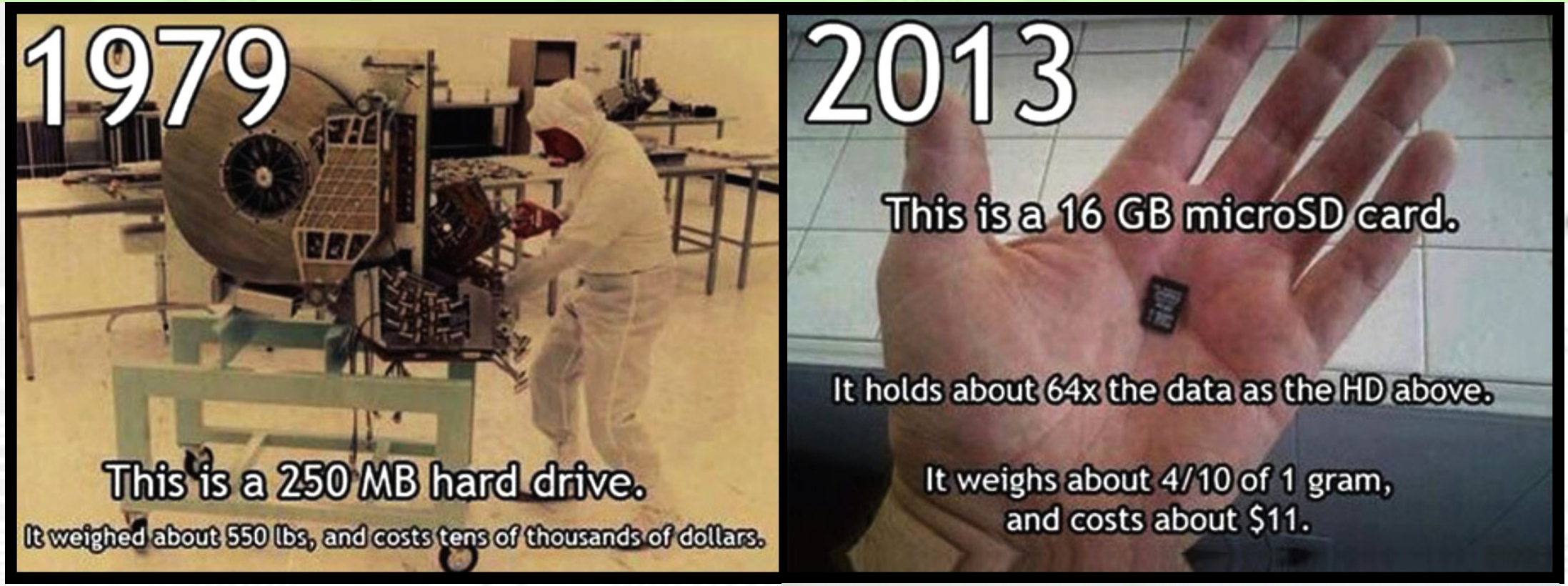

SICONTACT
biztonság a digitális világban
eset
IT Business & Technology 2019.

Csizmazia-Darab István
Sicontact, IT biztonsági szakértő

1968. KFKI - TPA
- Tárolt Programú Analizátor (KB döntés)
- A DEC PDP-8 nyomán, Assembler, FORTRAN
- Lyukszalag-olvasó, szalaglyukasztó

1969.07. Apolló 11. DSKY
- 2kB RAM, 36 kB ROM
- 1 MHz 16 bit CPU
- 1300x gyengébb, mint iPhone 5C



1981. ZX81, IBM/PC XT
- 1982. C64, IBM/PC AT
- 1985. Intel 386
- 1989. Intel 486
- 1993. Intel Pentium

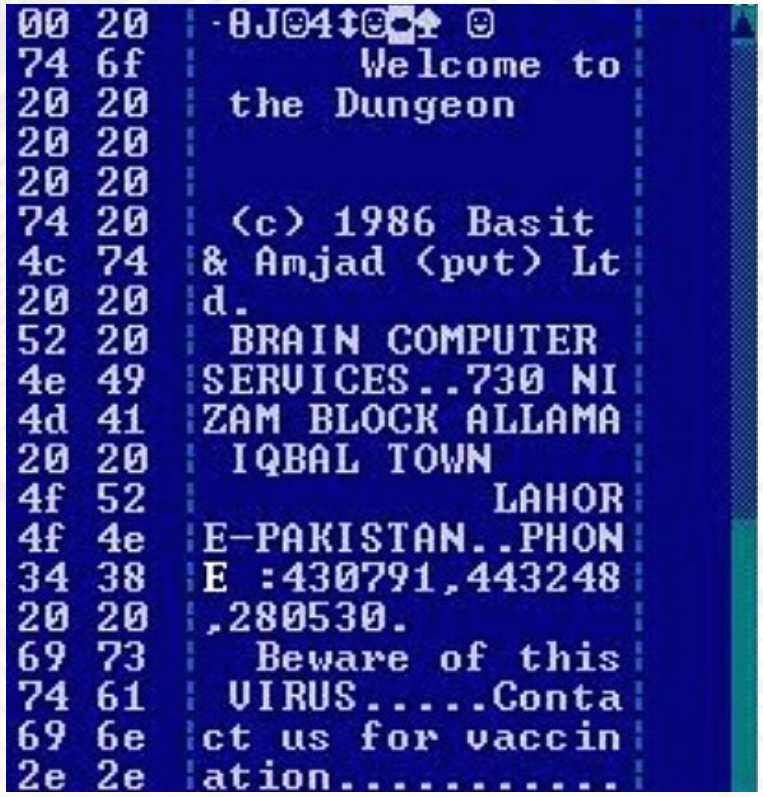
1997. Deep Blue Vs Kasparov - 4:2
- 259-ik szuperszámítógép, 11.38 GigaFlops

