SICONTACT™

biztonság a digitális világban

ESET®

Vírusvédelemtől a komplett kiberbiztonságig

SICONTACT
biztonság a digitális világban

Csizmazia-Darab István
Sicontact, IT biztonsági szakértő

Miről lesz szó?

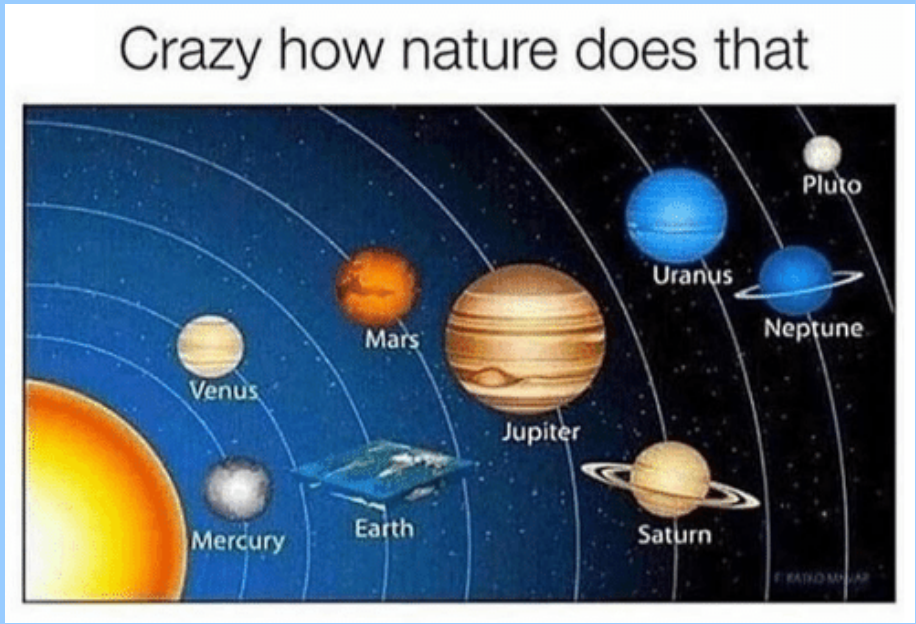
SICONTACT biztonság a digitális világban

Számítógép evolúció

Vírus evolúció

Védelmi evolúció

Összefoglaló



"Ki a múltat háborgatja, folyjon ki a fél szeme.
De ki a múltat elfelejti, annak mind a kettő"
(Alexander Szolzsenicin)

„Az ég kék, a fű zöld, a vírusok, kártevők támadják a sebezhetőségeket.
Népi megfigyelések, amiket az ember elfogad természeti törvénynek.”
(Hanula Zsolt)

Számítógép evolúció

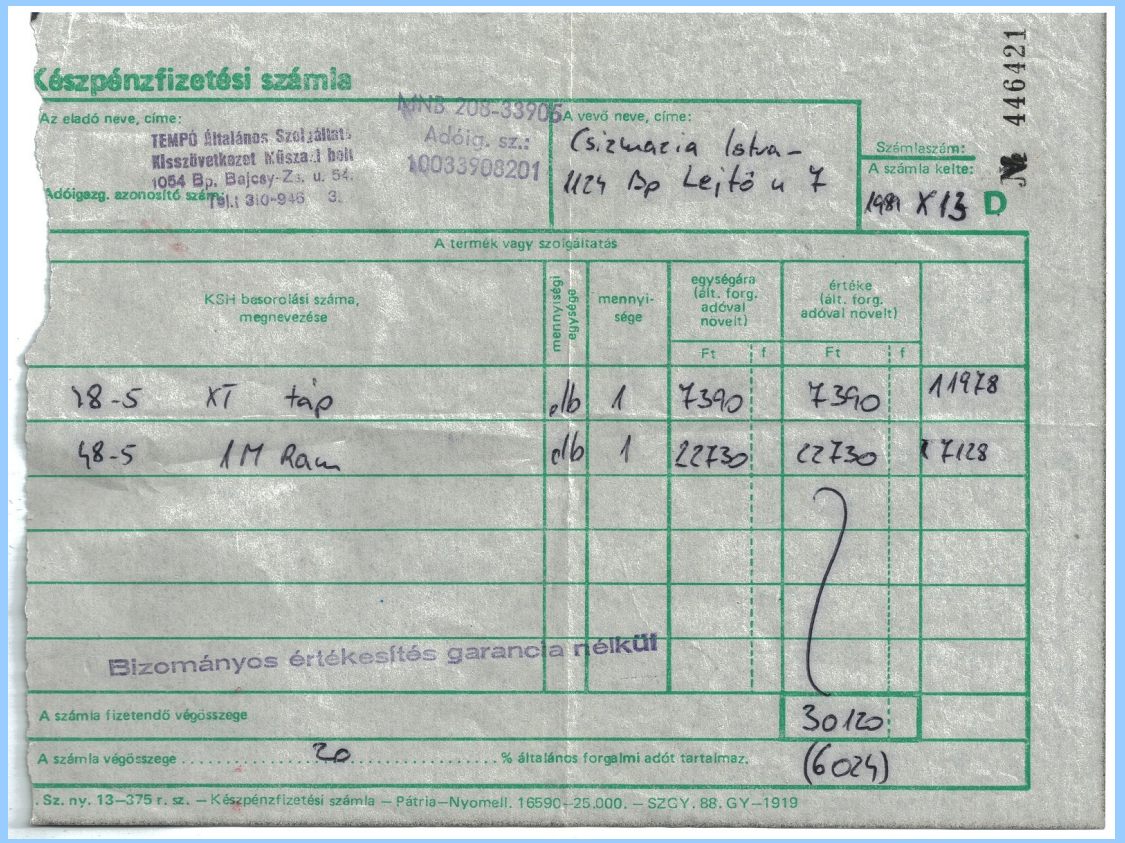
1968. KFKI - TPA
- Tárolt Programú Analizátor (Központi Bizottsági döntés)
- A DEC PDP-8 ötlete nyomán, gyártás a 90-es évekig
- Assembler, FORTRAN
- Perifériák: lyukszalag-olvasó, szalaglyukasztó

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

1979. R20/R40 operátor FÜTI
(Fővárosi Ügyviteltechnikai Iroda)

Számítógép evolúció

- 1981. ZX81, IBM/PC XT
- 1982. Commodore64 USA
- 1982. IBM/PC AT
- 1984. Műszaki Bizományi
- 1985. Intel 386
- 1986. 12.13-14.
  MŰEgyetem BIT-LET Karácsony
- 1989. 1 MB RAM
- 1989. Intel 486
- 1993. Intel Pentium


Készpénzfizetési számla

Az eladó neve, címe:
TEMPÓ Általános Szolgáltató Kisszövetkezet Műszaki bolt
1054 Bp. Bajcsy-Zs. u. 54.
Adóigazg. azonosító szám: Tel.: 310-945 3.

