyan eszközei, amelyek telepítik az Ön által letölteni kívánt programot, de további szoftvereket, többek között eszköztárakat vagy [reklámprogramokat](#) adnak hozzá. A további szoftverek szintén módosíthatják webböngészője kezdőlapját és a keresési beállításokat. A fájlátoló webhelyek gyakran nem értesítik a szoftver gyártóját vagy a letöltés címzettjét, hogy módosítások történtek, és gyakran elrejtik a módosítások elutasítására szolgáló beállításokat. Emiatt az ESET a szoftvercsomagolókat a kéretlen alkalmazások egyik típusaként sorolja be, hogy lehetővé tegye a felhasználóknak a letöltés fogadását vagy elutasítását.

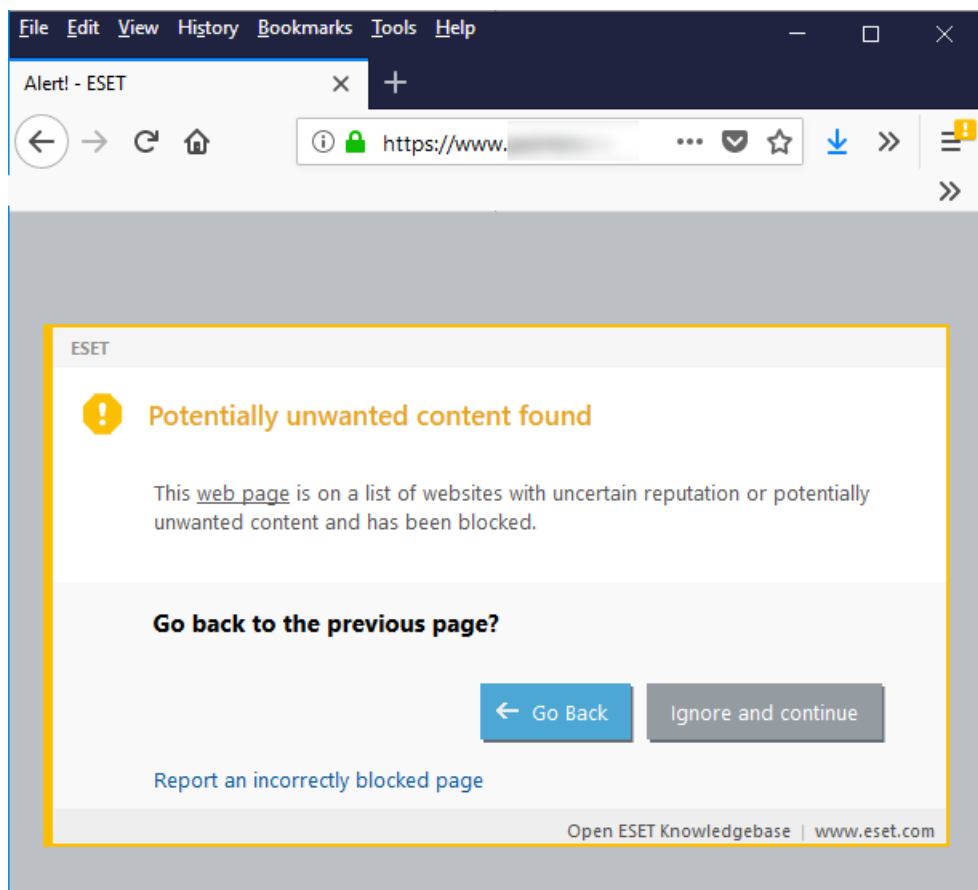


## Beállításjegyzék-tisztítók

A beállításjegyzék-tisztítók olyan programok, amelyek sokszor arra figyelmeztetnek, hogy a Windows beállításjegyzéke rendszeres karbantartást és tisztítást igényel. Beállításjegyzék-tisztító használata esetén kockázatoknak teheti ki számítógépes rendszerét. Ezenkívül néhány beállításjegyzék-tisztító szakszerűtlen, ellenőrizhetetlen vagy egyéb módon védhetetlen állításokat fogalmaz meg a program előnyeiről, illetve félrevezető jelentéseket generál a számítógépes rendszerről az „ingyenes ellenőrzés” eredményeire hivatkozva. Az ilyen félrevezető állítások és jelentések célja az, hogy Ön megvásárolja a teljes értékű verziót vagy előfizetést, és általában nincs lehetőség a beállításjegyzék-tisztító kipróbálására a fizetés előtt. Ezért az ESET kéri a kéréstlen alkalmazásoknak minősíti az ilyen programokat, és lehetőséget ad a felhasználónak az engedélyezésükre és a letiltásukra.

## Nemkívánatos tartalom

Ha a kéréstlen alkalmazások észlelése engedélyezve van az ESET-termékben, akkor nemkívánatos tartalomként letiltja az olyan webhelyeket, amelyek a kéréstlen alkalmazások reklámozásáról ismertek, illetve köztudottan olyan műveletek végrehajtására veszik rá a felhasználókat, amelyek negatív befolyást gyakorolhatnak a rendszerükre vagy a böngészési élményre. Ha arról kap értesítést, hogy a meglátogatni kívánt webhely nemkívánatos tartalomként van kategorizálva, a **Vissza** gombra kattintva elkerülheti a letiltott weboldalt, illetve a **Mellőzés és folytatás** gombra kattintva engedélyezheti a webhely beöltését.



Erről a témakörrel [ebben az ESET-tudásbáziscikkben](#) olvashat bővebben.

# Zsarolóprogramok

A zsarolóprogramok (más néven „filecoder”) olyan kártevők, amelyek zárolják az eszközöket, illetve titkosítják az eszközökön található tartalmakat, és pénzt követelnek a felhasználóktól azért, hogy ismét lehetővé tegyék a tartalmakhoz való hozzáférést. Az ilyen típusú kártevők sokszor beépített időzítővel rendelkeznek, amelyen be van programozva a fizetési határidő. Ha a felhasználó nem tartja a határidőt, növekszik az ár, vagy az eszköz végleg használhatatlanná válik.

Amikor megfertőzik az eszközöket, megkísérik titkosítani a megosztott meghajtókat az eszközökön. Ez a folyamat azt a látszatot keltheti, hogy a kártevő a hálózaton keresztül terjed, de valójában nincs erről szó. Akkor áll elő ez a helyzet, ha a fájlserveren titkosítják a megosztott meghajtót, viszont maga a szerver nem tartalmaz kártevőt (hacsak nem terminálszerver).

A zsarolóprogramok létrehozói két kulcsot hoznak létre – egy nyilvánosat és egy privátot –, majd a nyilvánosat elhelyezik a kártevőben. Maga a zsarolóprogram sokszor egy trójai részét képezi, vagy olyan fájlnak vagy képnek van álcázva, amelyet e-mailben, közösségi hálózatokon, illetve azonnali üzenetküldő alkalmazásokban szoktak kapni a felhasználók. Miután beszivárognak a számítógépre, a kártevők generálnak egy véletlenszerű, szimmetrikus kulcsot, és titkosítják az eszközön tárolt adatokat. A kártevőben található nyilvános kulcs segítségével titkosítják a szimmetrikus kulcsot. A zsarolóprogramok ezután pénzt követelnek az adatok visszafejtéséért. Az eszközön megjelenő fizetésre felszólító üzenet egy hamis figyelmeztetés lehet, amely szerint a felhasználó rendszerét illegális tevékenységekre használták, vagy a rendszeren illegális tartalmak találhatók. A zsarolóprogramok különböző fizetési módokat kínálnak a fizetésre. Ezek általában olyanok, amelyeket nehéz nyomon követni – ilyenek például a digitális (kripto-) valuták, emelt díjas SMS-üzenetek, illetve az előre kifizetett utalványok. Az összeg beérkezése után a zsarolóprogramok létrehozóinak fel kell oldaniuk a készüléket, illetve a privát kulccsal vissza kell fejteniük a szimmetrikus kulcsot, majd visszafejtik a felhasználói adatokat. Ez a művelet azonban nem garantált.