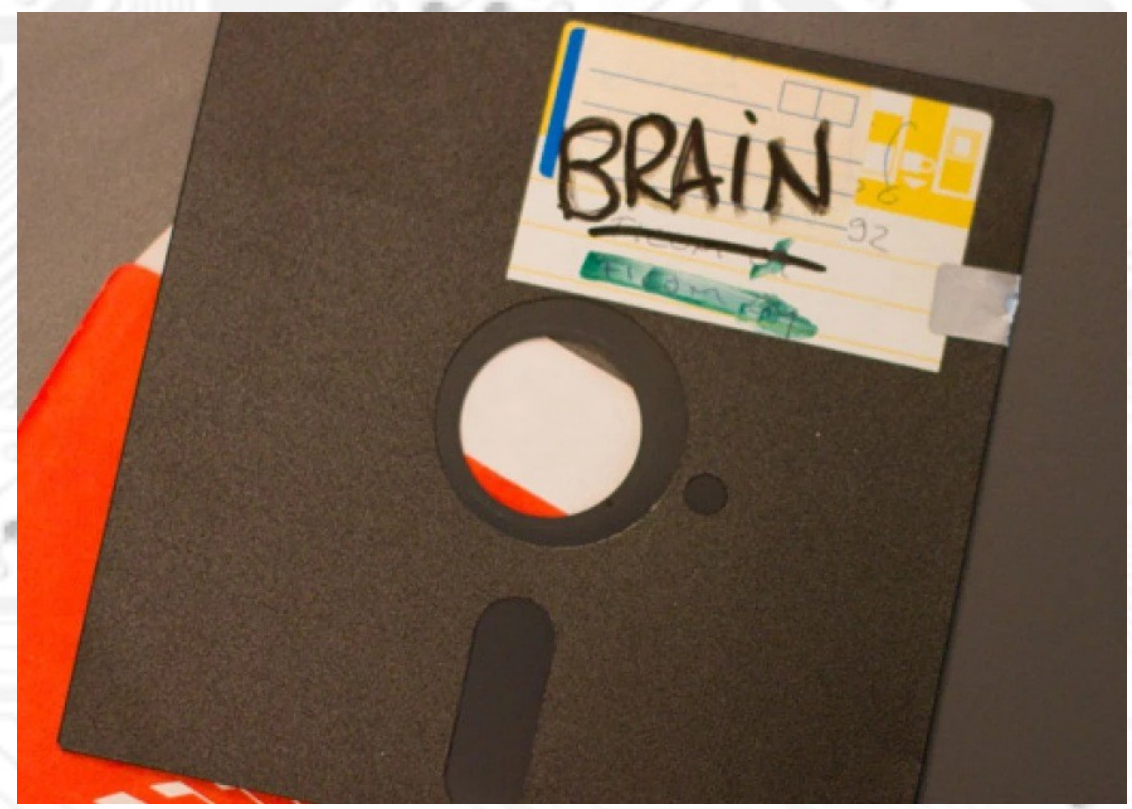
2016. Google DeepMind Challenge Match
- AlphaGo:dél-koreai Lee Sedol 4:1

- 2018. Summit IBM Power, 122 PetaFlops
- 2017. Sunway TaihuLight 93 PetaFlops
- 2016. Tianhe-2, 33 PetaFlops

2018. 7.6 mrd netező, 23.14. mrd netes eszköz (Internet World Stats, Statista)

- IBM PC Brain vírus
- Név, cím, telefonszám a kódban
- 5 1/4 floppy lemez boot rekord
- 1 hét alatt szétterjedt a világon





III. ÉVFOLYAM 25. SZÁM
1988. DECEMBER 14.

Hozzászólás vírusügyben

Több alkalommal írtak lapjukban és a *Mikrovilágban* is vírusokról szóló cikkeket. Ezek többnyire külföldi példákra hivatkoztak.

A vírus azonban hazánkat is elérte. Jó nevű felsőoktatási intézményünk több gépe is elfertőződött már. Még belegondolni is rossz, mi történik, ha minden felhasználó továbbadja barátainak, környezetének a veszélyes kórt. Most a vírusok egyik legkellemetlenebb fajtájáról lesz szó. Terjedése igen gyors, és mivel beleír a FAT táblába, teljes adatvesztést okozhat. További kísérőjelenség még, hogy a képernyőkarakterek időnként „lezuhannak" az alsó sorba. Ez azonban csak XT gépen fordul elő. E rövid ismertetővel segítséget szeretnék nyújtani a számítógépeseknek, hogy mi a teendő fertőzésgyanús esetben.

A vírus jelenléte felismerhető a PC-Tools 4.xx-es verziójával. A program F(ind) funkcióját kell meghívni, és a következő hexa-sorozatot keresni: 01 FA 8B EC E8 00 00 5B 81 EB. Először a winchestert, majd utána minden egyes hajlékonylemezünket végig kell vizsgálni. Ha találtunk ilyen karaktersorozatot, az egyértelműen jelzi, hogy fertőzött a lemezünk. Az érintett program nevét a PC-Tools kiírja. Könnyen észrevehetjük a vírus jelenlétét úgy is, hogy írásvédett lemezt teszünk a meghajtóba, és katalógust kérünk. Ekkor az „Error on drive A, Attempt to write on write protected disk" hibaüzenetet kapjuk.

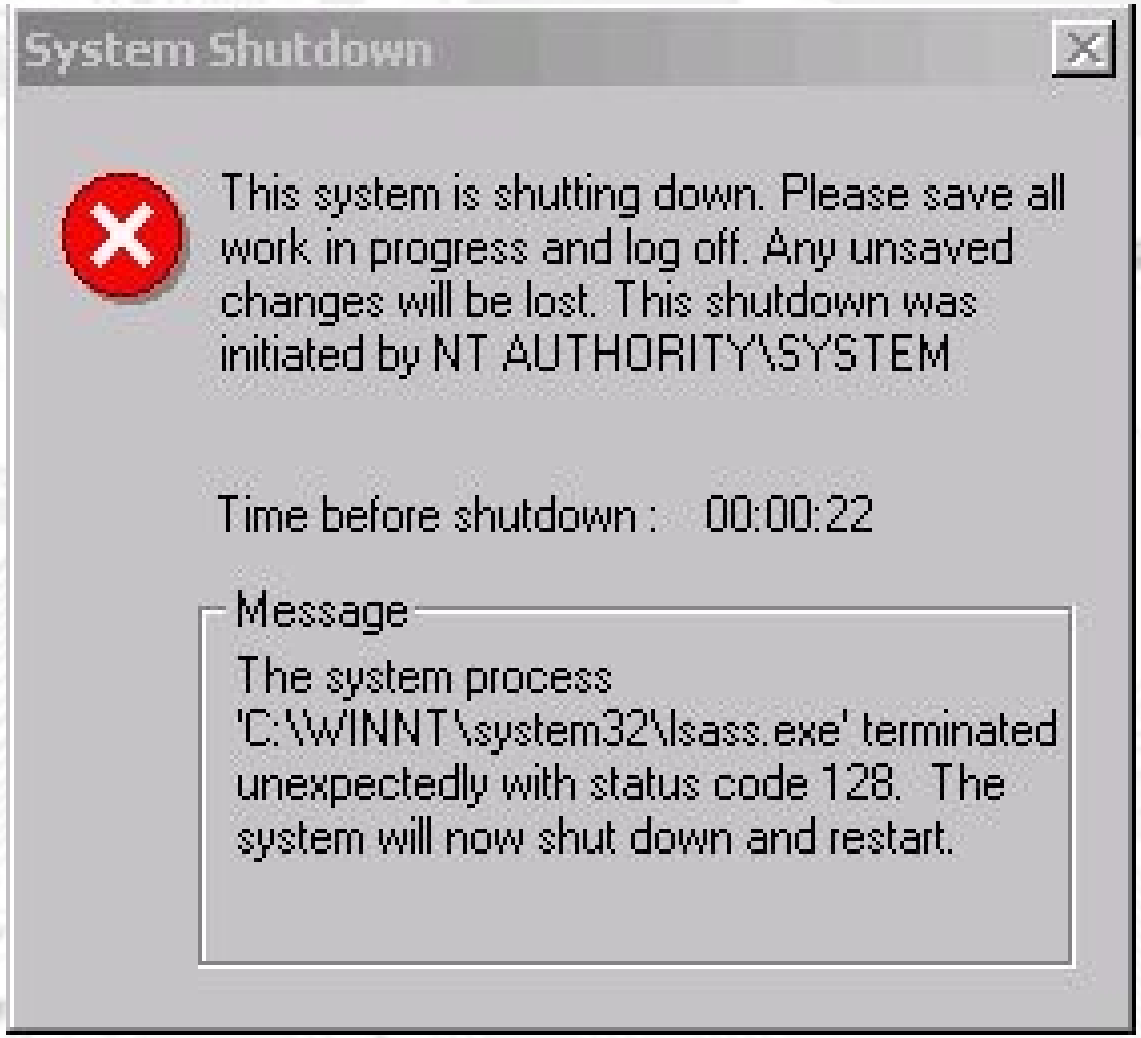
A vírus a DOS-utasításokkal is terjed, tehát ha egy gépen „csak" a winchester vírusos, hajlékonylemezünkre egy sima **dir a:** parancs is életveszélyes lehet. A rendszerállományok hosszát szintén megnézhetjük: a DOS 3.3-as COMMAND.COM eredeti hossza 25 307 bájt. Indításakor 1701 bájttal lesz hosszabb az eredeti program. A vírus az .EXE és a .COM állományokat támadhatja meg. Egy programhoz többször is hozzámásolódhat.