MNB 208-33906
Adóig. sz.: 10033908201

A vevő neve, címe:
Csizmazia István
1124 Bp Leitó u 7

Számlaszám: № 446421
A számla kelte: 1991 X 13 D

A termék vagy szolgáltatás

KSH besorolási száma, megnevezése	mennyiségi egység	mennyisége	egységára (ált. forg. adóval növelt) Ft	f	értéke (ált. forg. adóval növelt) Ft	f	
48-5 XT táp	db	1	7390		7390		11978
48-5 1M Ram	db	1	22730		22730		17128
Bizományos értékesítés garancia nélkül							
A számla fizetendő végösszege					30120		
A számla végösszege ..... 20 ..... % általános forgalmi adót tartalmaz.					(6024)		

. Sz. ny. 13–375 r. sz. – Készpénzfizetési számla – Pátria–Nyomell. 16590–25.000. – SZGY. 88. GY–1919

Számítógép evolúció

1997. Deep Blue Vs Kasparov - 4:2
- 259-ik szuperszámítógép a TOP500 listán
- 11.38 GigaFlops teljesítmény
  (High-Performance LINPACK teszt)

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

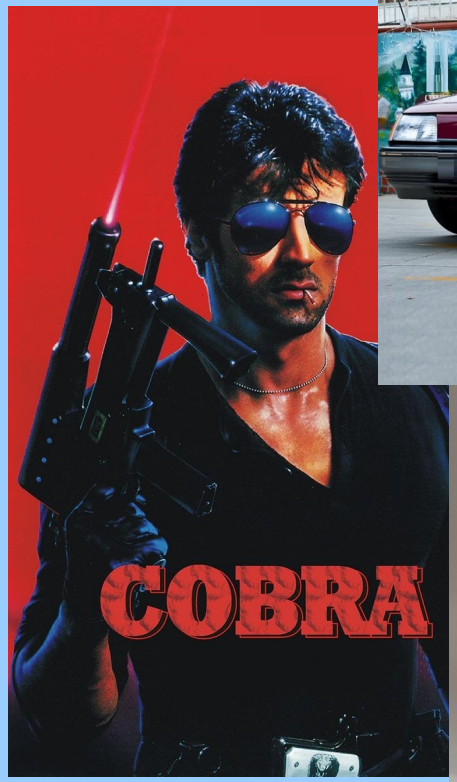
2016. Google DeepMind Challenge Match
- Az AlphaGo megveri a legjobb go játékost,
  a dél-koreai Lee Sedolt 4:1

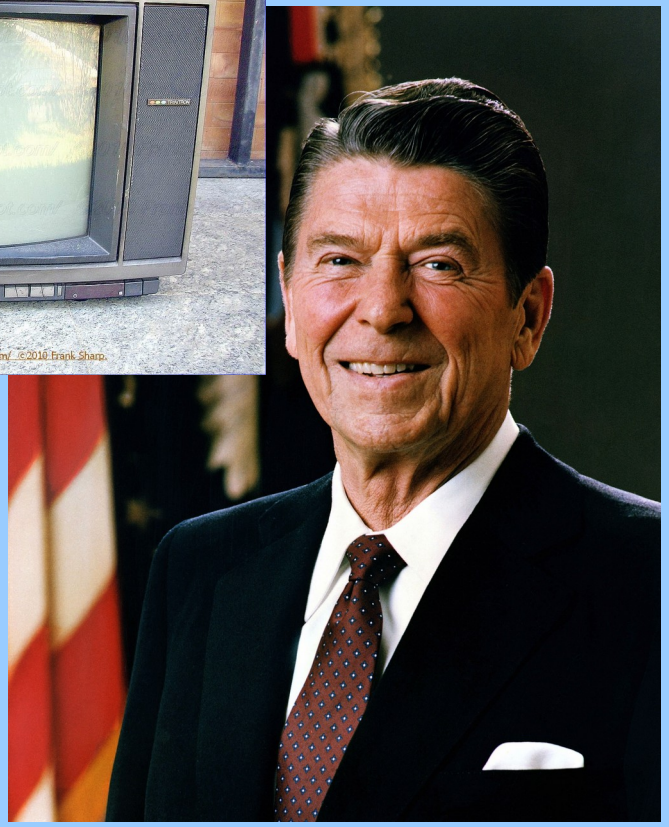
2018. 7.6 mrd netező, 23.14. mrd netes eszköz (Internet World Stats, Statista)

Vírus evolúció

SICONTACT biztonság a digitális világban

1986. Az USA elnöke: Ronald Reagen
- Super Bowl döntő: Chicago vs New England (46-10)
- Wimbledon: Navratilova-Mandlikova (7-6 6-3), Becker-Lendl (6-4 6-3 7-5)
- Stallone Cobra, Ford Taurus





Vírus evolúció

SICONTACT biztonság a digitális világban

1986. Az első C64 vírus: BHP
- BASIC-ben és SYS assembly hívással
- floppyról floppyra terjedt
- az ILOAD, az ISAVE, a MAIN, az NMI, a CBINV és a RESET vektorokhoz kapcsolódott
- Run/Stop-Restore-proof volt

Vírus evolúció

SICONTACT biztonság a digitális világban

1986. január - 0 kilométerkő
IBM PC-re írt Brain vírus, Lahore, Pakisztán
Név, cím, telefonszám a kódban: Farooq Alvi és Amjad Farooq Alvi
- lopakodó mechanizmust használt
- 5 1/4 collos floppy lemezeken a boot rekordot fertőzte felülírással
- egy hét alatt szétterjedt a világon
- Mikko Hyppönen látogatás tett náluk a 25 éves évfordulón
- 2011-ben még ugyanott laktak :)))

"Welcome to the Dungeon
© 1986 Basit & Amjad (pvt) Ltd.
BRAIN COMPUTER SERVICES
730 NIZAB BLOCK ALLAMA IQBAL TOWN
LAHORE-PAKISTAN
PHONE :430791,443248,280530.
Beware of this VIRUS....
Contact us for vaccination..... $#@%$@!!"

Vírus evolúció

1988. Cascade-1701

III. ÉVFOLYAM 25. SZÁM
1988. DECEMBER 14.

MONITOR 9

Hozzászólás vírusügyben

1988.12.14.

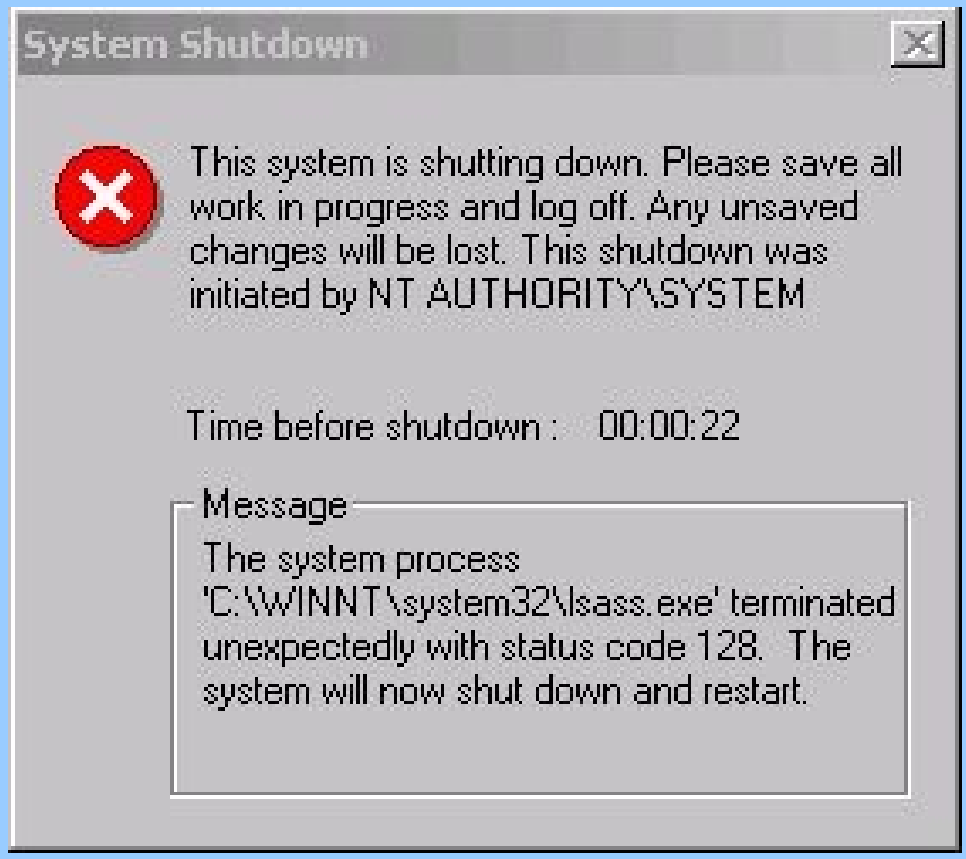
F(ind) funkcióját kell meghívni, és a következő hexa-sorozatot keresni: 01 FA 8B EC E8 00 00 5B 81 EB. Először a winchestert, majd utána minden egyes hajlékonylemezünket végig kell vizsgálni. Ha találtunk ilyen karaktersorozatot, az egyértelműen jelzi, hogy ... lemezünk. Az érint...