## További információk a zsarolóprogramok elleni védelemről



Az ESET-termékek többretegű technológiákat alkalmaznak, amelyek megvédik az eszközöket a zsarolóprogramoktól. Tekintse meg az [ESET tudásbáziscikkét](#), amely bemutatja azokat a bevált gyakorlatokat, amelyekkel megvédhető a rendszer a zsarolóprogramoktól.

# Rootkit

A rootkitek olyan kártékony programok, amelyek a támadónak hozzáférést biztosítanak a rendszerhez, miközben jelenlétüket elrejtik. Miután bejutnak a rendszerbe (általában annak biztonsági részét kihasználva), a rootkitek az operációs rendszer funkcióinak használatával igyekeznek észrevétlenek maradni a vírusvédelmi szoftverek előtt: folyamatokat, fájlokat és Windows-beállításértékeket (rendszerleíró adatbázisbeli adatokat) rejtenek el. Emiatt a szokványos vizsgálati technikákkal szinte lehetetlen felderíteni őket.

Kétféle felismerési szinten kerülhető el a rootkitek okozta fertőzés:

1. Az első szint az, amikor ezek a szoftverek megpróbálnak bejutni a rendszerbe. Még nincsenek jelen, ezért inaktívak. A legtöbb vírusvédelmi rendszer ezen a szinten képes elhárítani a rootkitekét (feltéve, hogy egyáltalán felismeri fertőzőtként az ilyen fájlokat).
2. Amikor a szokásos ellenőrzés elől elrejtőznek: az ESET felhasználói élvezhetik az aktív rootkitek észlelésére és elhárítására képes Anti-Stealth technológia előnyeit.

# Visszatérés-orientált programozás

A visszatérés-orientált programozás (Return-oriented programming – ROP) egy tipikus kód-újrafelhasználási támadás, ahol a támadó rosszindulatú céllal irányítja a vezérlési áramlást a meglévő kódon keresztül. A ROP-támadás a veremromboló támadások egy fejlett változata. Verem-puffertúlcsondolás akkor lép fel, amikor egy program a hívásveremén lévő egyik memóriacímre ír a tervezett adatstruktúrán kívül, általában rögzített hosszúságú pufferrel.

A ROP egy olyan kiaknázási technika, amely lehetővé teszi a kódvégrehajtatást a célrendszeren. A hívásverem irányításának megszerzésével a támadó vezérelni tudja a számítógépen futó megbízható szoftverek áramlását, és ezt manipulálva nem szándékolt feladatot hajt végre.

## Kémprogramok

Ebbe a kategóriába tartozik az összes olyan alkalmazás, amely magánjellegű információkat továbbít a felhasználó tudta vagy hozzájárulása nélkül. A kémprogramok nyomkövető funkciókat használva különféle statisztikai adatokat küldhetnek, például a felkeresett webhelyek listáját, a felhasználó névjegyalbumában lévő e-mail címeket vagy a leütött billentyűk listáját.

A kémprogramok szerzői azt állítják, hogy ezek az eljárások a felhasználók igényeinek és érdeklődési körének feltérképezésére, így hatékonyabban célzott reklámok létrehozására szolgálnak. A probléma azonban az, hogy nincs világos határvonal a hasznos és a kártékony alkalmazások között, és senki sem lehet biztos abban, hogy az összegyűjtött információkkal nem élnek-e vissza. A kémprogramokkal megszerzett adatok lehetnek biztonsági kódok, PIN kódok, bankszámlaszámok és így tovább. A kémprogramokat szerzőik gyakran ingyenes programverziókkal csomagolják egybe, hogy jövedelemre tegyenek szert, vagy szoftverük megvásárlására csábítsanak. Gyakran előfordul, hogy egy program a telepítéskor tájékoztatja a felhasználót a kémprogram jelenlétéről, amivel arra igyekszik rávenni őt, hogy frissítsen a szoftver kémprogrammentes verziójára.

Az egyenrangú (P2P) hálózatok kliensalkalmazásai például olyan ingyenes („freeware”) termékek, amelyekről köztudott, hogy kémprogrammal egybecsomagolva jelennek meg. A Spyfalcon vagy a Spy Sheriff (és sok más) szoftver külön alkategóriába tartozik – ezek kémprogramvédelmi alkalmazásoknak tüntetik fel magukat, ám valójában maguk is kémprogramok.

Ha a számítógép valamelyik fájljáról kiderül, hogy kémprogram, ajánlatos törölni, mivel nagy valószínűséggel kártékony kódot tartalmaz.

A kémprogramok alkategóriájának számító keyloggerek hardver vagy szoftver alapúak lehetnek. A szoftveralapú keyloggerek csak egyetlen webhelyre vagy alkalmazásba beírt információkat tudnak begyűjteni. A kifinomultabb keyloggerek mindent rögzíteni tudnak, amit a felhasználó begépel, beleértve az átmásolt/beillesztett információkat is. A mobil eszközöket célzó keyloggerek némelyike ezenkívül rögzíteni tudnak hívásokat, információkat az üzenetküldő alkalmazásokból, helyeket vagy akár mikrofon- és kamerafelvételeket is.

## Trójai

Előzményeiket tekintve a számítógépes trójaiak (trójai falovak) olyan kártékony kódok, amelyek hasznos programként tüntetik fel magukat, és csalárd módon ráveszik a felhasználót a futtatásukra.

Tág fogalomról lévén szó, gyakran különböző alkategóriákra osztják őket.

- Letöltő – Olyan kártékony program, amely le tud tölteni más kártevőket az internetről.
- Vírushordozó – Olyan kártékony program, amelynek az a rendeltetése, hogy más típusú kártevő szoftvereket telepítsen a fertőzött számítógépekre.
- Hátsó kapu – Olyan kártékony program, amely távoli támadókkal kommunikál, lehetővé téve számukra a számítógépbe való behatolást és a számítógép irányításának átvételét.
- Billentyűzetfigyelő (gépelésfigyelő) – Olyan program, amely rögzíti, hogy a felhasználó milyen billentyűket üt le, és elküldi ezt az információt a távoli támadóknak.
- Tárcsázó – Olyan kártékony program, amely a felhasználó internetszolgáltatója helyett emelt díjas telefonszámokat hív fel. Szinte lehetetlen észrevenni, amikor egy ilyen program új kapcsolatot létesít. A tárcsázók csak faxmodemek révén tudnak kárt okozni, ezek azonban már egyre ritkábbak.

Ha a számítógép valamelyik fájljáról kiderül, hogy trójai, ajánlatos törölni, mivel nagy valószínűséggel kártevő kódot tartalmaz.

## Vírus

A számítógépes vírusok a számítógépen lévő fájlok elé helyezett vagy mögé fűzött kártékony kódok. A vírusok a biológiai vírusokról kapták a nevüket, mert hozzájuk hasonló technikával terjednek egyik helyről a másikra. A „vírus” kifejezést gyakran helytelenül használják a fenyegetések valamelyik fajtájának a megnevezésére. Használatát azonban fokozatosan egy pontosabb elnevezés, a „kártevő” (angolul malware – malicious software, vagyis kártékony szoftver) kezdi kiszorítani.