Ha már a gépünkben van, akkor csak a merevlemez újraformázása segít, abból is a kemény, vagyis fizikai formázás. Erre azért van szükség, mert van a vírusnak olyan formája, amely több DOS-formázást is elvisel a winchesteren. Megfelelő erre a célra például a Disk Manager vagy a diagnosztikai lemez. Ezt vírusmentes gépen másoljuk hajlékonylemezre, és onnan indítsuk el. A rendszert és a használatban levő programjainkat utána kizárólag biztos forrásból másoljuk vissza.

Ha „tiszták" vagyunk, elég arra vigyázni, hogy a jövőben új programokat csak a fent leírt ellenőrzés után másoljuk be winchesterünkre. A vizsgálat előtt még katalógust sem szabad kérni! További védekezésként, különösen ha többen is dolgoznak egy gépen, hasznos lehet egy rövid programot írni a COMMAND.COM hosszának figyelésére, és ezt az AUTOEXEC.BAT-ba beleírni.

Csizmazia D. István

- Nincs fájl, a memóriába töltődött
- Hálózati csomagban terjedt
- Az első félórában 75 ezer gép
- Kb. 750 millió USD összkár
- MS 2002-es javítócsomag



2008. 90% használ antivírust, de csak 10% tudja a nevét, hogy milyet

A Macintosh sem "érinthetetlen"

- 2012-ig: "Itt nincsenek vírusok"

- 2012-től: "A rendszert úgy alakították ki, hogy az biztonságos legyen, és védjen a rosszindulatú szoftverek letöltése ellen"

Store Mac iPod iPhone iPad iTunes Support

Flashback malware removal tool

About Flashback malware removal tool

This update removes the most common variants of the Flashback malware. This update contains the same malware removal tool as Java for OS X 2012-003.

If the Flashback malware is found, a dialog will be presented notifying the user that malware was removed.

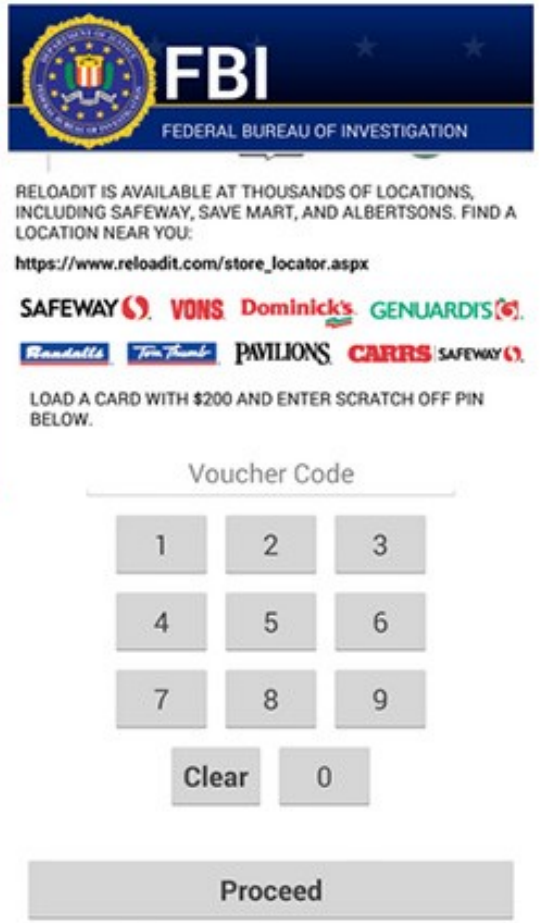
In some cases, the Flashback malware removal tool may need to restart your computer in order to completely remove the Flashback malware.