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

Vírus evolúció

2003. SQL Slammer flashworm
- csak hálózati csomagokban terjedt
- MS 2002-es javítócsomag
- nincs fájl, hálózatról a memóriába töltődött
- az akkori antivírusoknak itt esélye sem volt
- az első félórában 75 ezer gép esett el
- kb. 750 millió USD kár



Vírus evolúció

SICONTACT biztonság a digitális világban

2007.03. Windows 2000, XP, és Vista
- ANI animált kurzor vírus
- patch: 2007.04.03.

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

c|net BEST PRODUCTS REVIEWS NEWS VIDEO HOW TO SMART HOME CARS DEALS

MOBILE

Windows animated cursor attack

The way Microsoft Windows handles animated cursors on Web sites puts PCs at risk.

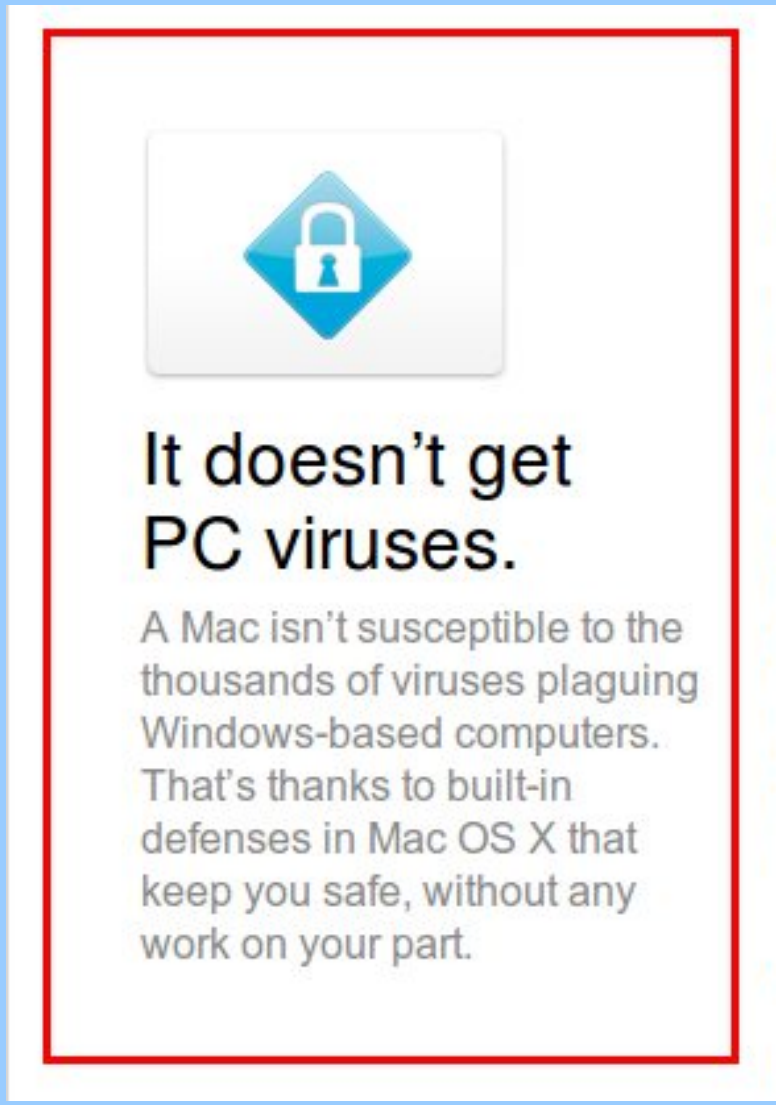
BY ROBERT VAMOSI / APRIL 10, 2007 10:25 AM PDT

There's a new Microsoft Windows vulnerability being exploited across the Internet on over 100 Web sites, according to security vendor Websense. The vulnerability is caused by an unspecified error in the way Windows 2000, XP, and Vista handles animated cursors. Animated cursors allow a mouse pointer to appear animated on a Web site. The feature is often designated by the .ani

Vírus evolúció

No Platform is Safe - sebezhetőségek mindenhol

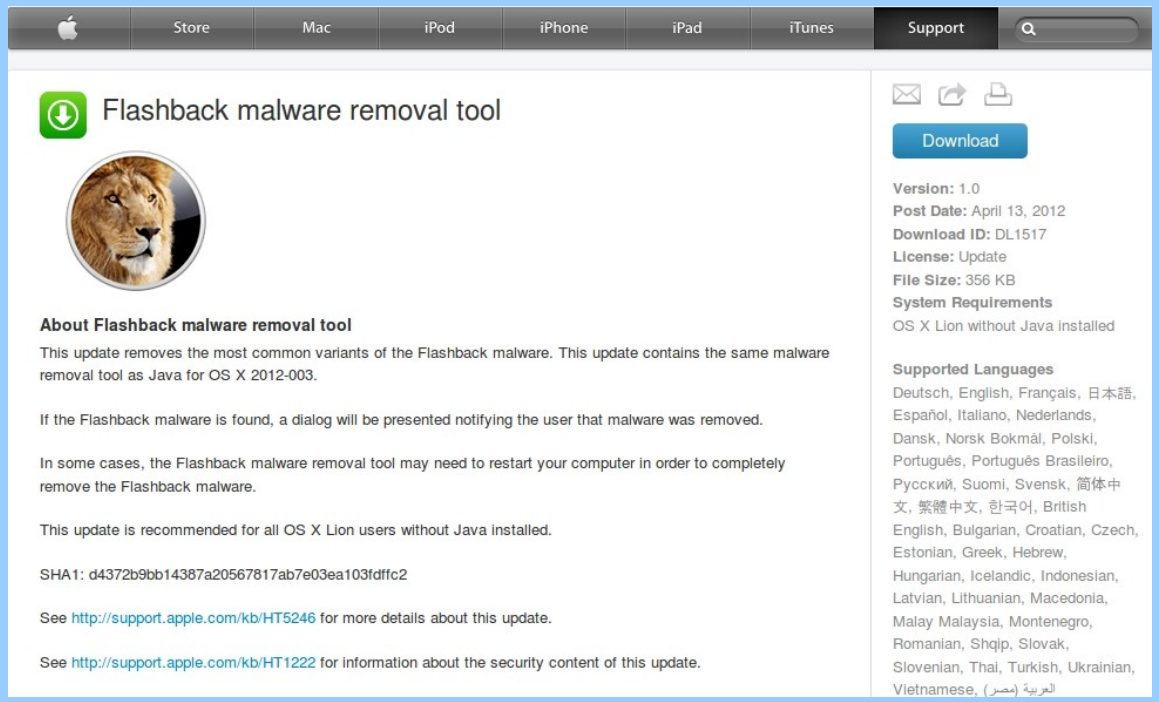
A Macintosh sem "érinthetetlen"
- 2012-ig: "Itt nincsenek vírusok"



