

SICCONTACT ™

biztonság a digitális világban



Vírusvédelemtől a komplett kiberbiztonságig



Csizmazia-Darab István
Sicontact, IT biztonsági szakértő

Miről lesz szó?

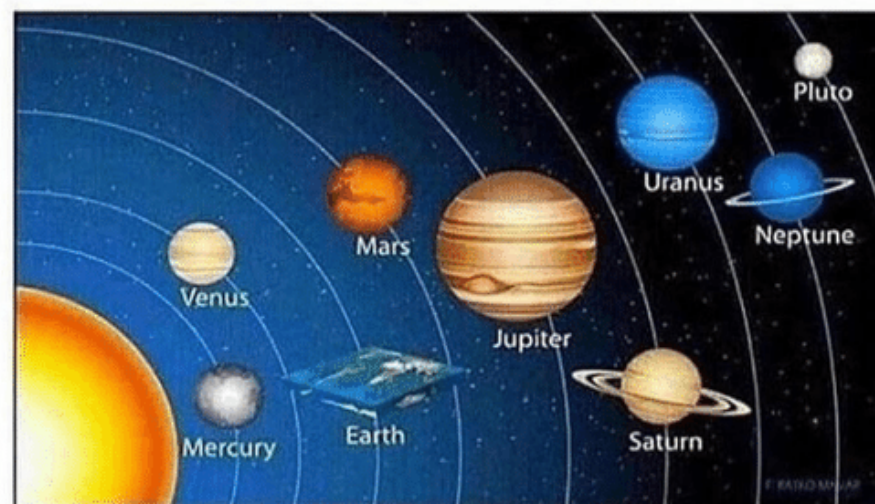
Számítógép evolúció

Vírus evolúció

Védelmi evolúció

Összefoglaló

Crazy how nature does that



*"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 Kiszá. I. bék.**
1054 Bp. Bajcsy-Zs. u. 54.
Tel.: 310-945 31.

Adóig. azonosító szám: **10033908201**

A vevő neve, címe: **Csizmazia István**
1124 Bp. Lejtő u. 7

Számlaszám: **446421**
A számla kelt: **1989. X.13 D**

A termék vagy szolgáltatás

KSH besorolási száma, megnevezése	mennyiség	mennyiség	egységre (ált. forg. adóval növelt)		érték (ált. forg. adóval növelt)	
			Ft	f	Ft	f
18-5 XT táp	1db	1	7390		7390	11978
48-5 1M Ram	1db	1	22730		22730	7128
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

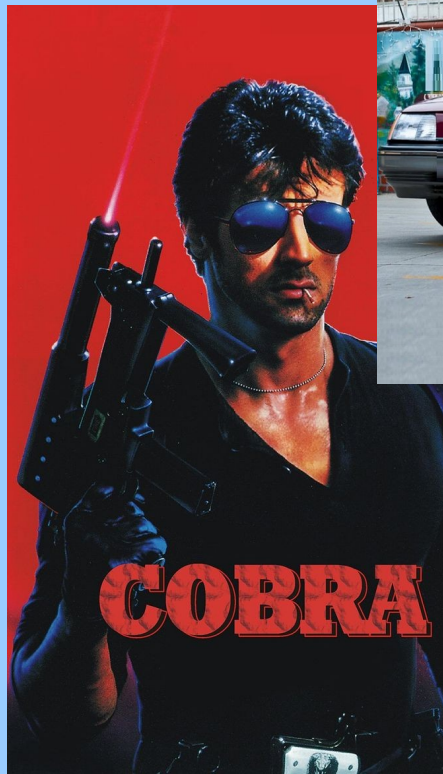
- Az AlphaGo megveri a legjobb go játékost,
a dél-koreai Lee Sedolt 4:1

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

Vírus evolúció

1986. Az USA elnöke: Ronald Reagan

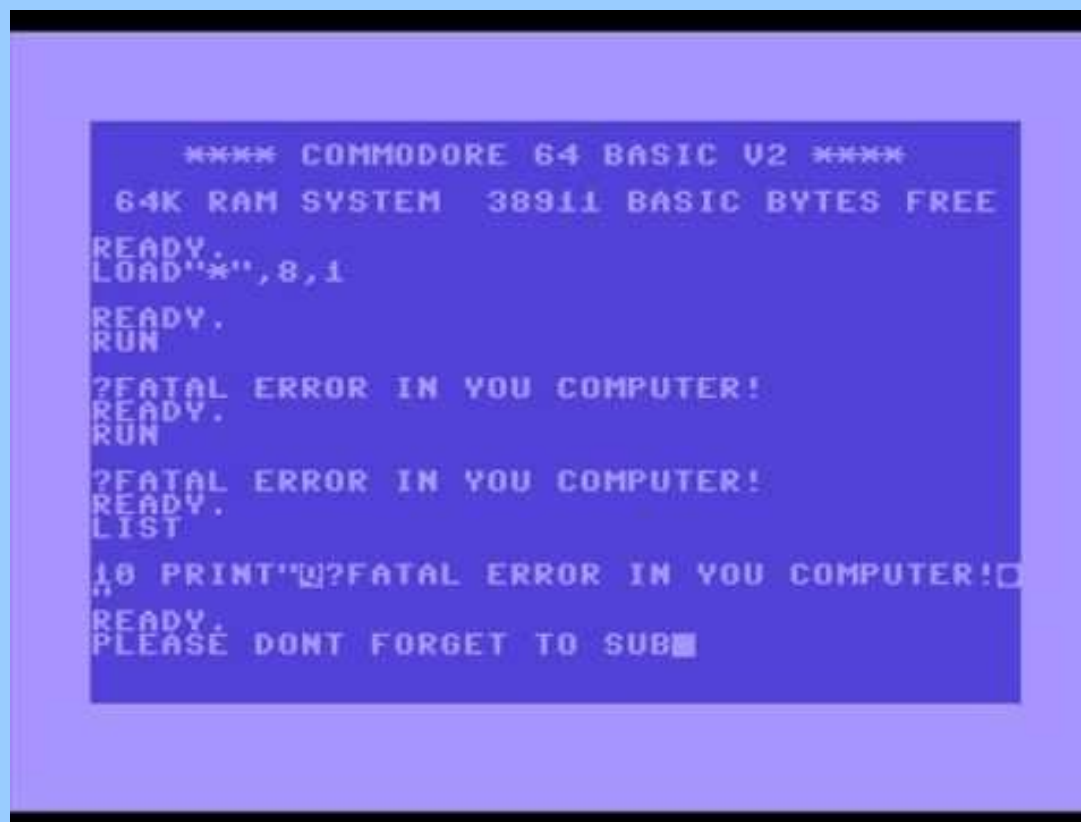
- Super Bowl döntő: Chicago vs New England (46-10)
- Wimbledon: Navratilova-Mandlikova (7-6 6-3), Becker-Lendl (6-4 6-3 7-5)
- Stallone Cobra, Ford Taurus