Download

Version: 1.0
Post Date: April 13, 2012
Download ID: DL1517
License: Update
File Size: 356 KB
System Requirements
OS X Lion without Java installed

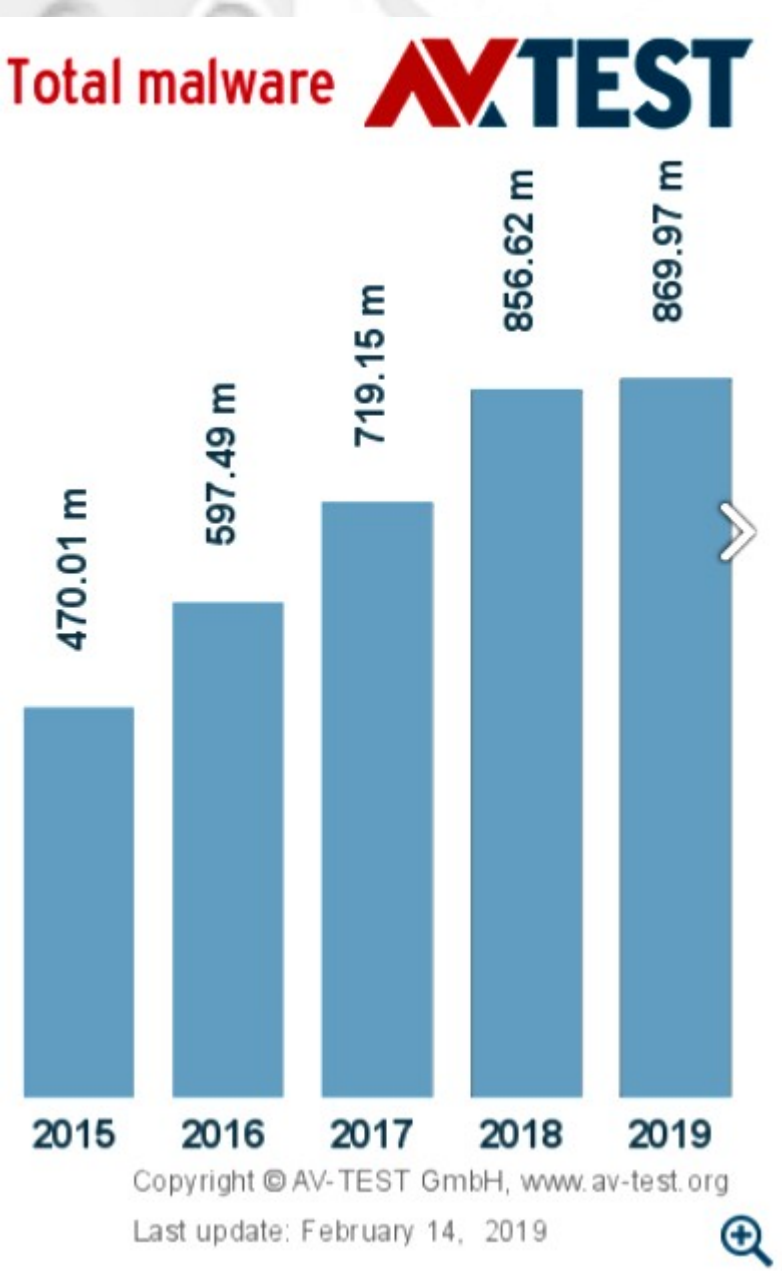
Supported Languages
Deutsch, English, Français, 日本語, Español, Italiano, Nederlands, Dansk, Norsk Bokmål, Polski, Português, Português Brasileiro, Русский, Suomi, Svensk, 简体中

- 2012. március 600 ezer Flashback botnet
- Java sebezhetőség, egyes változatok közbeavatkozás nélkül is terjedtek



- 2014. SimpLocker Android, 260 ukrán Hrivnya, AES, TOR, ZIP, 7z, RAR
- 2015. Linux/BSD szervereken Mumblehard botnet
- 2016. OpenSSH 12 éves CVE-2004-1653 bug (router, NAS, CCTV, DVR, IoT, stb.)
- 2016. Samsam ransomware javítatlan Red Hat JBoss szerverek

Total malware, meghackelési idők a kezdeti behatolást követően

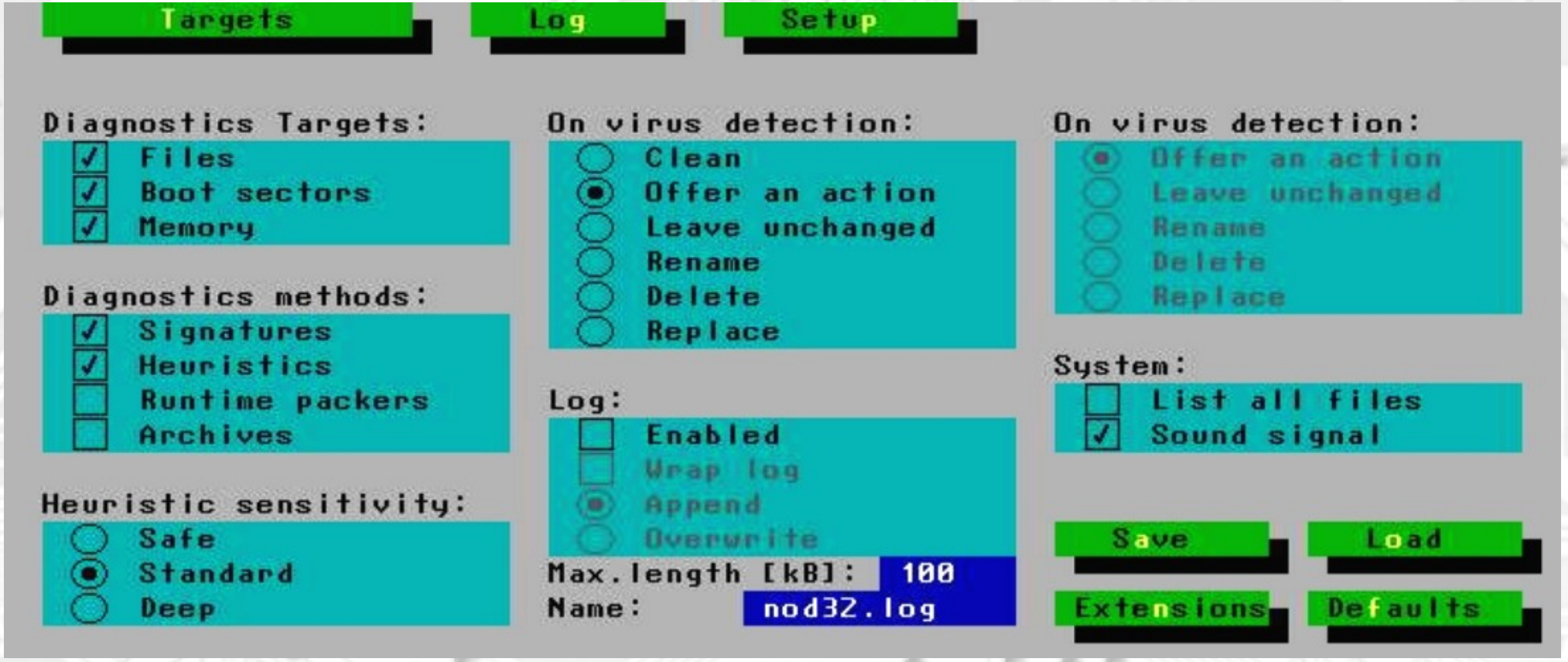


2019. Crowdstrike Global Threat Report, toplista

1. - 0 óra 18 perc 49 másodperc - oroszok
2. - 2 óra 28 perc 14 másodperc - észak-koreaiak
3. - 4 óra 00 perc 26 másodperc - kínaiak
4. - 5 óra 09 perc 04 másodperc - irániak