Vírus evolúció

SICONTACT biztonság a digitális világban

- 2012. március 600 ezer OS X Flashback botnet
- Egyes változatok közbeavatkozás nélkül is terjedtek
- Java sebezhetőséget használt ki
- **2012.04.13.**
  "Flashback Malware Removal Tool" frissítés



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

Vírus evolúció

SICONTACT biztonság a digitális világban

2013. KITM = "Kumar in the Mac" trójai

- kémked, képernyőfotókat készít, távoli C&C
- 2012. 10.8-as Apple Gatekeeper Execution Prevention technológia
- megkerülés, érvényes Apple Developer ID (Rajender Kumar névre)
- visszavonták, de ez a már megfertőződött áldozatoknak nem segített
- ha a kártevő átjutott a Gatekeeperen, nincs újra ellenőrzés
- csak a vírusvédelmi alkalmazás segíthet

Vírus evolúció

SICONTACT biztonság a digitális világban

- 2014. SimpLocker Android, 260 ukrán Hrivnya, AES, TOR, ZIP, új verzió 7z és RAR is

- 2015. Linux/BSD Mumblehard botnet szervereken

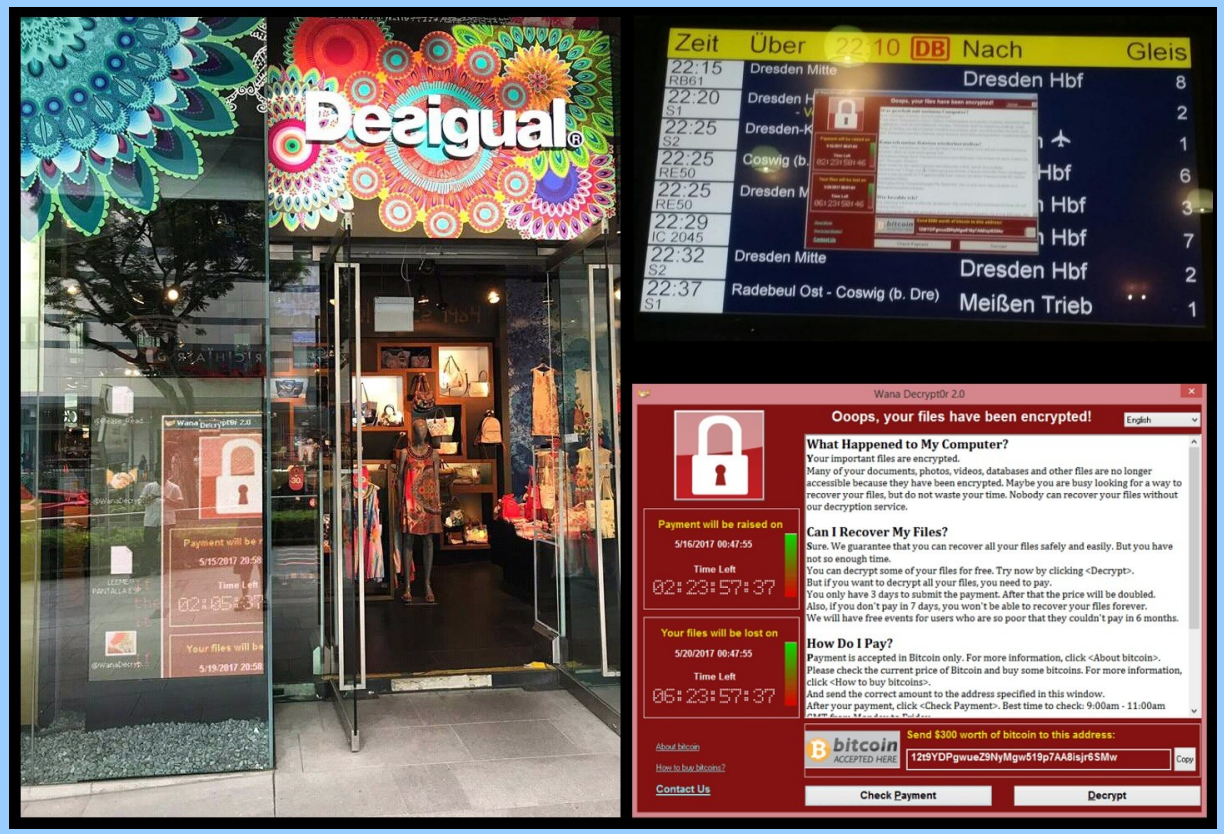
- 2016. OpenSSH 12 éves CVE-2004-1653 bug (router, NAS, CCTV, DVR, IoT, stb.)

- 2016. Samsam ransomware javítatlan Red Hat JBoss vállalati szerverek

Vírus evolúció

SICONTACT biztonság a digitális világban

- 2016: Ransomware növekedés 6000% (IBM)
- 2017. 6 in 10 malware payloads were ransomware in Q1 (Barkly Statistics)
- 2017 Ransomware earned its creators $25 million 2015-2016. (Source: Business Insider)
- The average ransom demand has risen to $1,077
- 1 in 5 businesses that paid the ransom never got their files back