Elsősorban végrehajtható fájlokat és dokumentumokat támadnak meg. A vírusok működése dióhéjban a következő: a fertőzött fájl végrehajtása után a program meghívja a kártékony kódot, és az eredeti alkalmazás előtt végrehajtja azt. A vírusok bármilyen fájl képesek megfertőzni, amelyhez az aktuális felhasználónak írási jogosultsága van.

A számítógépes vírusok céljukat és súlyosságukat tekintve igen változatosak. Némelyikük rendkívül veszélyes, mert képes szándékosan fájlokat törölni a merevlemezről. Ugyanakkor vannak vírusok, amelyek nem okoznak valódi károkat, és egyetlen céljuk, hogy bosszantsák a felhasználót, vagy fitogtassák szerzőjük műszaki jártasságát.

Ha számítógépét megfertőzte egy vírus, és a megtisztítás nem lehetséges, küldje el a fájlt elemzésre az ESET víruslaborjába. Egyes esetekben előfordulhat, hogy a fertőzött fájlok olyan mértékben módosulnak, hogy nem lehetséges a megtisztításuk, és le kell cserélni őket egy nem fertőzött példányra.

## Féreg

A számítógépes féreg olyan kártékony kódot tartalmazó program, amely hálózatra kötött számítógépeket támad meg, és a hálózaton önmagától terjed. A vírusok és a férgek között az az alapvető különbség, hogy a férgek önállóan képesek terjedni – ehhez nincs szükségük gazdafájlokra (vagy rendszertöltő szektorokra). A férgek a névjegylista e-mail címein keresztül terjednek, illetve a hálózati alkalmazások biztonsági réseit használják ki.

A férgek tehát sokkal életképesebbek, mint a vírusok. Az internet széles körű hozzáférhetősége miatt kibocsátásuk után már néhány órán – esetenként néhány percen – belül a világon bárhol felbukkanhatnak. Az önálló és gyors replikációra való képességük más kártevő szoftvereknél lényegesen veszélyesebbé teszi őket.

A rendszerben aktiválódott féreg számos kellemetlenséget okozhat: fájlokat törölhet, ronthatja a rendszer

teljesítményét, sőt akár kikapcsolhat egyes programokat. A férgek természetéből adódóan alkalmasak más típusú kártékony kódok szállítására.

Ha a számítógép féreggel fertőződik meg, ajánlatos törölni a fertőzött fájlokat, mivel azok nagy valószínűséggel kártékony kódot tartalmaznak.

## Credential stuffing

A Credential stuffing egy olyan számítógépes támadás, amelynek során kiszivárgott hitelesítő adatokat tartalmazó adatbázisból származó adatokat használnak fel. A támadók botok és más automatizálási módszerek segítségével jelentkeznek be fiókokba számos webhelyen a kiszivárgott adatok felhasználásával. A támadók azokat a felhasználókat használják ki, akik több webhelyen és szolgáltatásban használják ugyanazokat a bejelentkezési adatokat. Ha a támadás sikeres, a támadók teljes hozzáférést tudnak szerezni a fiókhoz és a fiókban tárolt felhasználói adatokhoz. A támadók így személyes adatokat tudnak ellopni, csalárd tranzakciókat hajtanak végre, levélszemetet terjesztenek, vagy más rosszindulatú tevékenységeket végeznek.

## DNS-mérgezés

A DNS (tartománynévszerver) mérgezésével a hackerek becsaphatják a számítógép által használt DNS-szervert, hogy az általuk küldött hamis adatokat szabályszerűnek és hitelesnek fogadja el. A hamis adatok egy ideig a gyorsítótárban találhatók, lehetővé téve, hogy a támadók átírják például a DNS-szerver IP-címek formájában küldött válaszait. Ennek következményeként a webhelyekhez hozzáférni kívánó felhasználók az eredeti tartalom helyett vírusokat és férgeket fognak letölteni.

## Szolgáltatásmegtagadási támadások (DoS, DDoS)

A szolgáltatásmegtagadás olyan támadás, amely megkísérli a számítógépet vagy a hálózatot elérhetetlenné tenni a felhasználók számára. Előfordulhat, hogy az érintett felhasználók közötti kommunikáció megszakad, és később sem működik normálisan. A szolgáltatásmegtagadási támadásnak kitett számítógépeket általában újra kell indítani, mert egyébként nem működnek megfelelően.

A támadás célpontja a legtöbb esetben egy webszerver, a célja pedig, hogy bizonyos időre elérhetetlenné tegye azt a felhasználóknak.

## ICMP-protokollon alapuló támadások

Az ICMP (Internet Control Message Protocol) egy elterjedt és széles körben alkalmazott internetes protokoll. Legfőképpen hálózati számítógépek használják különféle hibaüzenetek küldésére.

Távoli támadók megkísérlik kihasználni az ICMP protokoll sebezhetőségét. Az ICMP protokoll a hitelesítést nem igénylő egyirányú kommunikációhoz használható. Hibáit kihasználva úgynevezett szolgáltatásmegtagadási (DoS, Denial of Service) támadás idézhető elő. Elképzelhető olyan támadás is, amely jogosulatlan személyeknek biztosíthat hozzáférést a számítógép bejövő és kimenő adatcsomagjaihoz.

Az ICMP-alapú támadások tipikus példái a pingelárasztás, az ICMP\_ECHO-elárasztás és a smurf-támadások. Az ICMP-alapú támadásnak kitett gépek (főleg az interneten kommunikáló alkalmazások) lényegesen lassabban működnek, és az internetkapcsolat létrehozásakor különböző hibákat érzékelnek.

# Portfigyelés

A portfigyeléssel megállapítható, hogy mely portok nyitottak egy hálózatba kötött számítógépen. A portfigyelő olyan szoftver, amelyet ilyen portok felderítésére terveztek.

A számítógép portjai a kimenő és a bejövő adatokat kezelő virtuális pontok, így biztonsági szempontból kulcsfontosságúak. Nagyméretű hálózatokon a portfigyelők által gyűjtött információk segítséget nyújthatnak a lehetséges biztonsági rések felderítéséhez. A portfigyelők ilyen célú használata törvényes.

A portfigyelést azonban a biztonság megsértésével kísérletező hackerek is alkalmazzák. Első lépésként adatcsomagokat küldenek mindegyik portra. A visszaérkező válaszok típusától függően megállapíthatják, hogy mely portok vannak használatban. Maga a figyelés nem okoz károkat, de jó tudni, hogy az ilyesfajta tevékenység felfedheti az esetleges biztonsági réseket, és lehetővé teszi, hogy a támadók átvegyék az irányítást a távoli számítógépek felett.

A hálózati rendszergazdáknak tanácsos a használaton kívüli portokat letiltani, a használatban lévőket pedig védeni a jogosulatlan hozzáférés ellen.

## SMB-továbbítás

Az SMB Relay és az SMB Relay2 olyan speciális programok, amelyek képesek távoli számítógépek megtámadására. Ehhez a Server Message Block fájlmegosztási protokollt használják, amely réteg a NetBIOS felett helyezkedik el. A helyi hálózaton keresztül mappát vagy könyvtárt megosztó felhasználók nagy valószínűséggel ezt a fájlmegosztási protokollt használják.