1987. A legelső NOD verzió megjelenése

Peter Paško, Miroslav Trnka



- Proaktív technikák, virtuális kódemuláció, heurisztikus felismerés (Advanced Heuristics)
- Új, ismeretlen kártevők ellen, minimális vakriasztás
- Kiterjesztett heurisztikában gépi tanulás (ML) alkalmazása

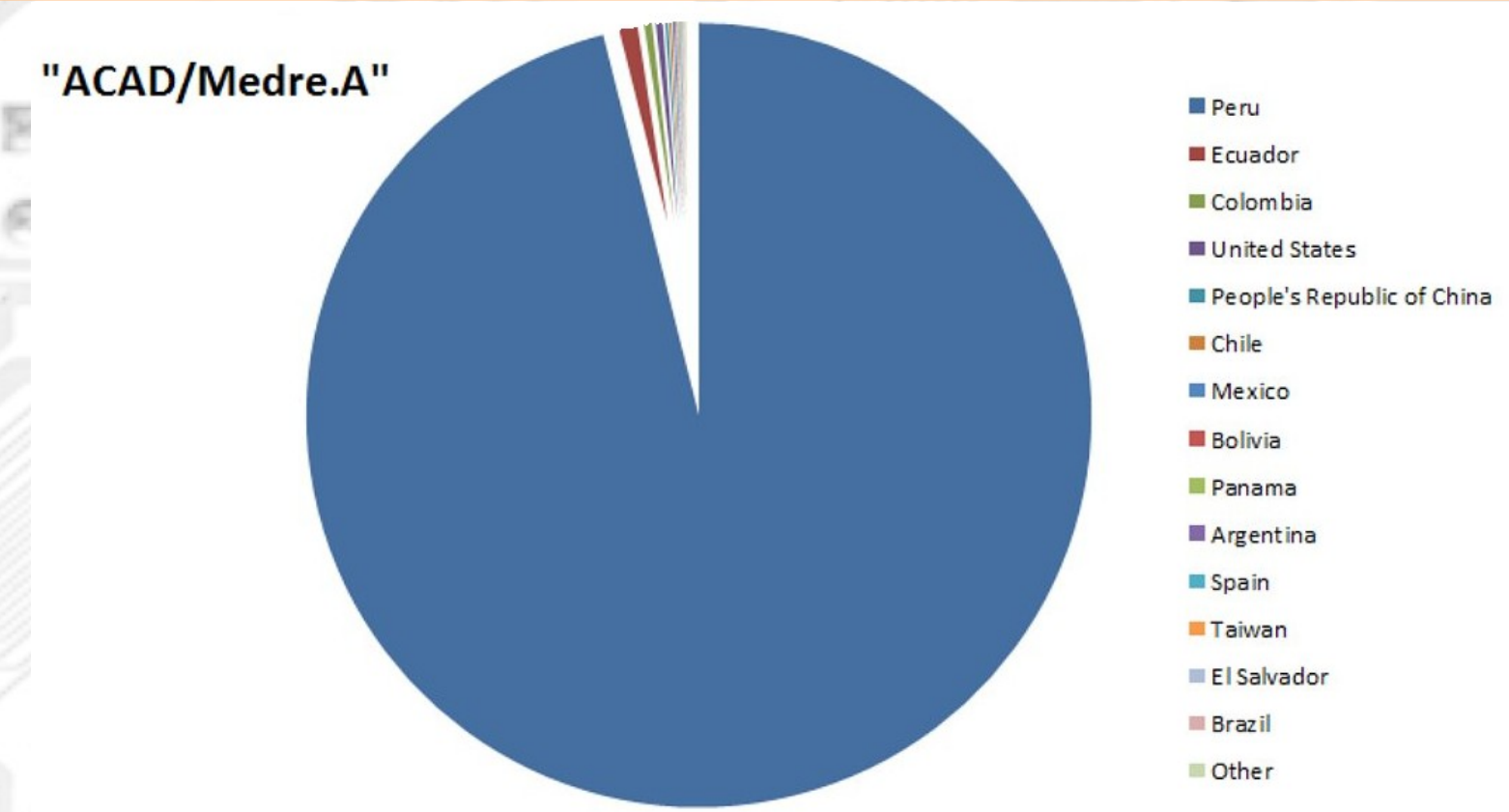
1995. HIPS és Sandbox

- Host-based Intrusion Detection System, host-alapú behatolásmegelőző rendszer
- Figyeli a rendszer aktivitását, meghatározott szabályok szerint azonosítja a szokatlan viselkedést

- A fertőzés megpróbálhatja elkerülni az azonosítást a forráskód értelmezhetetlenné tételével
- A sandbox felfedi a fertőzés eredeti célját és működési mechanizmusát
- Mivel a teljes emulációs folyamat során bináris kódot használ, emiatt gyors