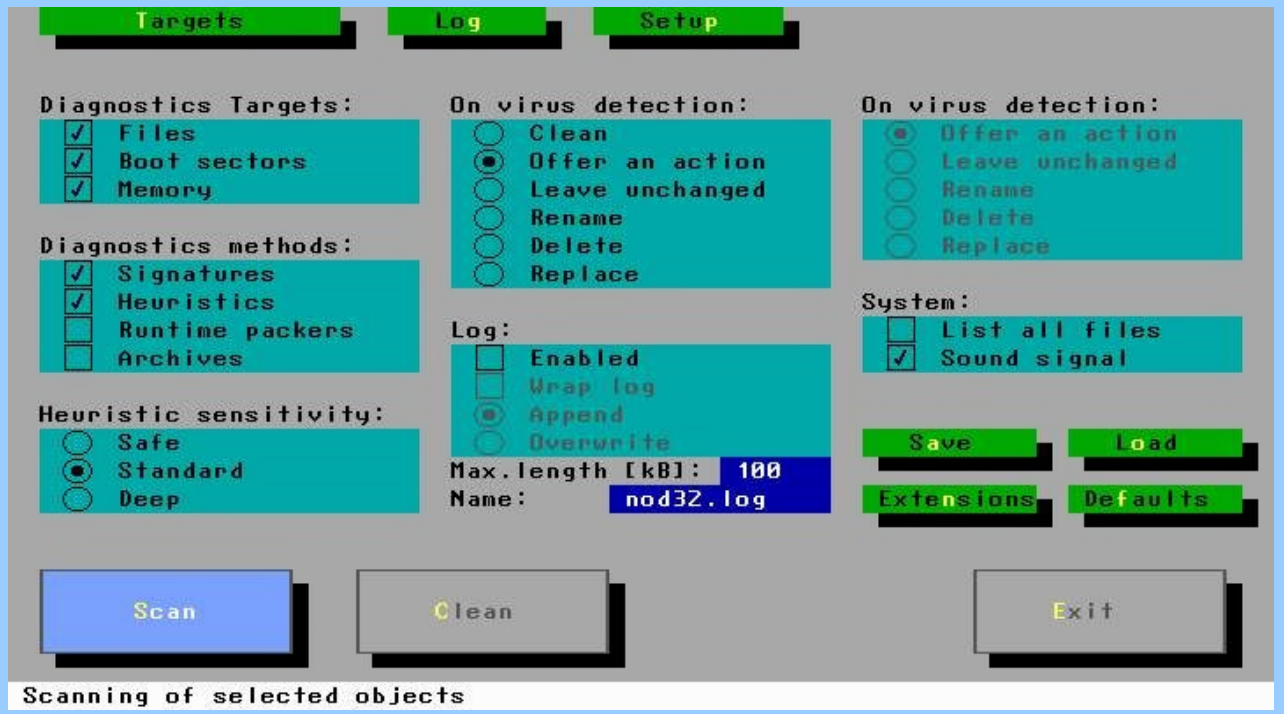
Vírus evolúció

2018.
- Nem az internet tönkretétele a cél
- hanem a fertőzött gépről adatlopás, váltságdíj szedés, illetve zombivá változtatás
- Nearly 40 percent of ransomware victims paid the ransom. (Source: Malwarebytes)
- The average ransomware demand in 2017 was half of what it was in 2016, changing from over $1,000 on average to $522. (Source: Symantec)
- Ransomware is costing businesses more than $75 billion per year. (Source: Datto)

Védelmi evolúció

SICONTACT biztonság a digitális világban

1987. A legelső NOD verzió megjelenése (Peter Paško, Miroslav Trnka)



Védelmi evolúció

SICONTACT biztonság a digitális világban

1995. ESET Heurisztika és viselkedés elemzés, sandbox

- proaktív technikák használata, virtuális kódemuláció, heurisztikus felismerés
- rendkívül erős heurisztikai képességek (pl. rootkit)
- új, ismeretlen kártevők ellen
- minimális számú téves vakriasztás
- A kiterjesztett heurisztikával (Advanced Heuristics) indult az ESET-nél a gépi tanulás (ML) alkalmazása
- Nem csodaszer, hiszen folyamatosan szükséges az állandó emberi megerősítés az osztályozás során

Védelmi evolúció

SICONTACT biztonság a digitális világban

1995. ESET Heurisztika és viselkedés elemzés, sandbox

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

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

Védelmi evolúció

2005. Live Grid
- korai riasztási rendszer, az ESET azonnal és folyamatosan értesül az új fertőzésekről
- hatékonyabb védelmet biztosít a felhasználóknak
- összegyűjti a számítógép újonnan észlelt kártevőkkel kapcsolatos adatait
- segíti a keresőmotorok folyamatos frissítését
- a felhő alapú rendszer reakcióideje igen rövid
- gyorsan képes védelmet nyújtani újonnan felbukkanó fenyegetések ellen

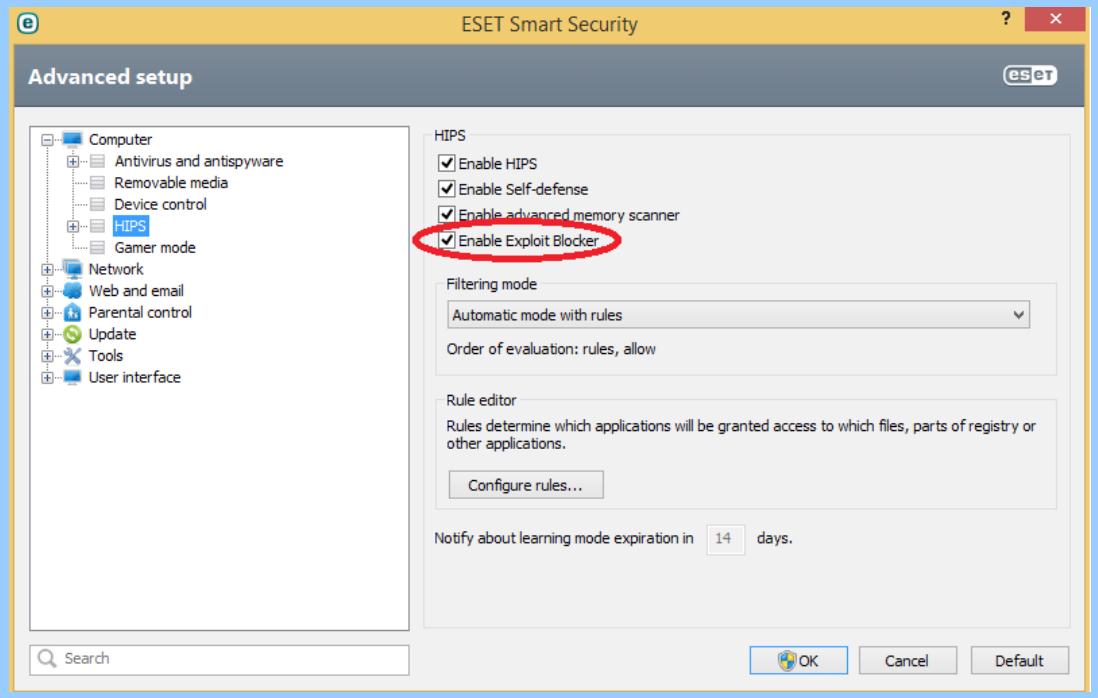
2012. ACAD/Medre
- a telemetriai rendszer szokatlan jelenséget észlelt Peruban
- tömeges AutoCAD rajzok áramlása Kínába, szellemi tulajdon, szabadalmak
- a fertőzés az AutoLISP acad.lsp indítóállományát támadta meg
- ESET felismerés + ingyenes EACADMedreCleaner.exe mentesítő program
- 2013. AutoCAD 13 és 14 service pack, futtatható fájlok csak a "TRUSTEDPATHS" útvonalról

Védelmi evolúció

SICONTACT biztonság a digitális világban

2012. Exploit Blocker

- a gyakran használt alkalmazástípusoknál megfigyeli a gyanús tevékenységeket, folyamatokat
- pl. egy nulladik napi kihasználható hiba kapcsán
- pl. webböngészőkben, PDF-olvasókban, e-mail kliensekben, MS Office összetevőkben
- Ha ilyennel találkozik, akkor azonnal leállítja az adott folyamatot
- rögzíti a fenyegetés részletes adatait, majd elküldi a ThreatSense felhőrendszerébe
- az ESET labor feldolgozza és felhasználja az ismeretlen fenyegetések azonosítására és a támadások védelmére