Vírus evolúció

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

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 lemezekon 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

Több alkalommal írtak lapunkban a Mikrovilágban vírusokról szóló cikkeket. Ezek többnyire külföldi példákat 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 „lezuhanhatnak” az alsó sorba. Ez azonban csak XT gépen fordul elő. E rövid ismertetővel segítséget szeretnék

nyújtani az áramító gépek a leendő felhasználóinak. A vírus a számítógépes hálón terjed, és a hálón keresztül is elterjedhet. A vírus jelenléte felismerhető a PC-nyok hosszát a FAT táblában és verziójában. A vírus a DOS 3.3-as 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 a lemezünk. Az érin-

ny a DOS-utalásokkal is terjed. Megfelelően a célra például a disk Manager egy a diagnosztikai lemez. Ezt a lemezt gépen másoljuk hajlékonylemezre, és onnan indítsuk el. A lemez 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 COM-MAND.COM hosszának figyelésére, és ezt az AUTOEXEC.BAT-ba beleírni.

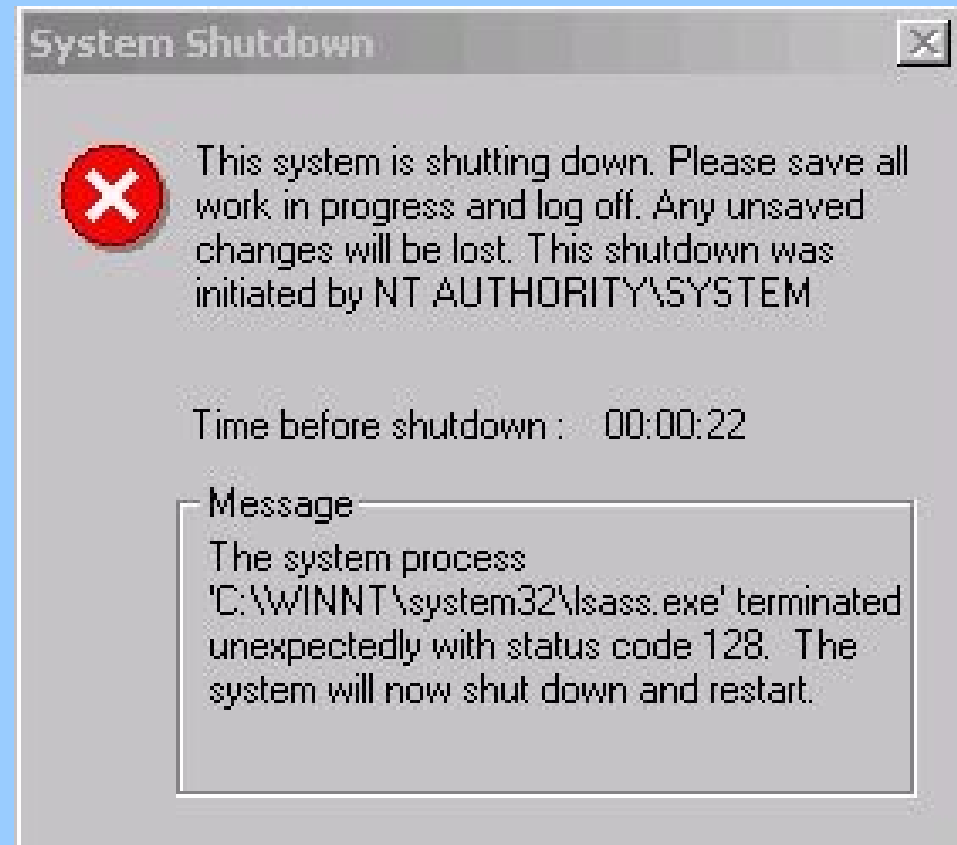
Csizmazia D. István



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

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 milyen



The screenshot shows a CNET article page. At the top is the CNET logo and a navigation bar with links: BEST PRODUCTS, REVIEWS, NEWS (highlighted), VIDEO, HOW TO, SMART HOME, CARS, and DEALS. Below the navigation bar, the word 'MOBILE' is centered. The main title of the article is 'Windows animated cursor attack' in a large, bold font. Below the title is a subtitle: 'The way Microsoft Windows handles animated cursors on Web sites puts PCs at risk.' The author information is 'BY ROBERT VAMOSI / APRIL 10, 2007 10:25 AM PDT'. Below this is a row of social media sharing icons: Facebook, Twitter, LinkedIn, Reddit, Email, and Print. The article text begins with '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"