2005. ESET Live Grid

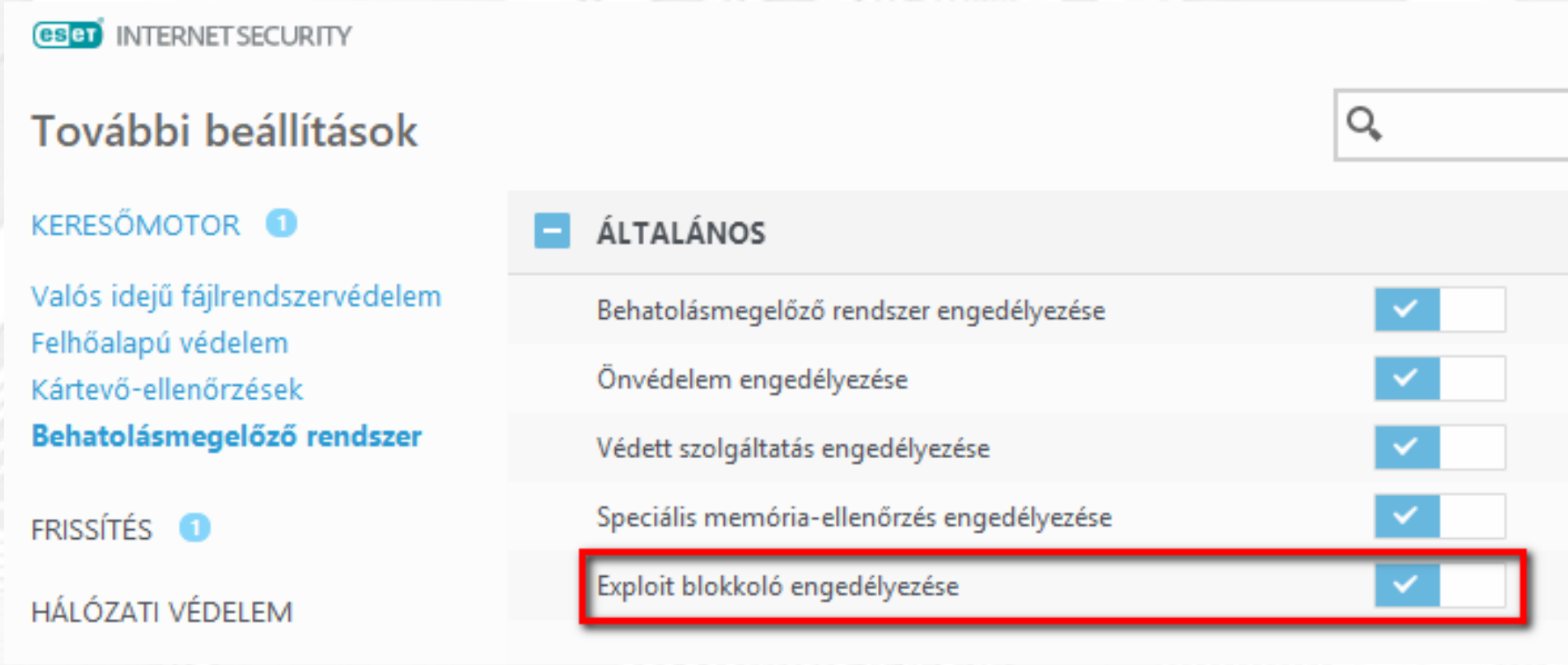
- Gyors védelem az új fenyegetések ellen, felhő alapú rendszer, rövid reakcióidő
- Korai riasztás, azonnali és folyamatos, összegyűjti a gyanús kódok adatait



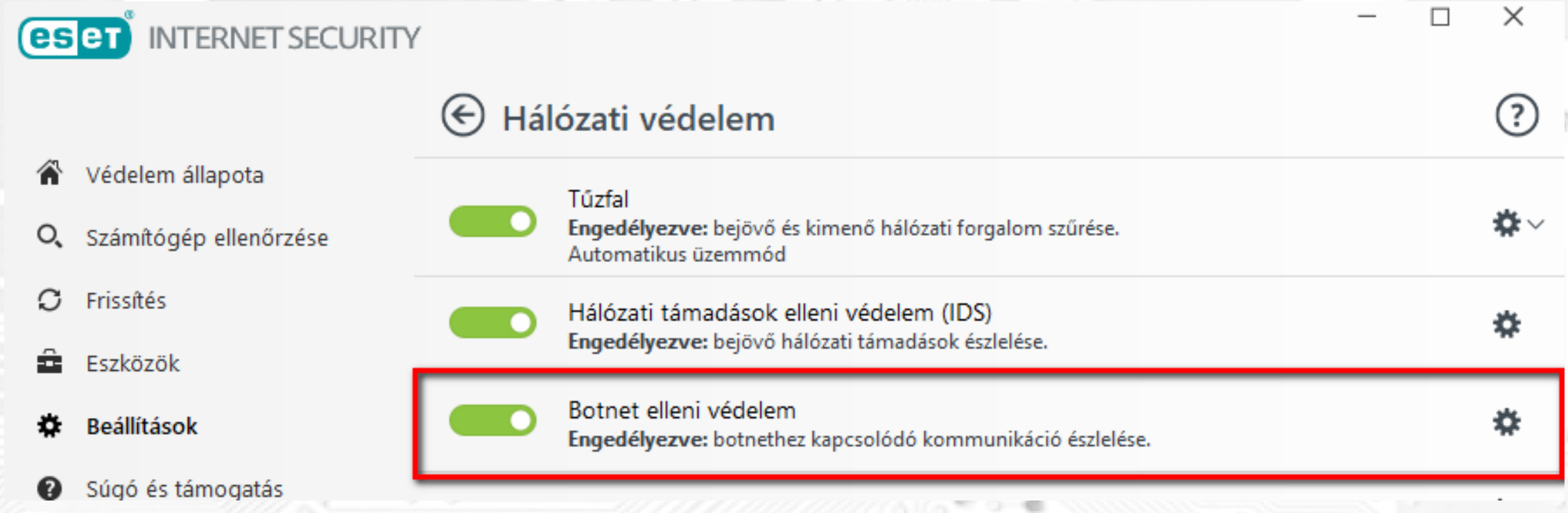
2012. ACAD/Medre, telemetriai rendszer, tömeges AutoCAD áramlás Kínába

- AutoLISP acad.lsp indítóállomány, ingyenes EACADMedreCleaner.exe mentesítő
- 2013. AutoCAD 13 és 14 service pack, futtatható fájlok csak a "TRUSTEDPATHS" útvonalról