A helyi hálózaton zajló kommunikációban jelszókivonatokat is továbbítódnak oda-vissza.

Az SMB Relay egy kapcsolatot fogad a 139-es és a 445-ös UDP-porton, továbbítja a kliens és a szerver között váltott csomagokat, és módosítja azokat. A csatlakozás és a hitelesítés után a kliens kapcsolata megszakad. Az SMB Relay egy új virtuális IP-címet hoz létre. Az új cím a „net use \\192.168.1.1” paranccsal érhető el, majd a Windows bármely hálózati szolgáltatásával használható. Az SMB Relay az egyeztetés és a hitelesítés kivételével továbbítja az SMB protokollon folytatott kommunikációt. A távoli támadók mindaddig használhatják az IP-címet, amíg a a kliensszámítógéppel fennáll a kapcsolat.

Az SMB Relay2 ugyanazon az elven működik, mint az SMB Relay, csak IP-címek helyett NetBIOS-neveket használ. Mindkét program képes a betolakodó illetéktelen személyek általi támadások kivitelezésére. Ez azt jelenti, hogy távoli támadók észrevétlenül elolvashatják és módosíthatják azokat az üzeneteket, amelyeket két kommunikációs végpont között váltanak, illetve üzeneteket szűrhetnek be a kommunikációs folyamatba. Az ilyen jellegű támadásoknak kitett számítógépek gyakran lefagyhatnak, vagy váratlanul újraindulhatnak.

A támadások elkerülése érdekében azt javasoljuk, hogy alkalmazzon hitelesítő jelszavakat vagy kulcsokat.

## TCP-deszinkronizáció

A TCP-deszinkronizáció a TCP-eltérítéssel támadásokban alkalmazott eljárás. Ezt egy folyamat váltja ki, amelyben a bejövő adatcsomagok sorozatszáma eltér a várttól. A váratlan sorozatszámú csomagokat a rendszer elveti (vagy pufferbe menti, ha az aktuális kommunikációs ablakban találhatók).

A deszinkronizációban mindkét kommunikációs végpont elveti a fogadott csomagokat. Ezen a ponton a távoli

támadók behatolhatnak a rendszerbe, és helyes sorozatszámú csomagokat juttathatnak be. A támadók befolyásolhatják vagy akár módosíthatják is a kommunikációt.

A TCP-eltérítéssel támadások célja, hogy megszakítsák a szerver és a kliens, illetve az egyenrangú társgépek kommunikációját. Sok támadás elkerülhető azzal, ha minden TCP-szegmens hitelesítést alkalmaznak. Szintén tanácsos a hálózati eszközöket az ajánlott konfigurációval használni.

## Féregtámadás

A számítógépes féreg olyan kártékony kódot tartalmazó program, amely hálózatba kötött számítógépeket támad meg, és a hálózaton önmagától terjed. A hálózati férgek különböző alkalmazások biztonsági réseit aknázzák ki. Az internet elterjedtsége miatt kibocsátásuk után már néhány órán

A legtöbb féregtámadás (például a Sasser vagy az SqlSlammer) kivédhető a tűzfal alapértelmezett biztonsági beállításainak alkalmazásával, vagy a nem védett, illetve nem használt portok letiltásával. Szintén fontos az operációs rendszer frissítése a legújabb biztonsági javítócsomagok letöltésével és telepítésével.

## ARP-gyorsítótármérgezés

Az ARP (Address Resolution Protocol) az adatkapcsolati réteg (MAC-címek) és a hálózati réteg (IP-címek) címei között fordít. Az ARP-gyorsítótármérgezési támadás lehetővé teszi a támadók számára, hogy elfogják a hálózati eszközök közötti kommunikációt a hálózat ARP-tábláinak (Mac-IP eszközleképezések) megsértésével.

A támadó hamis ARP-válaszüzzenetet küld az alapértelmezett hálózati átjárónak, ezzel tájékoztatva arról, hogy a MAC-cím egy másik célpont IP-címéhez van társítva. Amikor az alapértelmezett átjáró megkapja az üzenetet, és továbbítja a változásokat a hálózat összes többi eszközére, a célpont bármely más hálózati eszközre irányuló összes forgalma a támadó számítógépén megy keresztül. Ez a művelet lehetővé teszi a támadó számára, hogy ellenőrizze vagy módosítsa a forgalmat, mielőtt továbbítja azt a kívánt rendeltetési helyre.

## E-mail útján terjedő kártevők

Az e-mail egy számos előnyt kínáló kommunikációs forma.

A nagyfokú anonimitás miatt azonban az e-mail (és általában az internet) levélszemétküldésre és hasonló illegális tevékenységekre is lehetőséget nyújt. A levélszemét magában foglalja a kényszerű reklámleveleket, a megtévesztő üzeneteket és a kártékony szoftverek, vagyis a [kártevők](#) terjesztését. Az ezzel járó kényelmetlenséget és veszélyt növeli, hogy a levélszemét küldése minimális költséggel jár, és készítőiknek számos eszköz rendelkezésükre áll ahhoz, hogy új e-mail címeket szerezzenek. Emellett a levélszemét mennyisége és változatossága is megnehezíti a kordában tartását. Minél hosszabb ideig használja e-mail-címét, annál nagyobb a valószínűsége, hogy az bekerül egy levélszemétküldő adatbázisába.

Néhány tipp a megelőzéshez:

- Lehetőség szerint ne tegye közzé az e-mail-címét az interneten.
- Címét csak megbízható embereknek adja át.
- A bonyolult címek kitalálására kevesebb az esély, ezért lehetőség szerint ne használjon egyszerű e-mail-címeket (aliasokat).



- Ne válaszoljon a már a postafiókjába került levélszemétre
- Az internetes űrlapok kitöltésekor legyen elővigyázatos, különösen az „Igen, szeretnék tájékoztatást kapni” jellegű válaszokkal.
- Használjon külön e-mail címeket – egyet például a munkához, másikat a barátokkal történő kapcsolattartáshoz stb.
- Rendszeresen módosítsa e-mail-címét
- Használjon levélszemétszűrő alkalmazást.

## Reklámok

Az internetes reklám a hirdetési módszerek egyik leggyorsabban fejlődő változata. Marketingszempontról ennek a módszernek a legjelentősebb előnyei a költségtakarékosság, a célközönség közvetlen elérése és a hatékonyság. Ezenkívül az üzenetek szinte azonnal célba érnek. Számos cég e-mailes marketingeszközöket használ a meglévő és a leendő ügyfelekkel való kapcsolattartáshoz.

Ez a hirdetési mód törvényes, mert a felhasználó bizonyos termékek esetében kíváncsi lehet kereskedelmi információkra is. Számos cég azonban kérés nélkül kereskedelmi üzeneteket küld. Ebben az esetben az e-mail reklám levélszemétnek minősül.

A kérés nélkül üzenetek száma napjainkra jelentős problémává vált, és nincs jele annak, hogy ez a szám csökkenne. A kérés nélkül e-mailek szerzői gyakran szabályszerű üzenetnek álcázzák a levélszemétnet.

## Megtévesztő üzenetek

A téves információkat hordozó megtévesztő üzenetek (angolul: hoax) az interneten terjednek. A megtévesztő üzenetek általában e-mailben és kommunikációs eszközökön (például ICQ és Skype) keresztül terjednek. Az üzenet tartalma gyakorta vicc vagy városi legenda.