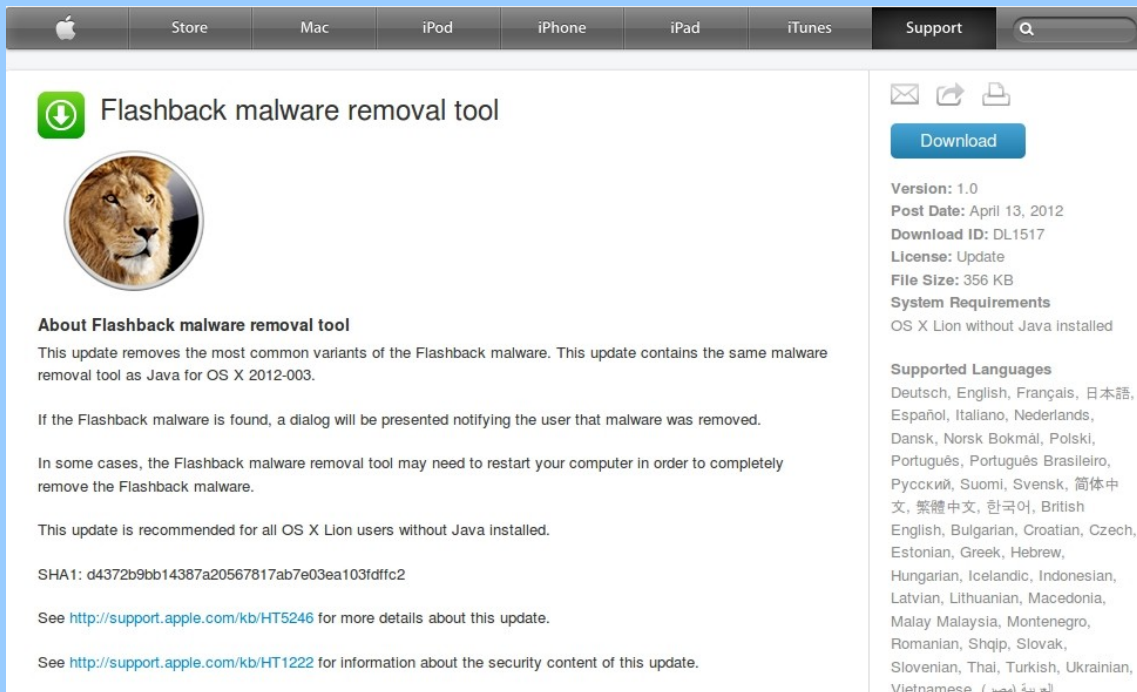


**It doesn't get
PC viruses.**

A Mac isn't susceptible to the thousands of viruses plaguing Windows-based computers. That's thanks to built-in defenses in Mac OS X that keep you safe, without any work on your part.

Vírus evolúció

- 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



The screenshot shows the Apple Support page for the "Flashback malware removal tool". The page is in English and features a lion's head icon. The "About Flashback malware removal tool" section states: "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." It also mentions that if the malware is found, a dialog will be presented notifying the user that malware was removed. In some cases, the tool may need to restart the computer to completely remove the malware. The update is recommended for all OS X Lion users without Java installed. The SHA1 hash is provided: d4372b9bb14387a20567817ab7e03ea103dfc2. Links to support.apple.com are provided for more details and security content.

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.

This update is recommended for all OS X Lion users without Java installed.

SHA1: d4372b9bb14387a20567817ab7e03ea103dfc2

See <http://support.apple.com/kb/HT5246> for more details about this update.

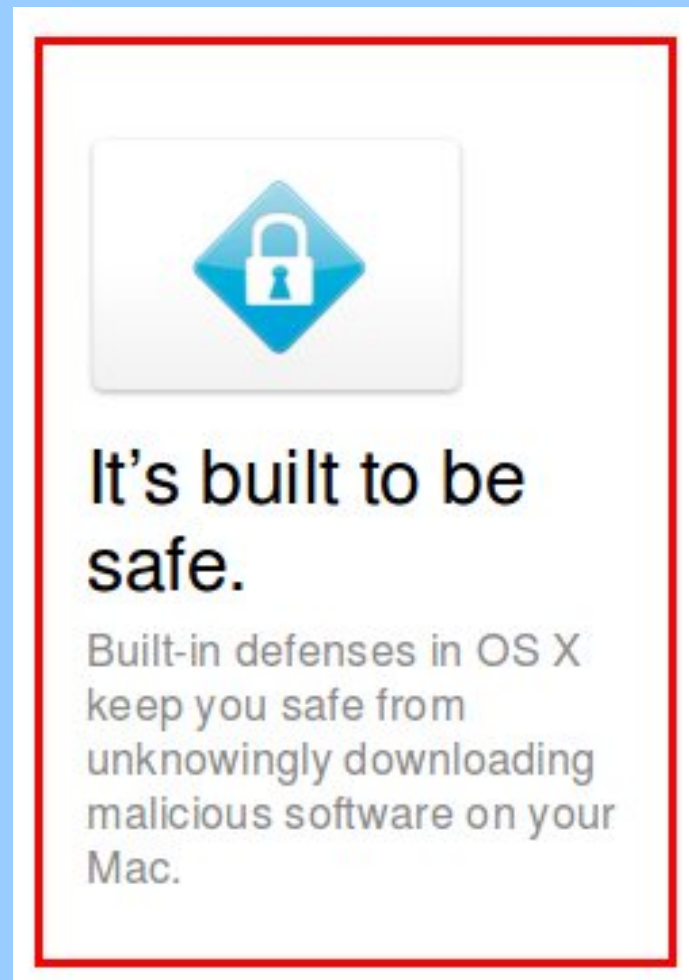
See <http://support.apple.com/kb/HT1222> for information about the security content of this update.

