

Fejlett védelmet biztosít a szervereken, megosztásokban - beleértve a OneDrive-ot is - és többfeladatos kiszolgálókon található adatai számára az alábbi védelmi modulok segítségével

Az ESET a **többrétegű technológiájával** túlmutat egy egyszerű vírusirtó program képességein . A továbbfejlesztett memóriaellenőrzés az ESET egyedülálló technológiája, amely hatékonyan kezeli a bonyolult összezavarást és/vagy erős titkosítást alkalmazó modern kártevők problémáját. Figyeli a gyanús folyamatokat, és ellenőrzi azokat, amint felfedik magukat a rendszer memóriájában.

Ha egy folyamat a memória egy addig nem használt futtatható területéről indít egy rendszerhívást, a továbbfejlesztett memóriaellenőrzés az ESET viselkedés-alapú észlelés használatával ellenőrzi az adott folyamatot. A hatékony gyorsítótárazásnak köszönhetően a továbbfejlesztett memóriaellenőrzés nem okoz észrevehető csökkenést a számítási sebességben.

Sőt mi több, a fejlett kártevőkben megfigyelhető egy új trend, miszerint azok egyre gyakrabban "kizárólag a memóriában" működnek, anélkül, hogy lenne a fájlrendszeren bármilyen komponensük, amelyet a hagyományos módszerekkel észlelni lehetne. Csak memóriaellenőrzéssel lehetséges az ilyen támadásokat felfedezni, és éppen erre való az ESET továbbfejlesztett memóriaellenőrzés modulja.

Az ESET keresőmotorja a rosszul formázott dokumentumokban rejlő sebezhetőségekre figyel, a hálózati támadások elleni védelem a kommunikációt ellenőrzi, az exploit blokkoló pedig magát a sebezhetőséget kihasználó folyamatot blokkolja. Ezt a technológiát folyamatosan fejlesztjük, és rendszeresen új észlelési módszerekkel bővítjük, hogy a sebezhetőségeket kihasználó új technikákat is felismerje.

Az ESET Zsarolóprogramok elleni védelme a védelmi alkalmazás egyik kiegészítő rétege. melynek feladata a felhasználók megóvása a váltságdíjat követelő vírusoktól, más néven zsarolóprogramoktól. Ez a védelmi modul a viselkedés- és reputáció alapú heurisztika segítségével figyeli és kiértékeli az összes futtatott alkalmazást.

A hálózati támadások elleni védelem a tűzfal technológiánk egy kiterjesztése, amely hálózati szinten javítja az ismert sérülékenységeket célzó támadások felismerését. A széles körben használt protokollokat (pl. SMB, RPC vagy RDP) érintő sérülékenységek felismeréséért felelős modul a védelmi rendszernek egy olyan fontos rétege, amely védelmet nyújt a kártevők terjedésével és a hálózati támadásokkal szemben, illetve az olyan sérülékenységek kiaknázása ellen is, amelyekre a gyártó által kiadott javítás még nem létezik, vagy nincs telepítve.

Az ESET botnet elleni védelme észleli a botnetek kártékony kommunikációját, és egyúttal azonosítja is a káros folyamatot. A vírusos objektum azonosítását követően meg lehet tenni a szükséges ellenlépéseket, sőt alkalmanként még a kommunikálása során használt titkosítást is vissza lehet fejteni.