A megtévesztő üzenetek félelmet, bizonytalanságot és kétséget próbálnak kelteni a címzettekben, elhitetve velük, hogy egy felderíthetetlen vírus fájlokat töröl és jelszavakat olvas be, illetve más káros tevékenységet folytat a rendszerben.

Egyes megtévesztő üzenetek arra kérik a címzetteket, hogy továbbítsák az üzeneteket ismerőseiknek, és így életben tartják az adott megtévesztő üzenetet. Vannak mobiltelefonos témájú, segélykérő, külföldről pénzt ajánló stb. témájú üzenetek is. A készítő célját a legtöbbször nem lehet megállapítani.

Ha egy üzenet arra szólítja fel, hogy minden ismerősének továbbítsa, az jó eséllyel lehet megtévesztő üzenet. Az interneten számos webhely képes ellenőrizni, hogy egy e-mail szabályszerű-e. Továbbküldés előtt keressen rá az interneten a megtévesztésgyanús üzenetekre.

## Adathalászat

Az adathalászat kifejezés olyan bűnözői tevékenységet határoz meg, amely manipulációs technikákat alkalmaz (vagyis a felhasználót bizalmas információk kiszolgáltatására veszi rá). Célja bizalmas adatok, például bankszámlaszámok vagy PIN kódok megszerzése.



Hozzáférésre általában úgy tesznek szert, hogy megbízható személyek vagy cégek (például pénzügyi intézetek, biztosítási társaságok) nevében e-mailt küldenek a célszemélynek. Az esetleg az eredeti forrásból származó grafikus vagy tartalmi elemeket tartalmazó e-mail külsőre eredetinek tűnhet. Benne különféle ürügyekkel (adategyeztetés, pénzügyi műveletek) arra kérhetik a felhasználót, hogy adjon meg bizonyos személyes adatokat, például bankkártyaszámot vagy felhasználónevet és jelszót. Az ily módon megadott adatokat azután könnyűszerrel ellophatják, és visszaélhetnek velük.

A bankok, biztosítási társaságok és más törvényesen működő cégek sohasem kérnek felhasználóneveket és jelszavakat kérés nélkül levelekben.

## Levélszemét felismerése

A kérés e-mailek azonosításában segítségére lehet néhány ismerv. Ha egy üzenet megfelel az alábbi feltételek némelyikének, akkor az valószínűleg levélszemét.

- A feladó címe nem szerepel az Ön címjegyzékében.
- Az üzenet nagyobb pénzügyi összeget ígér, de előzetesen egy kisebb összeget kér.
- Az üzenet különféle indokokra (adategyeztetés, pénzügyi műveletek) hivatkozva személyes adatok (bankszámlaszám, felhasználónév, jelszó stb.) megadását kéri.
- Az üzenetet idegen nyelven írták.
- Olyan termék megvásárlására szólít fel, amely iránt Ön nem érdeklődik. Ha mégis vásárolni szeretne, ellenőrizze, hogy az üzenet feladója megbízható forgalmazó-e. Ehhez forduljon az eredeti termék gyártójához.
- Egyes szavakat hibás írásmóddal tartalmaz a levélszemétszűrő megtévesztése érdekében. Ilyen például a „vaigra” a „viagra” helyett.

## Szabályok

A levélszemétszűrő megoldások és levelezőprogramok területén a szabályok elősegítik a levelezés működésének szabályozását. Két logikai részből állnak:

1. Feltétel (például egy adott címről érkező üzenet vagy egy bizonyos e-mail-tárgy)
2. Művelet (például az üzenet eltávolítása vagy egy adott mappába helyezése)

A szabályok száma és párosítási lehetőségei vírusvédelmi alkalmazásként eltérőek. Ezek a szabályok jelentik a levélszemét (kérés e-mailek) elleni védővonalat. Tipikus példák:

1. Feltétel: A beérkező e-mail olyan szavakat tartalmaz, amelyek gyakran fordulnak elő kérés e-mailekben
2. Művelet: A levél törlése

1. Feltétel: A beérkező e-mail .exe kiterjesztésű mellékletet tartalmaz
2. Művelet: A melléklet törlése, és a levél kézbesítése a postaládába

1. Feltétel: A beérkező e-mail attól a cégtől érkezik, ahol dolgozik
2. Művelet: Az e-mail áthelyezése a „Munka” mappába

A levélszemét hatékonyabb kezelése és kiszűrése érdekében azt javasoljuk, hogy vegyesen alkalmazza az ilyen szabályokat a levélszemétszűrő programokban.

## Engedélyezőlista

Általánosságban az engedélyezőlista olyan elemek vagy személyek listája, amelyek vagy akik elfogadottak, illetve hozzáférési engedélyt kaptak. Az „e-mail engedélyezőlista” (engedélyezett címek) kifejezés olyan partnerek listáját jelenti, akiktől a felhasználó üzeneteket fogad. Az ilyen listák e-mail címekben, tartománynevekben vagy IP-címekben keresett kulcsszavakon alapulnak.

Ha az engedélyezőlista „kivételek” módban működik, a többi címről, tartományból vagy IP-címről érkező üzeneteket a program nem fogadja. Ha azonban ha a lista nem kizáró jellegű, a program az ilyen üzeneteket nem törli, hanem más módon szűri.

Az engedélyezőlista a [tiltólista](#) alapelvének fordítottjára épül. Karbantartása viszonylag egyszerű, sokkal inkább, mint a tiltólistáké. A levélszemét hatékonyabb szűrése érdekében azt javasoljuk, hogy engedélyező- és tiltólistát egyaránt használjon.

## Tiltólista

A tiltólista általános értelemben a nem elfogadott vagy tiltott elemek és személyek felsorolása. A virtuális világban ez egy olyan technika, amely a listán nem szereplő összes felhasználótól származó üzenet fogadását engedélyezi.

A tiltólistának két típusa van. A felhasználók által a levélszemétszűrő alkalmazásukban létrehozott és a speciális szervezetek által létrehozott professzionális, rendszeresen frissített, az interneten megtalálható tiltólisták.

A hatékony levélszemétszűréshez elengedhetetlen a tiltólisták használata, a listák kezelése azonban a minden nap megjelenő új letiltandó elemek miatt bonyolult. A levélszemét hatékonyabb szűrése érdekében azt javasoljuk, hogy engedélyező- és tiltólistát egyaránt használjon.

## Kivétel

A kivétellista (más néven a kivételek listája) az esetleg hamisított és kéretlen levelek küldésére használt e-mail-címeket tartalmazza. A kizárási listán szereplő címekről érkező e-maileket a program mindig ellenőrzi. Alapértelmezés szerint a kizárási lista a meglévő levelezőfiókokról származó összes e-mail-címet tartalmazza.

## Szerveroldali ellenőrzés

A szerveroldali ellenőrzés olyan technika, amellyel a fogadott üzenetek száma és a felhasználók reakciója alapján azonosítható a tömegesen küldött levélszemét. Minden üzenet (a tartalmától függően) egyedi digitális „lenyomatot” hagy a szerveren. Az egyedi azonosítószám semmit nem árul el az e-mail tartalmáról. Két azonos

üzenet azonos lenyomatot hagy, de két különböző üzenet lenyomata eltérő.

Ha a felhasználó egy üzenetet levélszemétként jelöl meg, a program elküldi az üzenet lenyomatát a szervernek. Ha a szerver több azonos lenyomatot kap (egy bizonyos levélszemétre vonatkozóan), adatbázisba menti őket. A bejövő üzenetek ellenőrzésekor a program a lenyomatukat elküldi a szervernek. A szerver azt az információt küldi vissza, hogy mely lenyomatok felelnek meg a felhasználók által már levélszemétként megjelölt üzenetnek.