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, 简体中文, 繁體中文, 한국어, British English, Bulgarian, Croatian, Czech, Estonian, Greek, Hebrew, Hungarian, Icelandic, Indonesian, Latvian, Lithuanian, Macedonia, Malay Malaysia, Montenegro, Romanian, Shqip, Slovak, Slovenian, Thai, Turkish, Ukrainian, Vietnamese, العربية (مصر)



The advertisement features a blue padlock icon inside a diamond shape. Below the icon, the text reads: "It's built to be safe." and "Built-in defenses in OS X keep you safe from unknowingly downloading malicious software on your Mac."

It's built to be safe.

Built-in defenses in OS X keep you safe from unknowingly downloading malicious software on your Mac.

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

Vírus evolúció

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

OS X 10.8
Mountain Lion



2012.07.25.

**Introducing Developer ID
and Gatekeeper.**

macs Application



2013.05.18.

**Introducing Rajender Kumar
Apple Developer ID**

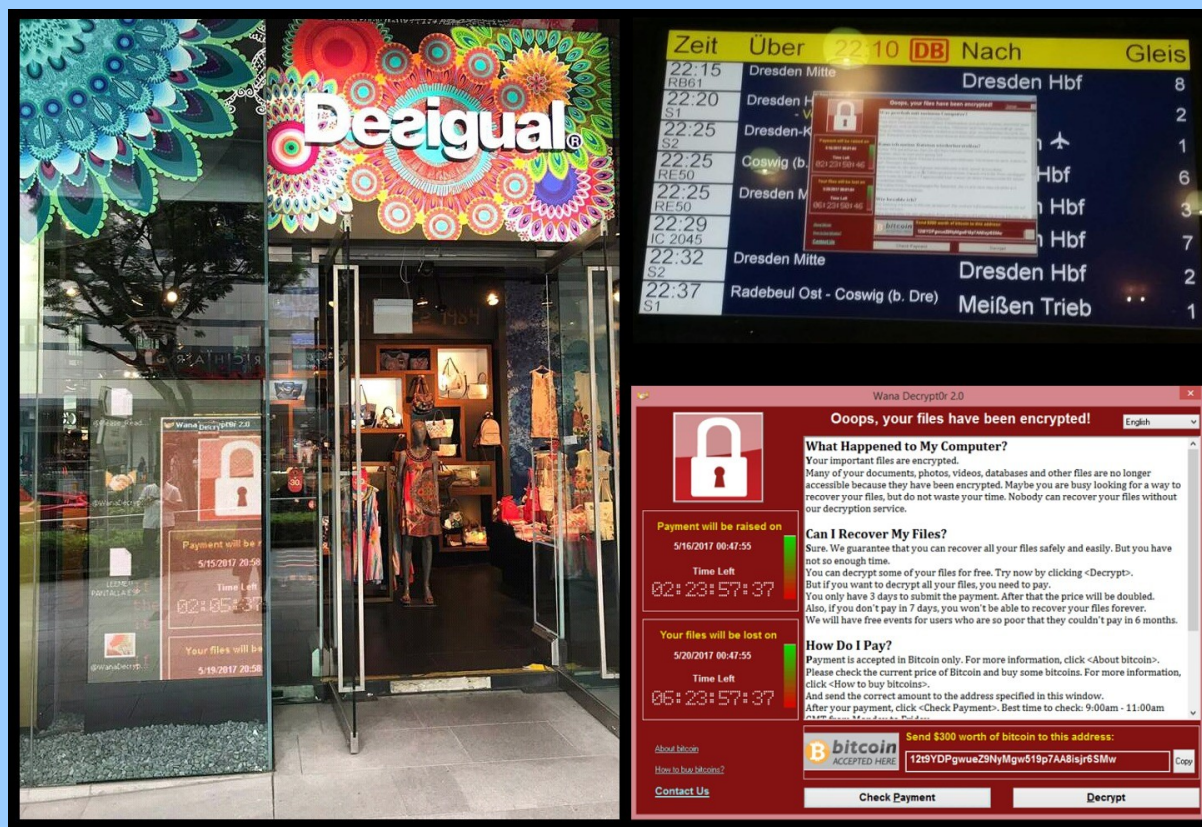
Vírus evolúció

- 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

- 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

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



Targets

Log

Setup

Diagnostics Targets:

- ☒ Files
- ☒ Boot sectors
- ☒ Memory

Diagnostics methods:

- ☒ Signatures
- ☒ Heuristics
- ☐ Runtime packers
- ☐ Archives

Heuristic sensitivity:

- ☐ Safe
- ☒ Standard
- ☐ Deep

On virus detection:

- ☐ Clean
- ☒ Offer an action
- ☐ Leave unchanged
- ☐ Rename
- ☐ Delete
- ☐ Replace

Log:

- ☐ Enabled
- ☐ Wrap log
- ☒ Append
- ☐ Overwrite

On virus detection:

- ☒ Offer an action
- ☐ Leave unchanged
- ☐ Rename
- ☐ Delete
- ☐ Replace

System:

- ☐ List all files
- ☒ Sound signal

Max.length [kB]: 100

Name: nod32.log

Save

Load

Extensions

Defaults

Scan

Clean

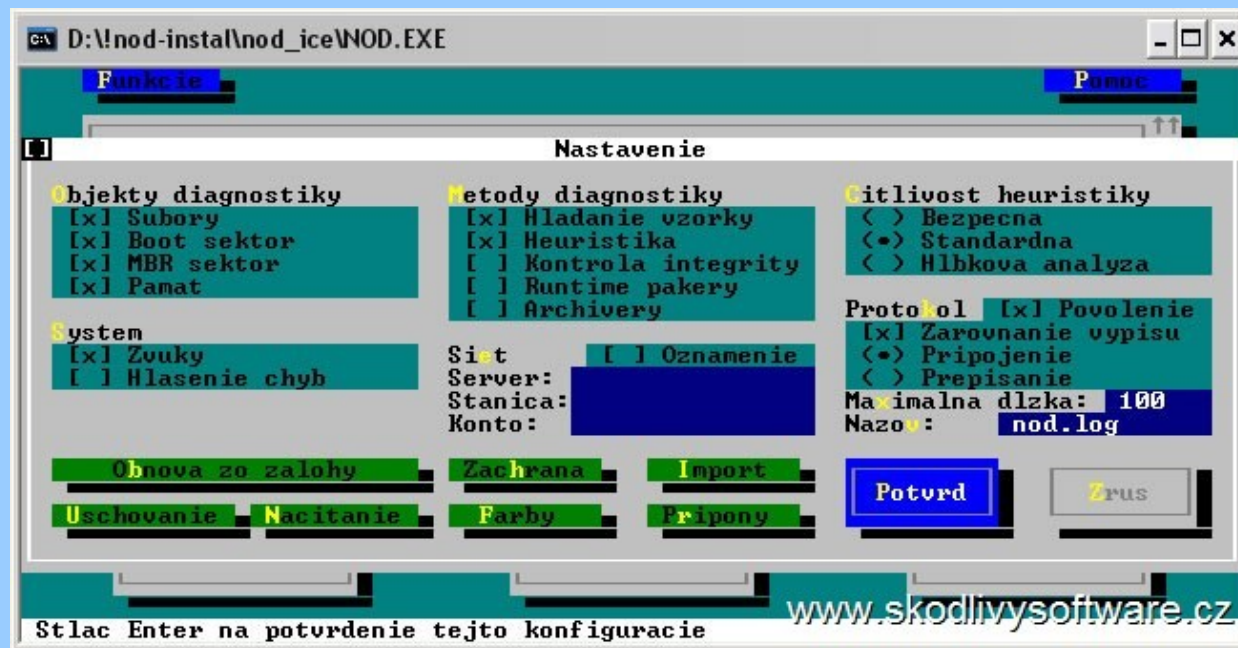
Exit

Scanning of selected objects

Védelmi evolúció

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

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



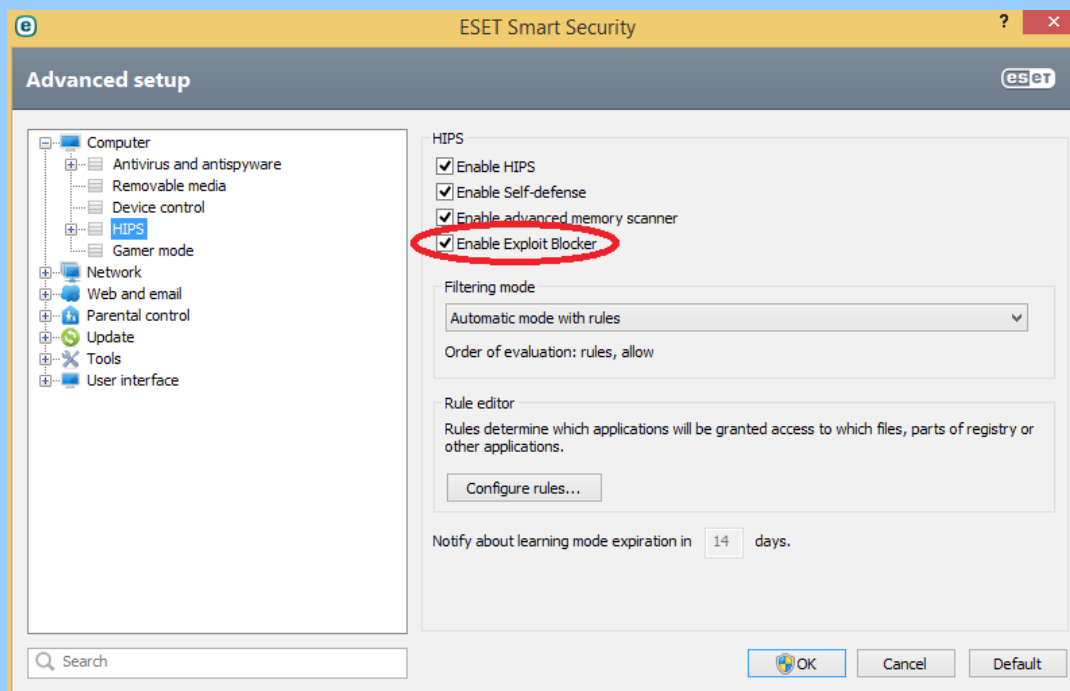
2012. ACAD/Medre

- 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

2012. Exploit Blocker

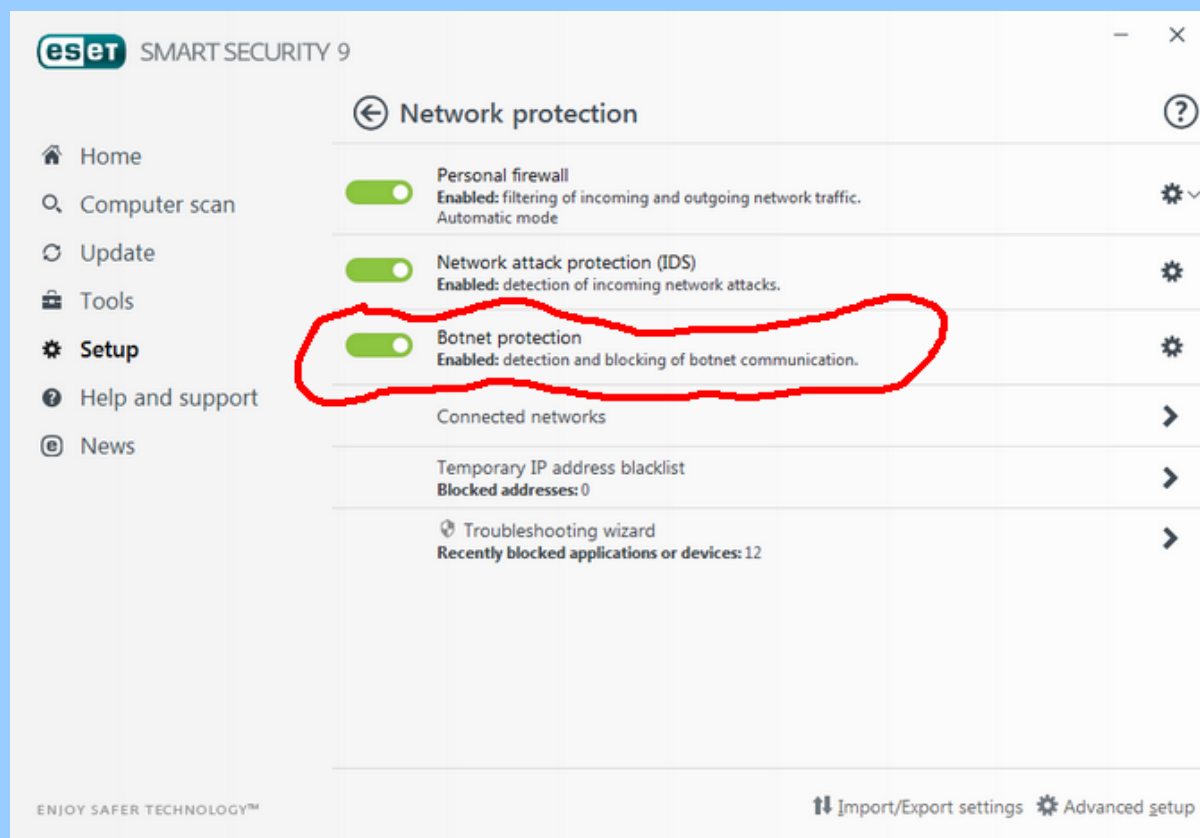
- a gyakran használt alkalmazástípusoknál megfigyeli a gyanús tevékenységeket, folyamatokat
- pl. egy nulladik napi kihasználható hiba kapcsán
- pl. webböngészőkben, PDF-olvasókban, e-mail kliensekben, MS Office összetevőkben
- Ha ilyennel találkozik, akkor azonnal leállítja az adott folyamatot