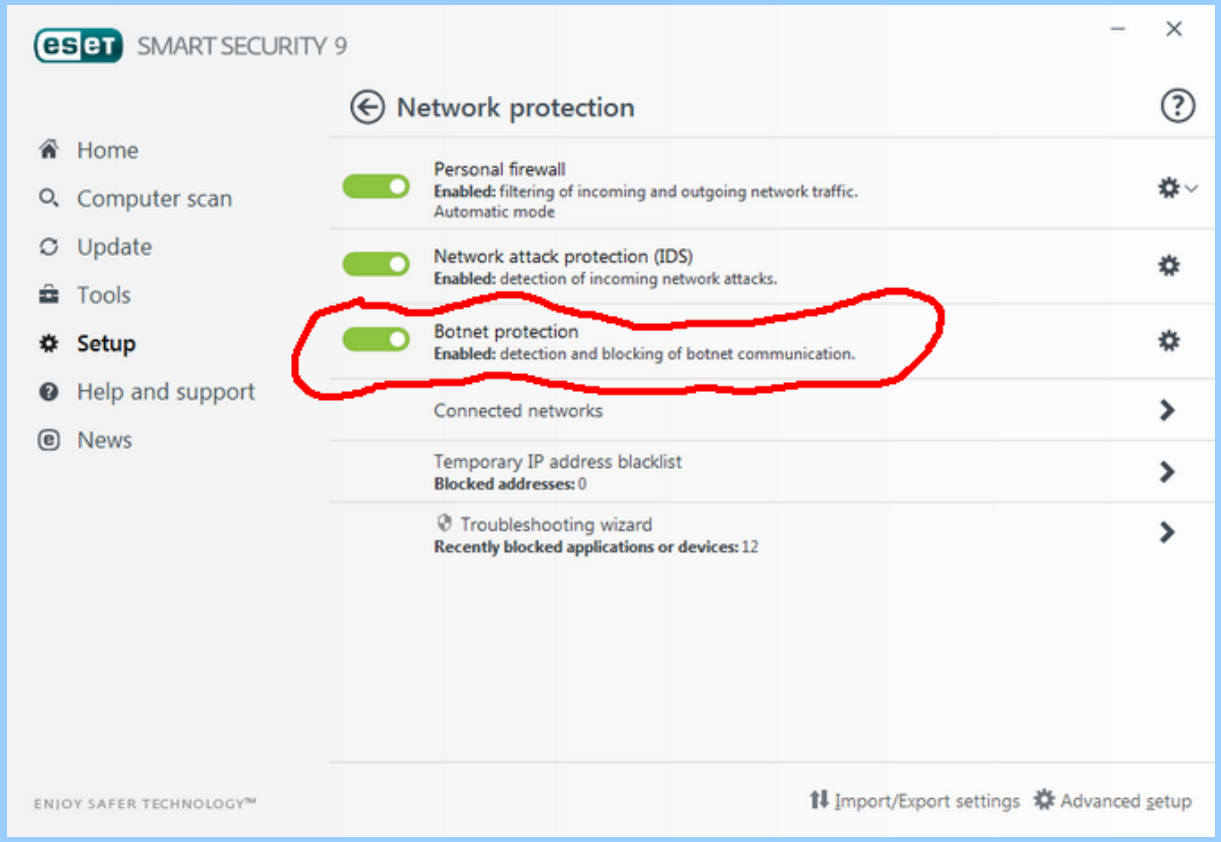


Védelmi evolúció

SICONTACT biztonság a digitális világban

2014. Botnet Protection

- A védelem észleli a zombihálózatokkal kapcsolatos kártékony programokat
- részletesen elemzi a hálózati kommunikációs protokollokat
- felismeri a jellegzetes botnetes működést, gyanús vagy rosszindulatú tevékenységét
- megakadályozza, hogy a számítógépet egy zombihálózathoz csatlakoztassák

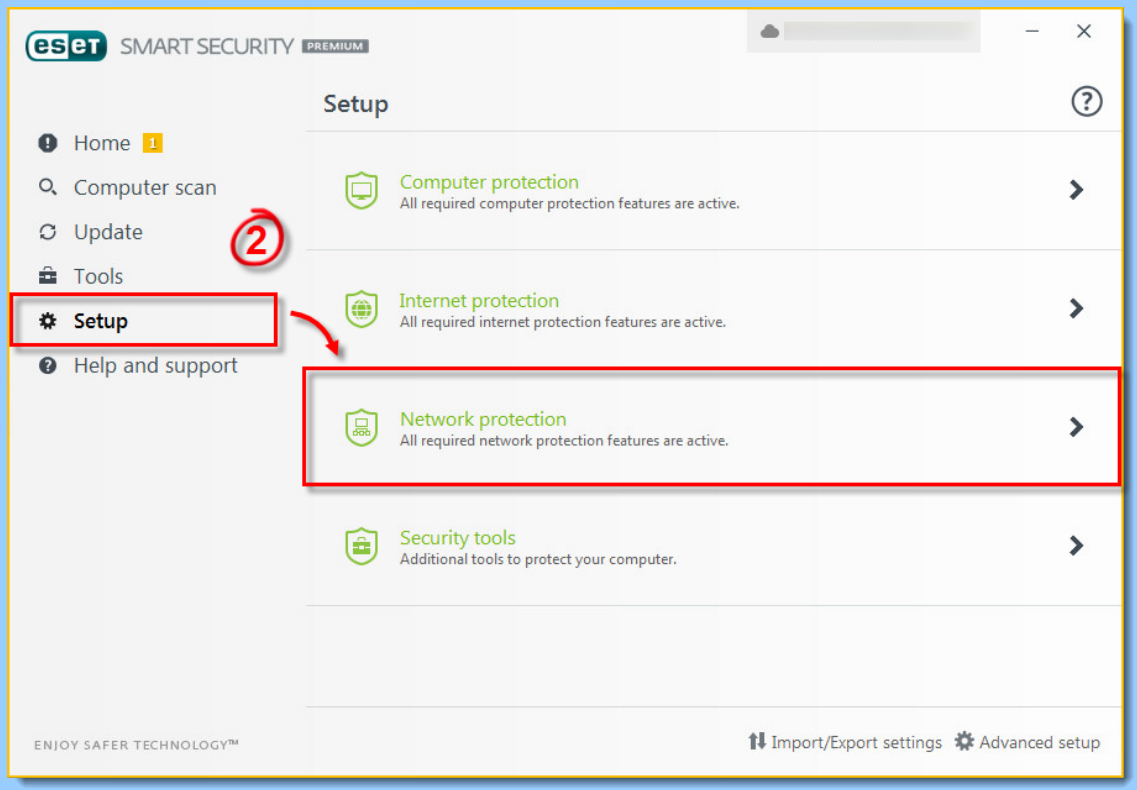


Védelmi evolúció

SICONTACT biztonság a digitális világban

2015. Hálózati támadások elleni védelem

- A tűzfal technológia egy kiterjesztése
- hálózati szinten javítja az ismert sérülékenységeket célzó támadások felismerését
- A széles körben használt protokollokat (pl. SMB, RPC vagy RDP) figyeli
- védelmet nyújt az még ismeretlen kártevők terjedésével és hálózati támadásokkal szemben
- ha a gyártó által kiadott javítás még nem létezik, vagy nincs telepítve



Védelmi evolúció

SICONTACT biztonság a digitális világban

2017. ESET Endpoint Encryption (korábban DESLock)
- Egyszerű és hatékony adattitkosító megoldás KKV-k és nagyvállalatok számára
- Könnyen használható, felhasználóbarát és egyszerűen menedzselhető titkosítás
- skálázható, rugalmas, könnyen adaptálható
- biztosítja a végponti titkosítókulcsok, valamint merevlemezekre, hordozható eszközökre és e-mailekre érvényesíthető policy-k központi kezelését
- hatékonyan felléphetünk az adatszivárgás megelőzése érdekében
- biztosítja a követelményeknek (pl. GDPR) való megfelelést