## Speciális memória-ellenőrzés

A Speciális memória-ellenőrzés az Exploit blokkolóval együttműködve erősíti a kártevőirtók általi észlelés elkerüléséhez összezavarást és/vagy titkosítást használó kártevőkkel szembeni védelmet. Azokban az esetekben, amikor a hagyományos elemzés vagy heurisztika nem feltétlenül észlel egy kártevőt, a speciális memória-ellenőrzés felismeri a gyanús viselkedést, és ellenőrzi a kártevőket, amikor megjelennek a rendszermemóriában. Ez a megoldás még az erősen elrejtett kártevőkkel szemben is hatásos.

Az Exploit blokkolótól eltérően, a speciális memória-ellenőrzés egy utólagos módszer, amely esetén fennáll a veszély, hogy a kártevők észlelése előtt már történt valamilyen kártékony tevékenység; más észlelési technikák kudarca esetén azonban egy további biztonsági lehetőséget jelent.

## Netbank- és tranzakcióvédelem

A Netbank- és tranzakcióvédelem a védelem egy újabb rétege, amellyel megóvhatja pénzügyi adatait az online tranzakciók során.

Az ESET Smart Security Premium és az ESET Internet Security beépített listát tartalmaz azokról az előre definiált webhelyekről, amelyek hatására védett böngésző nyílik meg. A termék konfigurációjában hozzáadhat egy webhelyet, illetve szerkesztheti a webhelyek listáját.

Az Összes böngésző védelme funkció bekapcsolásával elindíthatja az összes támogatott webböngészőt biztonságos módban.

A funkcióról az ESET alábbi tudásbáziscikkeiben talál további részleteket:

- [Hogyan használhatom az ESET Netbank- és tranzakcióvédelem modult?](#)
- [A Netbank- és tranzakcióvédelem szüneteltetése vagy letiltása az ESET Windows otthoni termékekben](#)
- [ESET Netbank- és tranzakcióvédelem – gyakori hibák](#)

A HTTPS titkosított kommunikáció használata a védett böngészés végrehajtásához szükséges. A netbank- és tranzakcióvédelmet a következő böngészők támogatják:

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

## Nyissa meg a Netbank- és tranzakcióvédelmet a böngészőjében

Amikor közvetlenül a termékmenü **Eszközök** lapjáról nyitja meg a Netbank- és tranzakcióvédelmet, akkor az abban a webböngészőben nyílik meg, amelyet alapértelmezettként állított be a Windows rendszerben. Ellenkező esetben az előnyben részesített webböngésző megnyitásakor (nem a termékmenüből) a védett webhelyek listáján szereplő webhelyek átirányításra kerülnek az ESET által védett azonos típusú webböngészőre.

## Botnet elleni védelem

A botnet elleni védelem úgy fedezi fel a kártevőket, hogy elemzi a hálózati kommunikációs protokolljaikat. Az elmúlt években változatlan hálózati protokollokkal ellentétben a botnetes kártevők gyakran változnak. Az ESET ennek az új technológiának a segítségével nyújt védelmet azok ellen a kártevők ellen, amelyek észrevétlenül megpróbálják a botnet hálózatához csatlakoztatni a számítógépet.

## DNA-észlelések

Az észlelési típusok a nagyon egyedi kivonatoktól kezdve egészen az ESET DNA-észlelésekig terjednek, amelyek a kártékony viselkedés és a kártevőjellemzők összetett definíciói. Míg a kártékony kódot könnyen módosítani és rejtjelezni tudják a támadók, az objektumok viselkedése nem módosítható ilyen egyszerűen, és az ESET DNA-észlelések ki is használja ezt az elvet.

Mélyreható elemzésnek vetjük alá a kódot, és kinyerjük a viselkedésért felelős „géneket”, majd megalkotjuk az ESET DNA-észleléseket, amelyekkel a gyanús kódok mérhetőek fel, akár a lemezen, akár a futó folyamatmemóriában találhatók. A DNA-észlelések azonosítani tud bizonyos ismert kártevőmintákat, egy-egy ismert kártevőcsalád új változatait, illetve akár korábban nem tapasztalt vagy ismeretlen kártevőt is, amely kártékony viselkedést jelző géneket tartalmaz.

## ESET LiveGrid®

Az ESET ThreatSense.Net korszerű korai riasztási rendszerre épülő ESET LiveGrid® felhasználja és az ESET víruslaborjába küldi az ESET felhasználói által szerte a világból beküldött adatokat. A gyanús minták és metaadatok biztosításával a ESET LiveGrid® lehetővé teszi, hogy azonnal választ adjunk ügyfeleink igényeire, és biztosítsuk az ESET hatékonyságát a legújabb kártevőkkel szemben.

Az ESET kártevőkutatói az adatokat használva állítják össze a globális kártevők természetét és körét tartalmazó pontos képet, amely hozzásegít bennünket ahhoz, hogy a megfelelő célokra összpontosítsunk. Az ESET LiveGrid® adatai fontos szerepet játszanak automatizált folyamataink prioritásának felállításában.

A technológia által megvalósított megbízhatósági rendszerrel emellett fokozható kártevőirtó szoftvereink általános hatékonysága. A felhasználók a [futó folyamatok](#) és megnyitott fájlok megbízhatóságát közvetlenül a program felületén, illetve az ESET LiveGrid® rendszerből származó járulékos információkat is megjelenítő helyi menükben tekinthetik meg. Amikor egy végrehajtható vagy tömörített fájl áll vizsgálat alatt a felhasználó rendszerében, először annak kivonatképe hasonlít össze az engedélyezett és a tiltólistán szereplő elemek adatbázisával. Ha a kivonatképe megtalálható az engedélyezettlistán, a megvizsgált fájl tisztának tekinthető, és a jövőbeli ellenőrzések alóli kivételként jelölhető meg. Ha a tiltólistán szerepel, a kártevő jellegétől függően a megfelelő műveleteket végzi el a rendszer. Ha nem található egyezés, a fájl alapos vizsgálaton megy keresztül. Az ellenőrzés eredményétől függően a fájlok besorolása lehet kártevő és nem kártevő. Ez a megoldás határozottan jó hatással van az ellenőrzés teljesítményére. A megbízhatósági rendszer hatékonyan felismeri a kártevőmintákat

még azt megelőzően, hogy vírusdefinícióik a vírusdefiníciós adatbázison keresztül a felhasználó számítógépére kerülnek (amely naponta többször is megtörténik).

Az ESET LiveGrid® megbízhatósági rendszeren kívül az ESET LiveGrid® visszajelzési rendszer az újonnan felfedezett kártevőkkel kapcsolatos információkat gyűjt a számítógépről. Ez az információ tartalmazhatja a kártevőt magában foglaló fájl mintáját vagy másolatát, a fájl elérési útját és nevét, a dátumot és az időt, azt a folyamatot, amelynek során a kártevő megjelent a számítógépen, valamint a számítógép operációs rendszerére vonatkozó adatokat.

### ESET LiveGrid®-szerverek



ESET LiveGrid®-szervereink Pozsonyban, Bécsben és San Diegóban találhatók, viszont ezek csupán azok a szerverek, amelyek az ügyfelektől érkező kérésekre válaszolnak. A leadott minták feldolgozása Pozsonyban (Szlovákia) megy végbe.