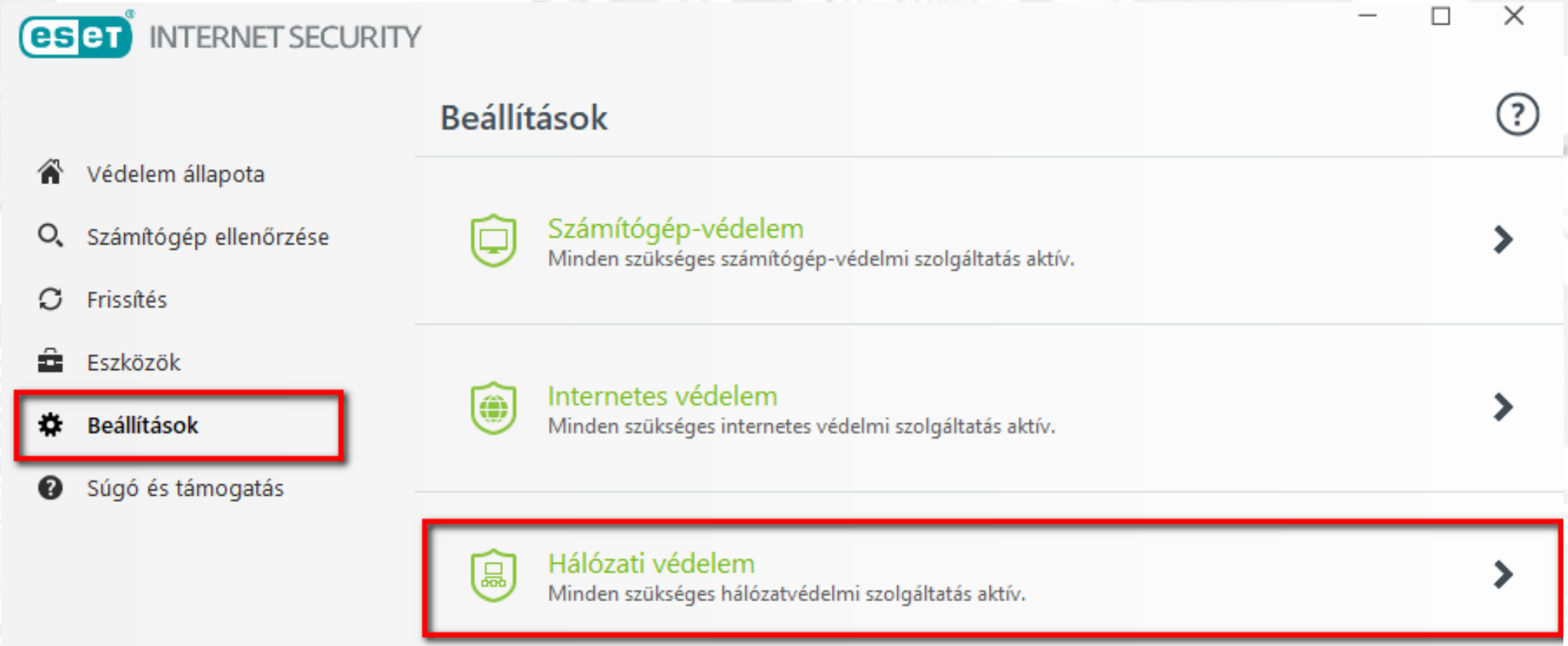
2012. Exploit Blocker



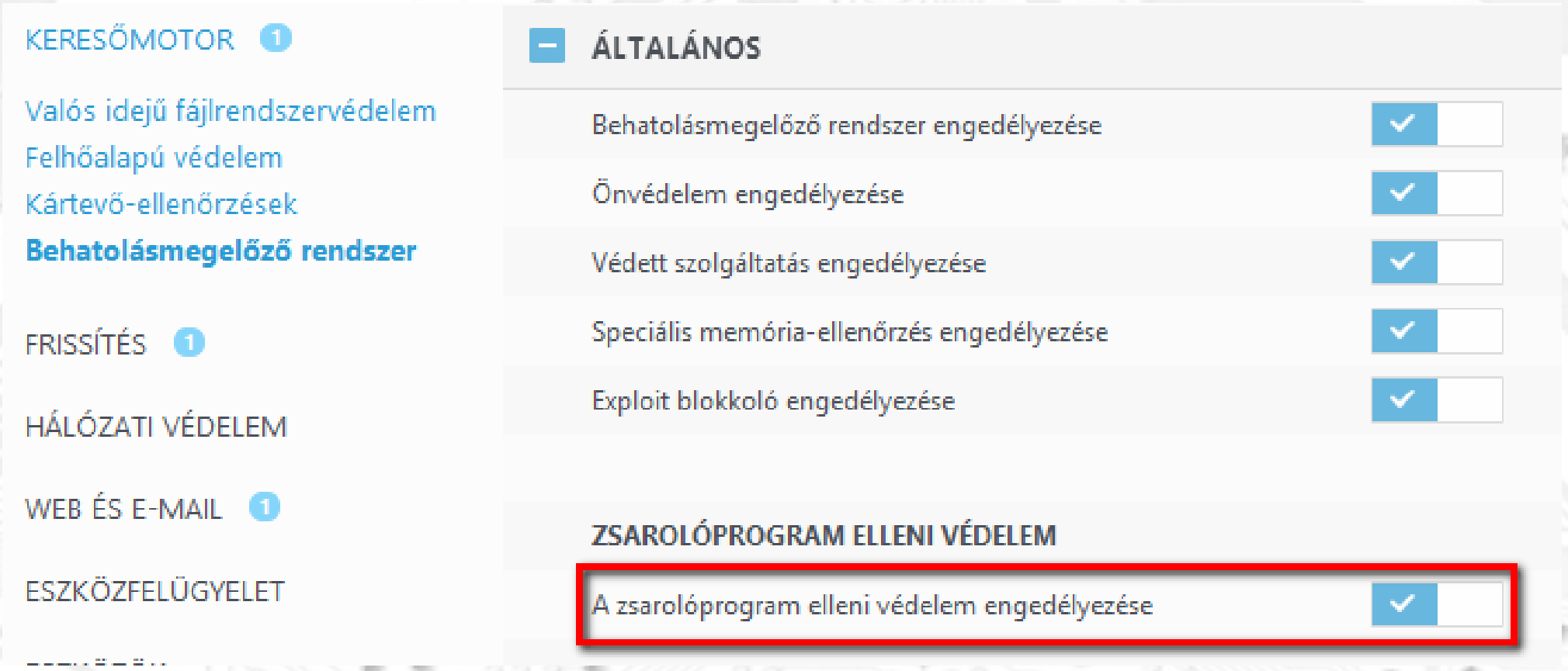
- Gyakran használt alkalmazástípusoknál gyanús folyamatok, pl. zeroday
- Böngészőben, PDF-olvasóban, e-mail kliensben, MS Office összetevőkben, stb.
- Azonnal leállítja az adott folyamatot
- A fenyegetés részletes adatait elküldi az ESET labor ThreatSense felhőrendszerébe



- Észleli a jellegzetes botnetes működést, gyanús vagy rosszindulatú tevékenységét, programokat
- Elemzi a hálózati kommunikációs protokollokat
- Megakadályozza, hogy a számítógépet egy zombihálózathoz csatlakoztassák