Vállalati > Végpontvédelem > ESET Endpoint Encryption titkosítás

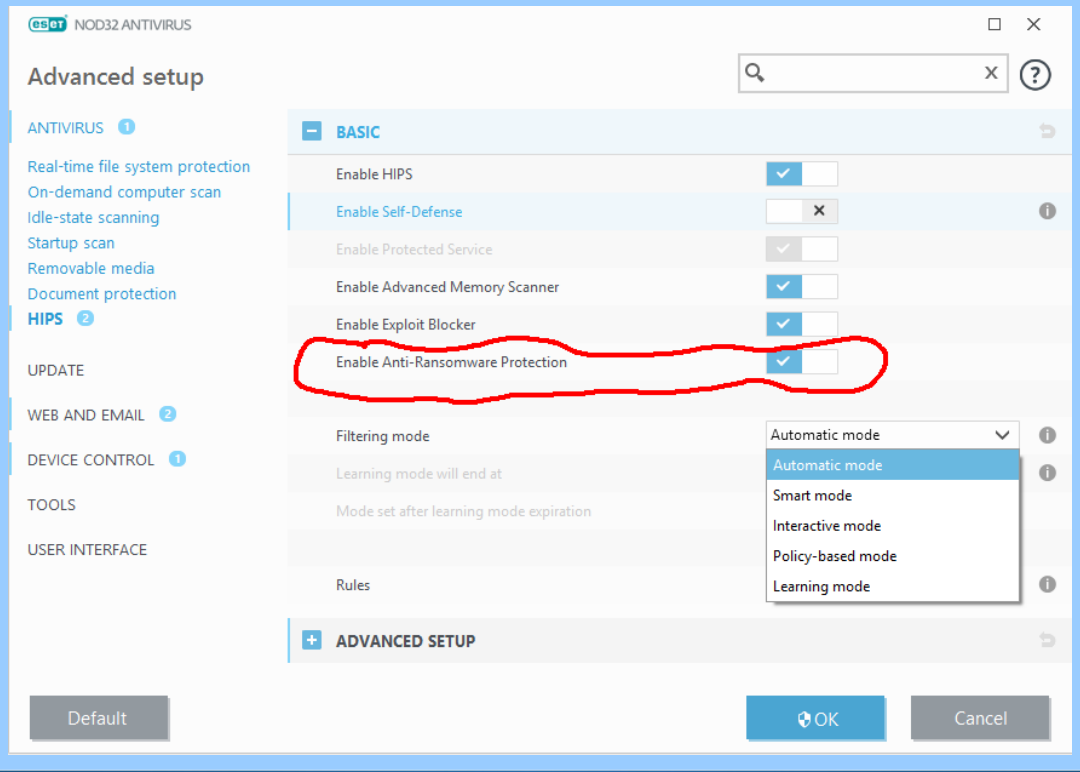
	Essential Edition	Mobile Edition	Standard Edition	Pro
Teljes merevlemez titkosítás	–	–	–	✓
Cserélhető adathordozók titkosítása	–	–	✓	✓
Go Portable titkosítás	–	–	✓	✓
Fájl- és könyvtártitkosítás	✓	✓	✓	✓
Outlook bővítmény - email és csatolmány titkosítás	✓	✓	✓	✓
Szöveg és vágólap titkosítás	✓	✓	✓	✓
Titkosított virtuális kötetek és tömörített állományok	✓	–	✓	✓
Központi menedzsment	✓	✓	✓	✓

Védelmi evolúció

SICONTACT biztonság a digitális világban

2017. Antiransomware

- a ransomware elkódolja a felhasználók adatait, virtuális valutában váltságdíjat követel
- a védelmi modul a viselkedés- és reputáció alapú heurisztika segítségével figyel
- kiértékeli az összes futtatott alkalmazást, észleli a zsarolóvírusra utaló viselkedést
- Észleli, ha a meglévő állományokon engedély nélküli módosításokat eszközölnek
- pl. fájlok tömeges titkosítása, jelez a felhasználónak és blokkolja a gyanús alkalmazást
- a működéshez az ESET LiveGrid® Reputation Systemnek is engedélyezettnek kell lennie



Védelmi evolúció

SICONTACT biztonság a digitális világban

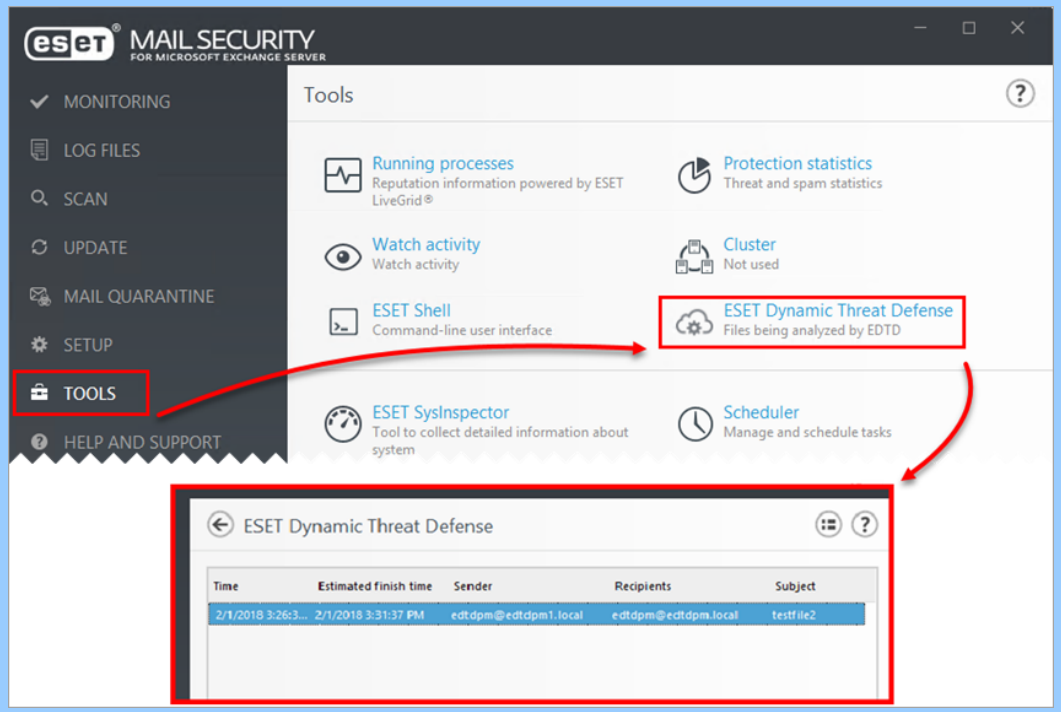
2017. 100-ik VB100

- A NOD32 századik alkalommal nyerte el a Virus Bulletin Virus Bulletin 100% díját
- erre egyetlen más vírusírtó termék sem volt képes eddig a világon
- A VB Award az egyik legelismertebb független, biztonsági szoftverek tesztelésével foglalkozó szervezet
- szigorú tesztelési rendszer - pl. tiltott a tesztelés ismétlése
- úgy kell 100%-osan felismerni az aktuális "WildList" lista kártevőit, hogy közben nem okozhatnak vakriasztást (false positive)
- a teszt emellett számos más hasznos, sebességbeli és teljesítmény mutatókat is közöl