- rögzíti 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

2014. Botnet Protection

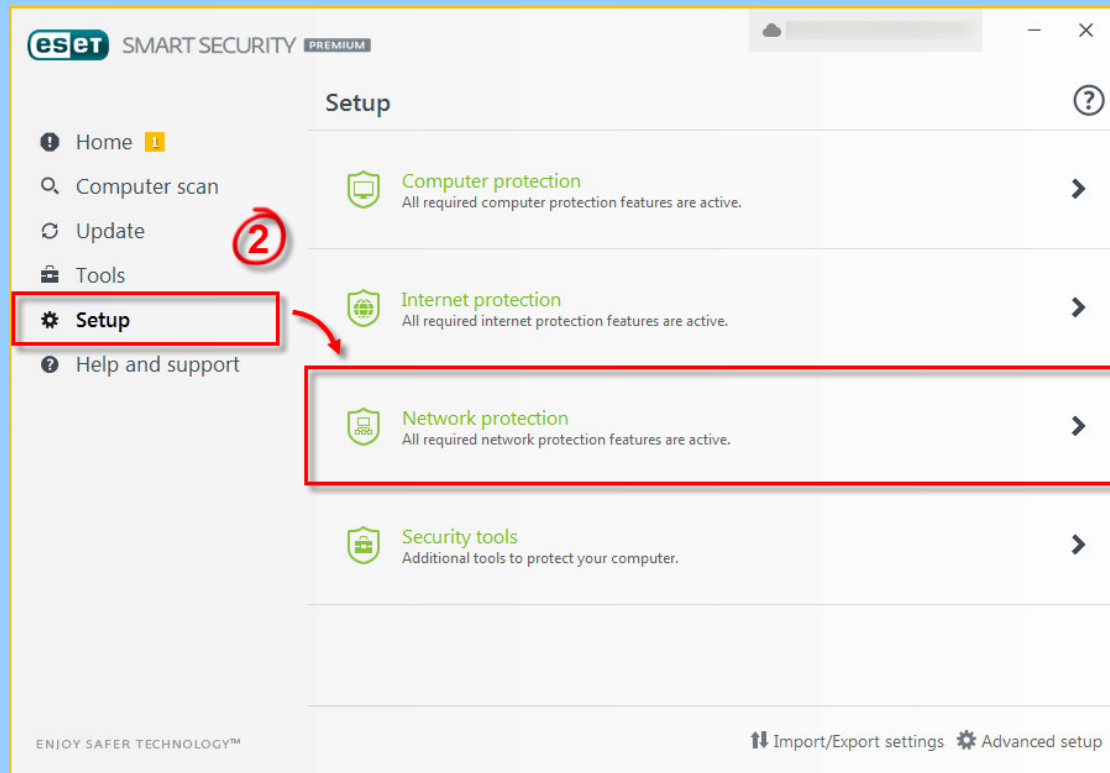
- A védelem észleli a zombihálózatokkal kapcsolatos kártékony programokat
- részletesen elemzi a hálózati kommunikációs protokollokat
- felismeri a jellegzetes botnetes működést, gyanús vagy rosszindulatú tevékenységét
- megakadályozza, hogy a számítógépet egy zombihálózathoz csatlakoztassák



Védelmi evolúció

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

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 merevlemezre, hordozható eszközökre és e-mailekre érvényesíthető policy-k központi kezelését
- hatékonyan felléphetünk az adatszivárgás megelőzése érdekében
- biztosítja a követelményeknek (pl. GDPR) való megfelelést