### Az ESET LiveGrid® engedélyezése vagy letiltása az ESET-termékekben



Az ESET LiveGrid® ESET-termékekben való engedélyezéséről és letiltásáról az [ESET tudásbáziscikkében](#) tájékozódhat részletesen.

## Exploit blokkoló

Az Exploit blokkoló a támadásoknak gyakran kitett alkalmazástípusok, például webböngészők, PDF-olvasók, levelezőprogramok és Microsoft Office-összetevők megerősítésére szolgál, és véd az [ROP-támadások](#) ellen. Az Exploit blokkoló alapértelmezés szerint elérhető és engedélyezve van minden ESET Windows otthoni termékben, Windows Serverhez készült ESET-termékben és Windowshoz készült ESET endpoint termékben.

A blokkoló a folyamatok viselkedésének figyelésével olyan gyanús tevékenységeket keres, amelyek biztonsági résekre utalhatnak.

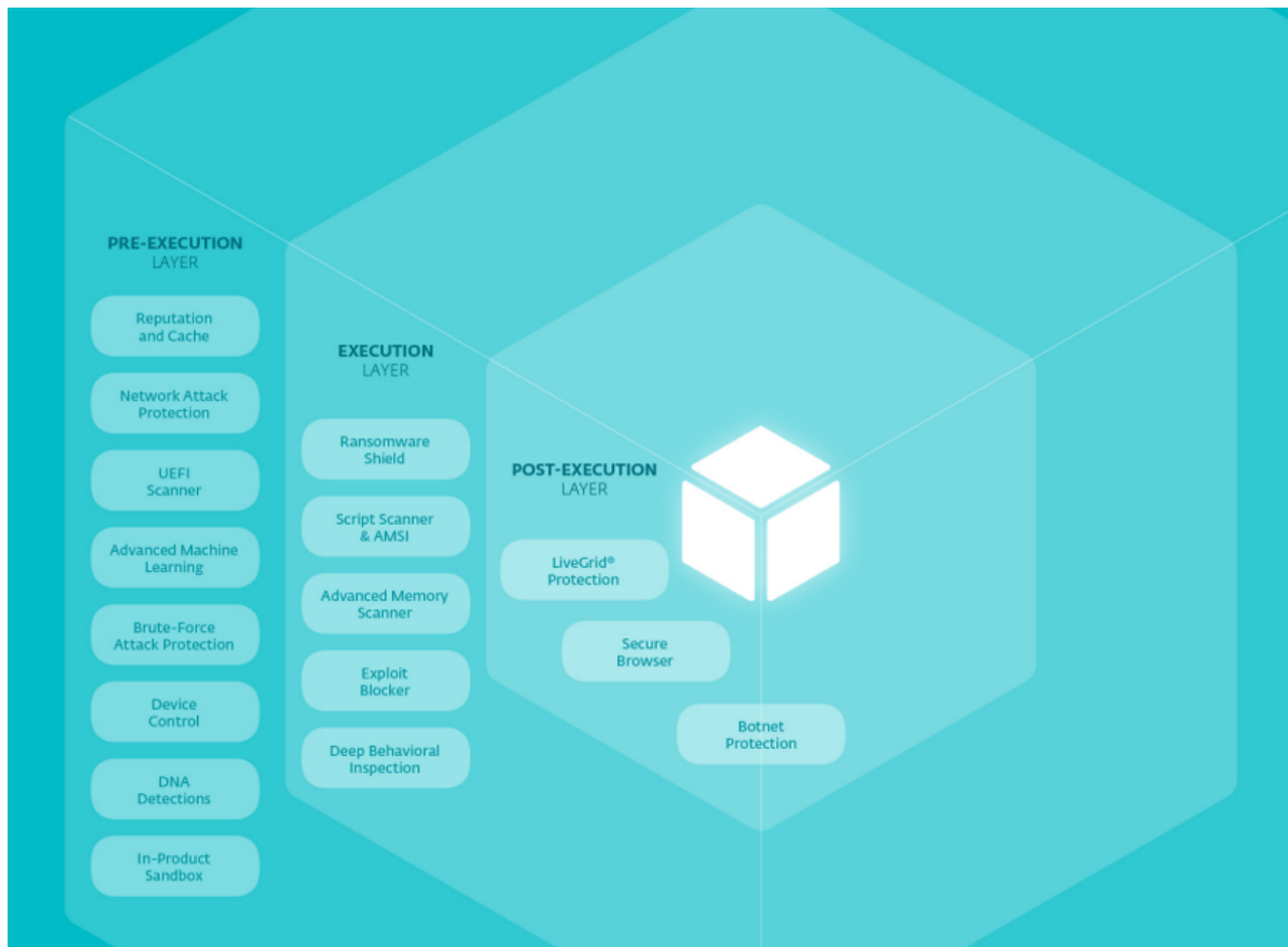
Amikor az Exploit blokkoló gyanús folyamatot talál, azonnal leállítja, valamint rögzíti és elküldi a kártevőre vonatkozó adatokat az ESET LiveGrid® felhőrendszernek. Az ESET feldolgozza és arra használja ezeket az adatokat, hogy javítsa a felhasználók védelmét az ismeretlen és a teljesen új kártevőkkel szemben, amelyek ellen még nem létezik előre beállított védekezés.

## Java Exploit blokkoló

A Java Exploit blokkoló a már eddig is létező [Exploit blokkoló technológia](#) bővítménye. Figyeli a Javát, és a biztonsági rések kiaknázására utaló viselkedéseket keres. A blokkolt minták jelenthetőek a kártevőkre szakosodott elemzőknek, akik így vírusdefiníciók létrehozásával blokkolhatják őket a különböző rétegeken (URL-blokkolás, fájlletöltés stb.).

## ESET LiveSense

Az ESET számos egyedi, szabadalmaztatott, többretegű védelmi technológiát használ, amelyek együttműködnek az ESET LiveSense szolgáltatásként. Az alábbi ábra bemutatja az ESET néhány alapvető technológiáját, és jelzi, hogy megközelítőleg mikor és hol tudnak észlelni, majd letiltani egy kártevőt az életciklusa alatt a rendszerben.



## Gépi tanulás

Az ESET 1990 óta gépi tanulási algoritmusok segítségével észleli és tiltja le a kártevőket. 1998-ban a neurális hálózatok is az ESET-termékek keresőmotorjának részévé váltak.

A gépi tanulás magában foglalja a [DNA-észleléseket](#), amelyek gépi tanulás révén alkotott modellek segítségével végeznek hatékony munkát felhőkapcsolattal vagy anélkül. A gépi tanulási algoritmusok a bejövő minták kezdeti válogatásának és osztályozásának is fontos részét képezik, és elhelyezik őket a képzeletbeli „kiberbiztonsági térképen”.

Az ESET kifejlesztette a saját, házon belüli gépi tanulási motorját. A motor a neurális hálózatok (például mélytanulás és hosszú rövid távú memória) és hat osztályozási algoritmus gondosan válogatott csoportjának kombinált hatékonyságát alkalmazza. Ezáltal konszolidált eredményt tud generálni, és megfelelően el tudja látni a bejövő mintát a tiszta, a potenciálisan káros vagy a rosszindulatú címkével.

A finomhangolás eredményeképpen az ESET gépi tanulási motorja más védelmi technológiákkal – például DNA, sandbox és [memóriaelemzés](#) –, valamint viselkedésalapú funkciókkal is együttműködik, ami által a legkiemelkedőbb észlelési arányokat és a lehető legalacsonyabb számú [téves riasztást](#) tudja biztosítani.