Védelmi evolúció

SICONTACT biztonság a digitális világban

2018. ESET Dynamic Threat Defense
- a feltöltött, új és ismeretlen állományokat egy Sandbox technológiával vizsgálja
- tartalmuk és nem fájlkiterjesztésük alapján
- a vállalati termékek tudnak vizsgálatra küldeni gyanús programállományokat (max. 64 MB)
- Éves díjjal külön licencként vásárolható, a kívánt gépekre aktiválni kell
- 205 végpontnál nagyobb hálózatok számára
- egy plusz védelmi réteget és egy automata riportot ad a megvizsgált állományokról
- könnyen kezelhető, a központi távadminisztrációs felületről lehet nyomon lehet követni

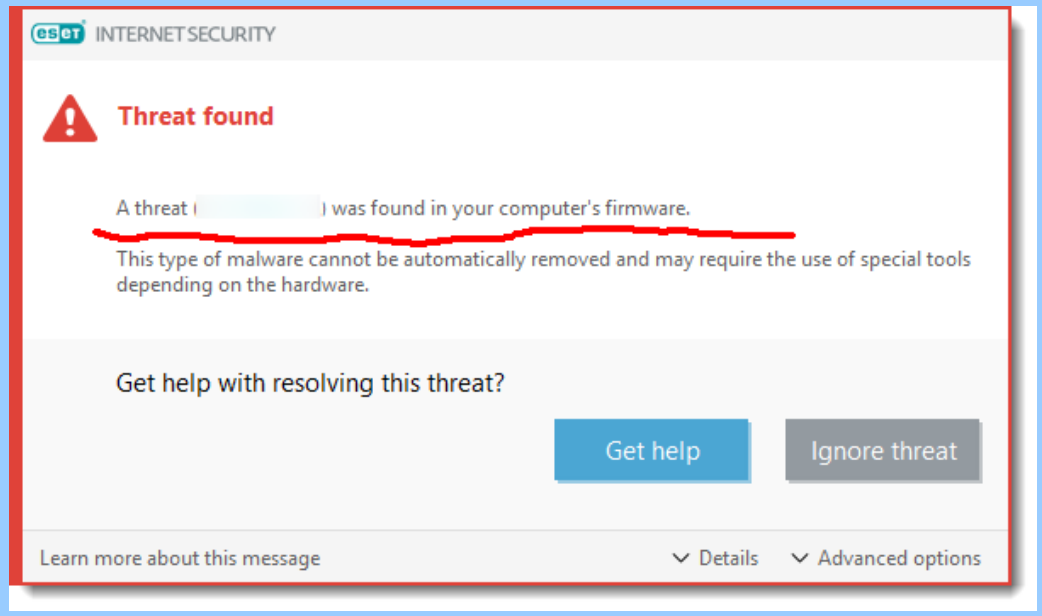


Védelmi evolúció

SICONTACT biztonság a digitális világban

2018. UEFI Scanner - V:11

- Az UEFI (Universal Extensible Firmware Interface, a BIOS utódja) vizsgálata
- ellenőrzi a számítógép firmware-jét
- szavatolja az UEFI szabványos, boot előtti rendszerkörnyezet érintetlenségét, biztonságát
- A fejlett rosszindulatú rootkiteket képes felismerni
- ezeknél a támadóknak fizikailag is hozzá kell férniük a célba vett számítógéphez
- ha sikerült, akkor nehezen ismerhetők fel a fertőzés jelei
- képesek túlélni az OS újratelepítést vagy a merevlemez cseréjét
- A LoJax rootkit a Sednit csoport politikai célpontokat támadó akciójában tűnt fel élesben
- Az ESET az egyetlen, amely dedikált védelmi modullal bővítette a vírusvédelmi termékeit

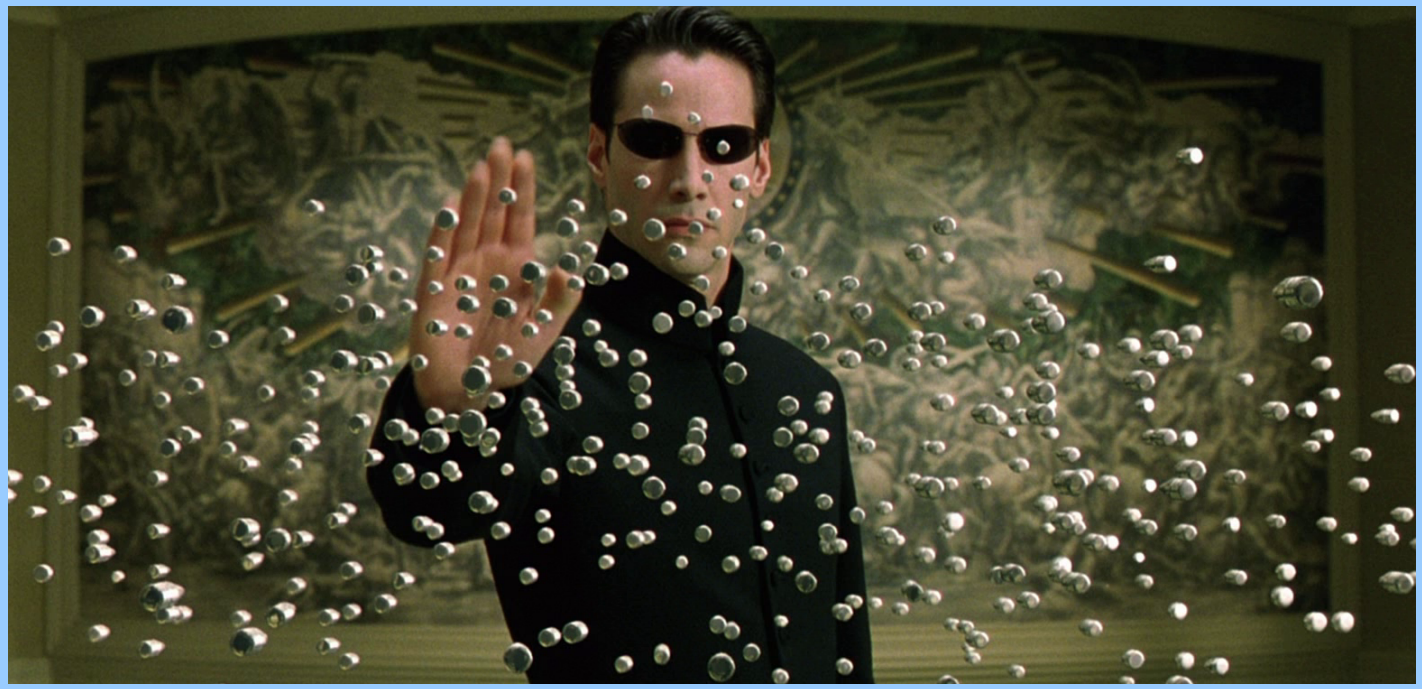


Összefoglaló

SICONTACT biztonság a digitális világban

KONKLÚZIÓ

- egyre fejlettebb, és sokszor célzott támadások
- nem létezik 100%-os védelem
- de a proaktív és többrétegű védelmi megoldások, felhővel kiegészített technológiák segíthetnek



Köszönöm a figyelmet!

csizmazia.istvan@sicontact.hu