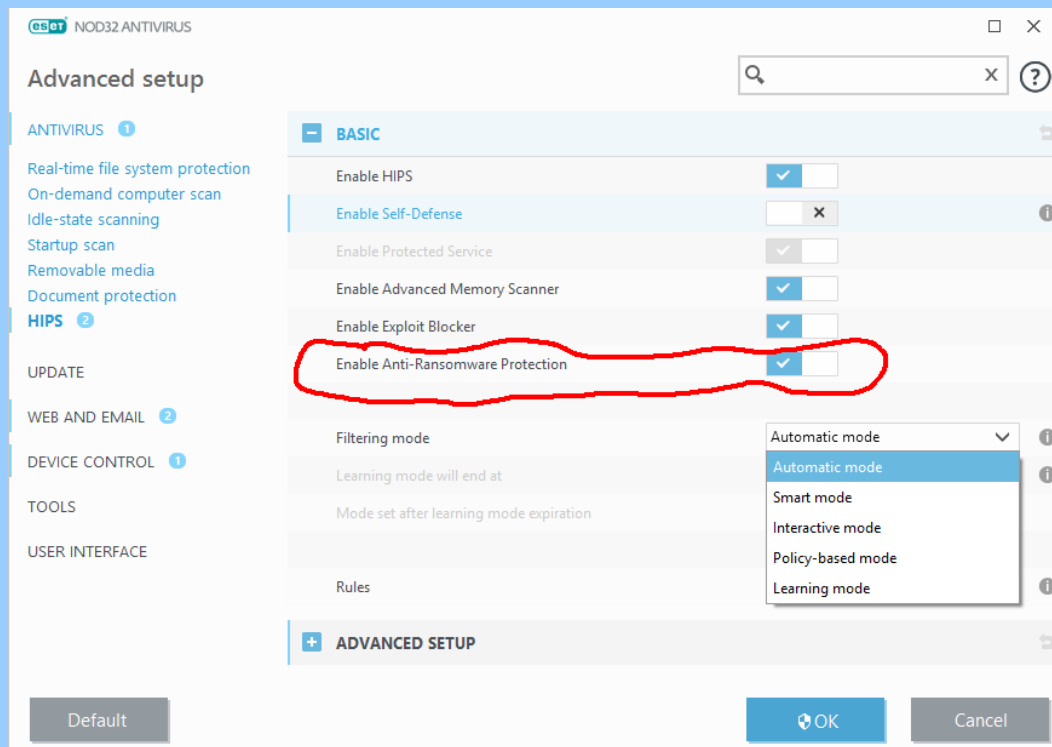
[🏠](#) > [Vállalati](#) > [Végpontvédelem](#) > ESET Endpoint Encryption titkosítás

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

Védelmi evolúció

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



2017. 100-ik VB100

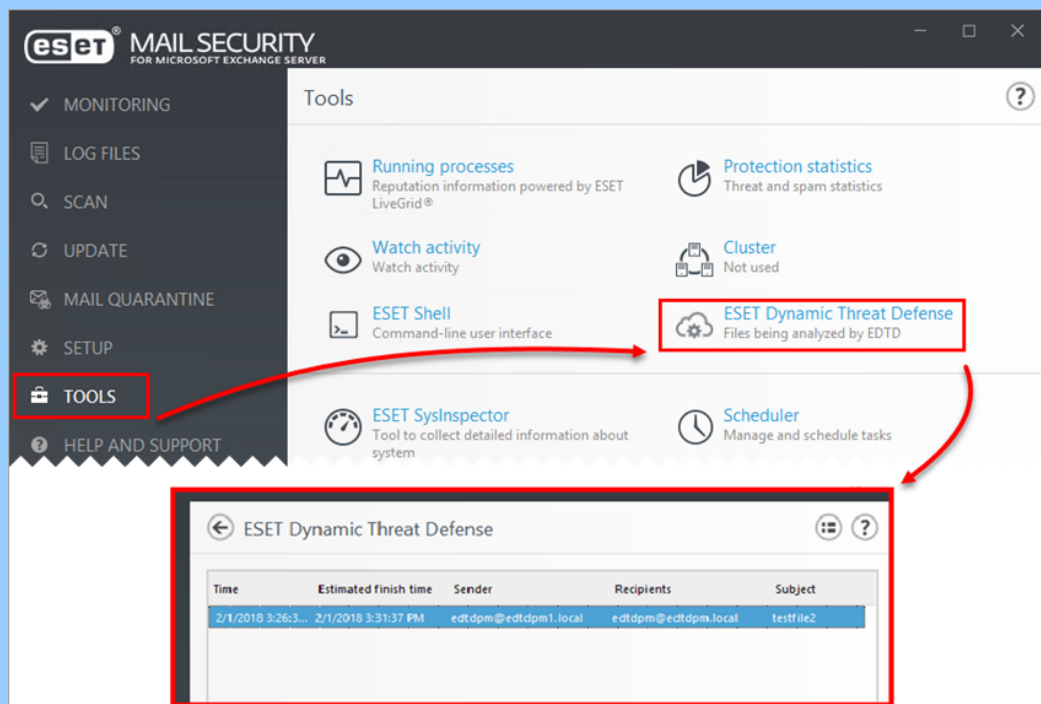
- A NOD32 századik alkalommal nyerte el a Virus Bulletin Virus Bulletin 100% díját
- erre egyetlen más vírusírtó termék sem volt képes eddig a világon
- A VB Award az egyik legelismertebb független, biztonsági szoftverek tesztelésével foglalkozó szervezet
- szigorú tesztelési rendszer - pl. tiltott a tesztelés ismételése
- 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