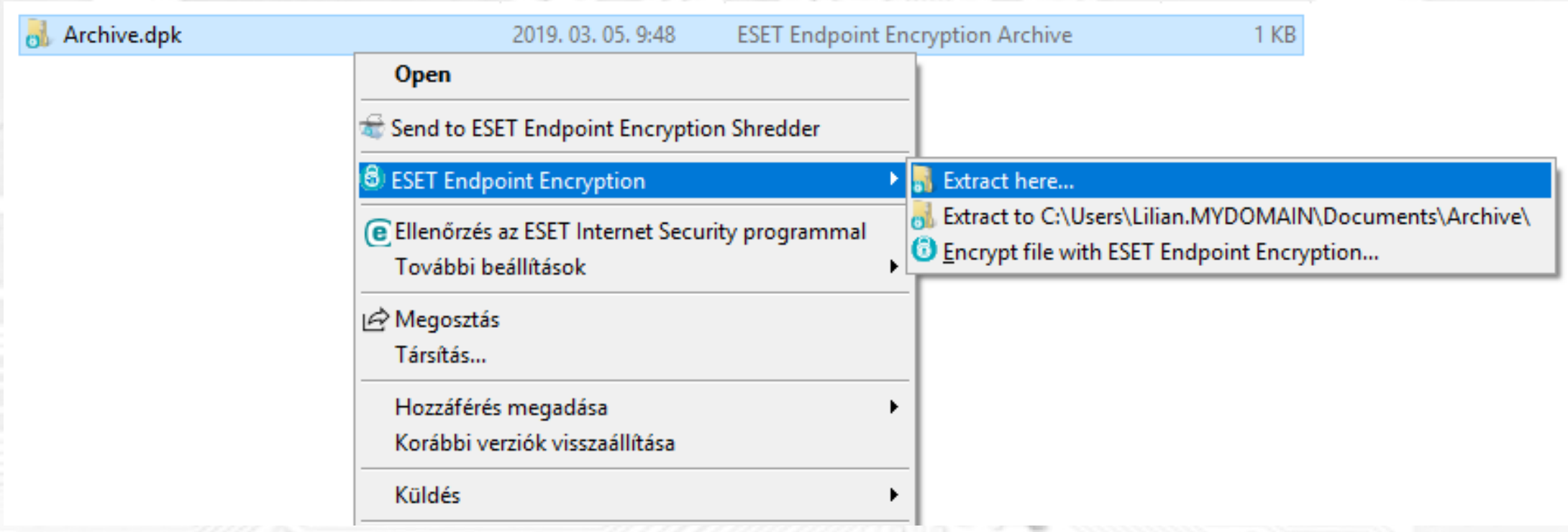


- Tűzfal technológia kiterjesztés, hálózati szinten felismeri az ismert sérülékenységek támadását
- Gyakori protokollok (pl. SMB, RPC, RDP), védelem ismeretlen támadásokkal szemben
- Akkor is, ha a gyártó által kiadott javítás még nem létezik, vagy nincs telepítve

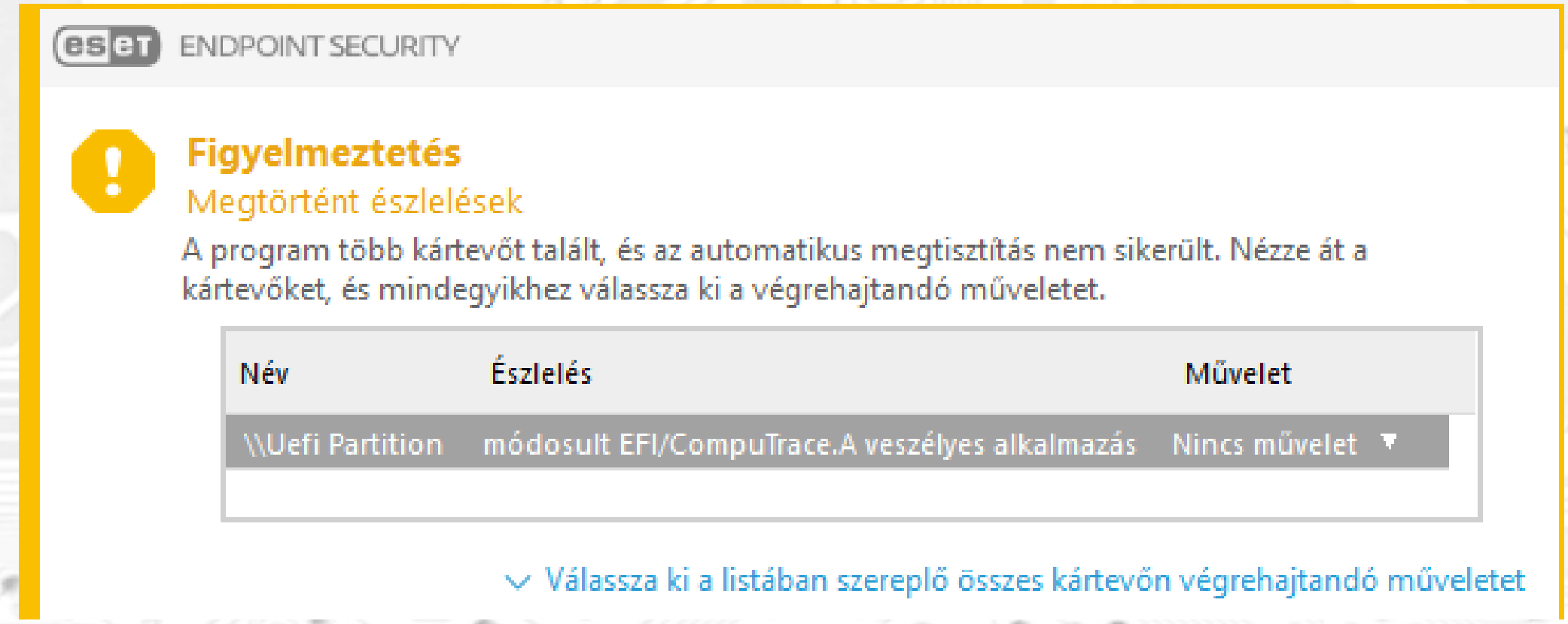


- Viselkedés- és reputáció alapú heurisztika kiértékeli az összes futtatott alkalmazást
- Észleli a jellegzetes viselkedést, pl. tömeges titkosítás, jelez és blokkolja a gyanús alkalmazást
- ESET LiveGrid Reputation Systemnek engedélyezettnek kell lennie hozzá

2017. ESET Endpoint Encryption (korábban DESLock)



- Hatékony adattitkosító megoldás, felhasználóbarát, egyszerűen menedzselhető (GDPR)
- Skálázható eszköz adatszivárgás megelőzéshez
- Biztosítja a végponti titkosítókulcsok, valamint merevlemezekre, hordozható eszközökre és e-mailekre érvényesíthető policy-k központi kezelését



- A V:11-ben Universal Extensible Firmware Interface vizsgálat, szabványos, boot előtti állapot
- Rootkiteknél fizikai hozzáférés kell, túléli az OS újratelepítést vagy a merevlemez cserét
- „Éles” LoJax rootkit a Sednit csoport politikai célpontokat támadó 2018-as akciójában

- **Fejlett és célzott támadások jönnek**

- **Nem létezik 100%-os védelem**

- **De a proaktív és többrétegű védelmi megoldások, felhővel kiegészített technológiák segítenek**

- **Nem érdemes spórolni a biztonságon**

Köszönöm a figyelmet!

csizmazia-darab.istvan@sicontact.hu

www.eset.hu antivirus.blog.hu