### A víruskereső konfigurálása az ESET-termék További beállítások lapján

- [ESET Windows otthoni termékek](#) (13.1-es verziótól)
- [ESET Windows otthoni termékek](#) (7.2-es verziótól)

# Hálózati támadások elleni védelem

A hálózati támadások elleni védelem a tűzfal bővítménye, amely javítja az ismert biztonsági rések felismerését a hálózat szintjén. A gyakori biztonsági rések felismerésének megvalósításával a széleskörűen használt protokollokban (például SMB, RPC és RDP) újabb fontos védelmi szintet hoz létre az olyan terjedő kártevőkkel, hálózati támadásokkal és biztonsági rések kihasználásával szemben, amelyekhez még nem adtak ki vagy nem telepítettek javítást.

## Zsarolóprogram elleni védelem

A Zsarolóprogramok elleni védelem egy viselkedésalapú észlelési technika, amely felügyeli azoknak az alkalmazásoknak és folyamatoknak a viselkedését, amelyek a [zsarolóprogramokhoz/fájlkódolókhöz](#) hasonló módon próbálnak meg fájlokat módosítani. Ha egy alkalmazás viselkedését károsnak ítéli, vagy ha a megbízhatóságon alapuló ellenőrzés gyanúsként jelenít meg egy alkalmazást, a védelmi modul letiltja az alkalmazást, vagy megkérdezi a felhasználót, hogy letiltsa vagy engedélyezze.



Az ESET LiveGrid® szolgáltatást engedélyezni kell a Zsarolóprogram elleni védelem megfelelő működéséhez. Tekintse meg az [ESET tudásbáziscikkét](#) annak biztosításához, hogy az ESET LiveGrid® engedélyezve legyen és működjön az ESET-termékben.

## Szkript-alapú támadások elleni védelem

A szkriptalapú támadások elleni védelem védelmet biztosít a webböngészőkben előforduló Javascript-tartalmak ellen, valamint Antimalware Scan Interface (AMSI) típusú védelmet nyújt a PowerShell-szkriptek ellen.



### Behatolásmegelőző rendszer (HIPS)

A funkció csak akkor működik, ha [engedélyezve](#) van a behatolásmegelőző funkció.

A szkript-alapú támadások elleni védelem az alábbi webböngészőket támogatja:

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



### Támogatott webböngésző használata

A webböngészők legrégebbi támogatott verziója változó lehet, mivel a böngészők fájlaláírása gyakran változik. A webböngészők legújabb verziója azonban mindig támogatott.

## Védett böngésző

A Védett böngésző a védelem egy újabb rétege, amellyel megóvhatja bizalmas jellegű adatait az internetes böngészés során (például a pénzügyi adatokat az online tranzakciók során).

Az ESET Endpoint Security 8-as és újabb verziói beépített listát tartalmaz az előre definiált webhelyekről, amelyek hatására védett böngésző nyílik meg. A termék konfigurációjában hozzáadhat egy webhelyet, vagy szerkesztheti a webhelyek listáját. A Védett böngésző alapértelmezés szerint le van tiltva a telepítést követően.

A funkcióról az [ESET alábbi tudásbáziscikkében](#) talál további részleteket:

A HTTPS használatával titkosított kommunikáció szükséges a védett böngészéshez. A Védett böngésző használatához a webböngészőnek teljesítenie kell az alábbi minimális követelményeket:

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

**i** Csak a Firefox és a Microsoft Edge támogatott az ARM processzorokkal felszerelt eszközökön.

## Az ESET Védett böngésző megnyitása a webböngészőben

Amikor közvetlenül a termékmenü **Eszközök** lapjáról nyitja meg az ESET Védett böngészőt, akkor abban a webböngészőben nyílik meg, amelyet alapértelmezettként állított be. Ellenkező esetben az előnyben részesített webböngésző megnyitásakor (nem a termékmenüből) az ESET belső listája átirányításra kerül az ESET által védett azonos típusú webböngészőre.

## UEFI Scanner

Az UEFI Scanner (Unified Extensible Firmware Interface) a Behatolásmegelőző rendszer (HIPS) részét képezi, amely az UEFI-firmware-t védi a számítógépen. Az UEFI egy olyan firmware, amely az indítási folyamat elején töltődik a memóriába. A kód az alaplapra hegesztett flashmemóriachipen található. A megfertőzésével a támadók olyan kártevőt tudnak telepíteni, amely a rendszer újratelepítésével és újraindításával sem pusztítható el. A kártevőt sokszor a kártevőirtó megoldások sem észlelik, mivel a legtöbbjük nem ellenőrzi ezt a réteget.

Az UEFI Scanner automatikusan aktiválódik. Manuálisan a fő programablakból indíthatja a számítógép ellenőrzését a **Számítógép ellenőrzése > További ellenőrzések > Egyéni ellenőrzés** elemre kattintva, majd a **Rendszerindítási szektorok/UEFI** elemet kiválasztva.

**i** Ha már megfertőzte a számítógépét egy UEFI-kártevő, olvassa el az ESET kapcsolódó tudásbáziscikkét: [A számítógépet megfertőzte egy UEFI-kártevő – mit tegyek?](#)

## Kanári fájl

A kanári fájl egy számítógépes áldokumentum, amelyet a tényleges dokumentumok közé kell elhelyezni, hogy segítse az adatokhoz való jogosulatlan hozzáférés, másolás vagy módosítás korai felismerését.

## Holtpont

A holtpont egy olyan helyzet, amikor az egyes számítógépes folyamatok egy másik folyamathoz rendelt erőforrásra várnak. Ilyen helyzetben egyik folyamat végrehajtása sem megy végbe, mivel a szükséges erőforrást egy másik folyamat tartja fel, amely szintén egy másik erőforrás feloldására vár. Fontos megakadályozni a holtpontot, mielőtt fellépne. A holtpont létrejöttét az erőforrás-ütemező tudja észlelni, amely segít az operációs



rendszernek nyomon követni a különböző folyamatokhoz rendelt összes erőforrást. Akkor kerülhet sor holtpontra, ha a következő négy feltétel egyszerre fennáll:

- **Nincs megelőző intézkedés** – Egy erőforrást csak az a folyamat oldhatja fel önként, amely azt feltartja, miután az adott folyamat befejezte a feladatát.
- **Kölcsönös kizárás** – A megosztott erőforráshoz való hozzáférés ellenőrzésére szolgáló bináris szemafor speciális típusa. Lehetővé teszi az aktuálisan legmagasabb prioritású feladatok blokkolását a lehető legrövidebb ideig.
- **Tartás és várakozás** – Ebben az állapotban a folyamatokat meg kell akadályozni abban, hogy egy vagy több erőforrást feltartsanak, miközben egyszerre várnak egy vagy több erőforrásra.
- **Körkörös várakozás** – Az összes erőforrástípus teljes megrendelését írja elő. A körkörös várakozás azt is megköveteli, hogy minden folyamat a felsorolás növekvő sorrendjében kérjen erőforrásokat.

Háromféleképpen lehet kezelni a holtpontot:

- Ne hagyja, hogy a rendszer a holtpont állapotába kerüljön.
- Hagyja, hogy a holtpont bekövetkezzen, majd tegye meg a megelőző lépéseket a kezeléséhez.
- Ha holtpont lépett fel, indítsa újra a rendszert.