2018. ESET Dynamic Threat Defense

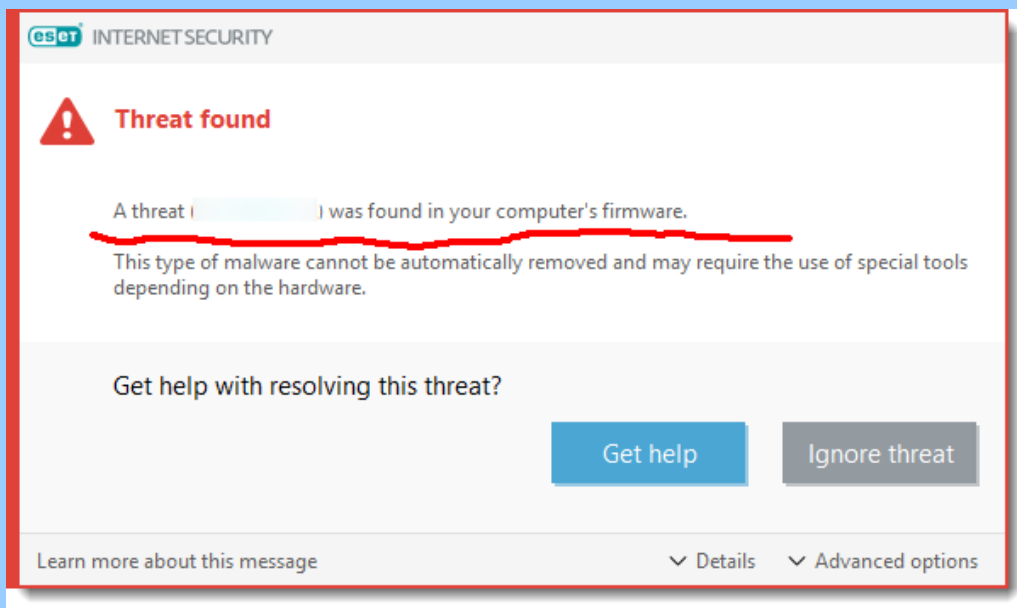
- a feltöltött, új és ismeretlen állományokat egy Sandbox technológiával vizsgálja
- tartalmuk és nem fájlkiterjesztésük alapján
- a vállalati termékek tudnak vizsgálatra küldeni gyanús programállományokat (max. 64 MB)
- Éves díjjal külön licencként vásárolható, a kívánt gépekre aktiválni kell
- 205 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

2018. UEFI Scanner - V:11

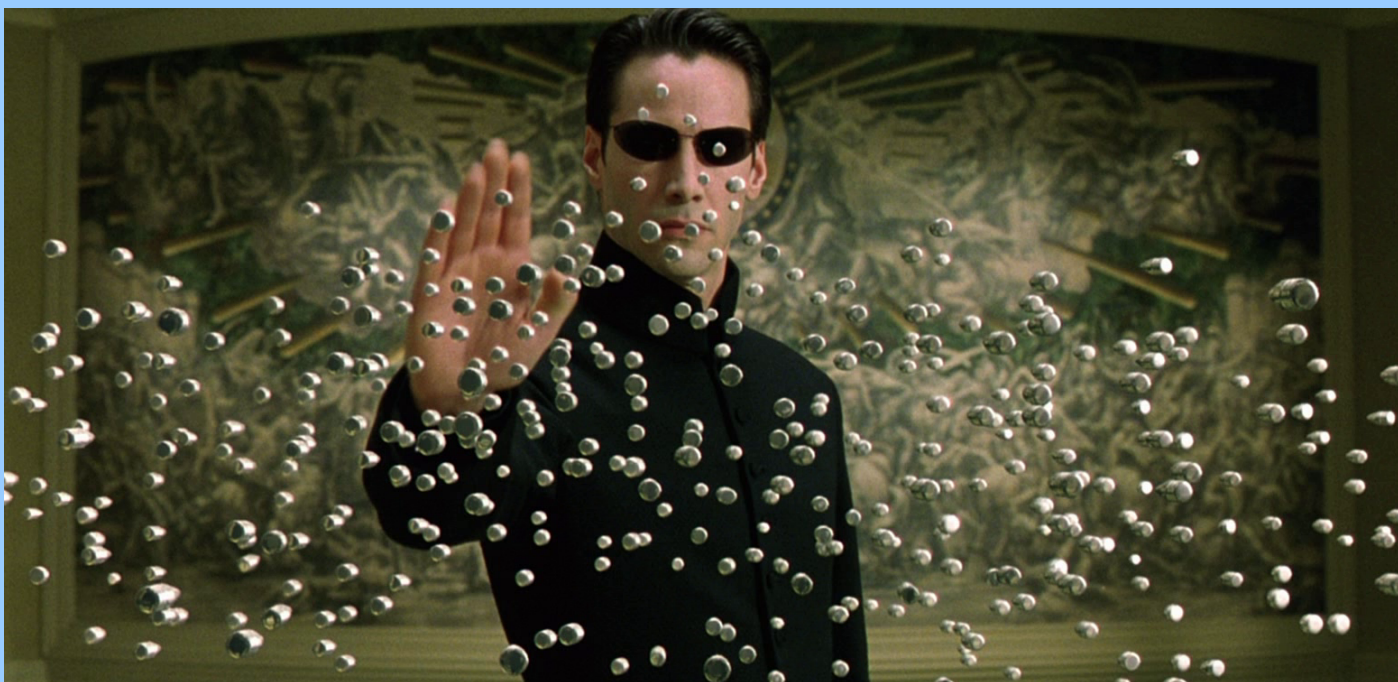
- Az UEFI (Universal Extensible Firmware Interface, a BIOS utódja) vizsgálata
- ellenőrzi a számítógép firmware-jét
- szavatolja az UEFI szabványos, boot előtti rendszerkörnyezet érintetlenségét, biztonságát
- A fejlett rosszindulatú rootkiteket képes felismerni
- ezeknél a támadóknak fizikailag is hozzá 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

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