

Megelőzés és AI a vírusvédelemben

CTO.hu

2019.10.10-11.

SICONTACT 
biztonság a digitális világban



Csizmazia-Darab István
Sicontact, IT biztonsági szakértő





- 1981. XT, 1982. AT, Basic, dBase, Clipper
- Nyugodt munka, minden egyszerű
- A programok egyetlen célja a hibátlan és gyors működés

```
00 20      .8J@4t@ @
74 6f      Welcome to
20 20      the Dungeon
20 20
20 20
74 20      <c> 1986 Basit
4c 74      & Amjad <pvt> Lt
20 20      d.
52 20      BRAIN COMPUTER
4e 49      SERVICES..730 NI
4d 41      ZAM BLOCK ALLAMA
20 20      IQBAL TOWN
4f 52      LAHOR
4f 4e      E-PAKISTAN..PHON
34 38      E :430791,443248
20 20      ,280530.
69 73      Beware of this
74 61      VIRUS.....Conta
69 6e      ct us for vaccin
2e 2e      ation.....
```



- 1986. Csernobil és Brain

- 0 „km kő”

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

On virus detection:

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

Log:

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

System:

- ☐ List all files
- ☒ Sound signal

Max. length [kB]: 100

Name: nod32.log

Save **Load**

Extensions **Defaults**

- 1987. ESET: felvett kesztyű
- Védelmi programok igénye





- Eseti fájl fertőzés veszélyek
- MBR elmentése után annak felülírása
- Vírusok számának exponenciális emelkedése
- Mentésítés, helyreállítás (szignatúra alapú keresés)



- Lopakodás, rejtőzködés, adatmegsemmisítés, szabotázs
- 2003. SQL Slammer (Zaphyre worm) MS SQL exploit, 205e gép, 1 mrd USD kár
- Frissítések fontossága



2015: wow I was so stupid last year
2016: wow I was so stupid last year
2017: wow I was so stupid last year
2018: wow I was so stupid last year
2019: wow I was so stupid last year

- 2013. Cryptolocker és társai
- 2017. WannaCry (EternalBlue exploit, NSA vs. The Shadow Brokers)
- mentések hiánya
- ransomware "elleni" biztosítás

```
LIB_FLAME_PROPS_LOADED__ = true
flame_props = {}
flame_props.FLAME_ID_CONFIG_KEY = "MANAGER.FLAME_ID"
flame_props.FLAME_TIME_CONFIG_KEY = "TIMER.NUM_OF_SEC"
flame_props.FLAME_LOG_PERCENTAGE = "LEAK.LOG_PERCENTAGE"
flame_props.FLAME_VERSION_CONFIG_KEY = "MANAGER.FLAME"
flame_props.SUCCESSFUL_INTERNET_TIMES_CONFIG = "GATOR"
flame_props.INTERNET_CHECK_KEY = "CONNECTION_TIME"
flame_props.BPS_CONFIG = "GATOR.LEAK.BANDWIDTH_CALCUL"
flame_props.BPS_KEY = "BPS"
flame_props.PROXY_SERVER_KEY = "GATOR.PROXY_DATA.PRO"
flame_props.getFlameId = function()
    if config.containsKey(flame_props.FLAME_ID_CONFIG_KEY)
        local l_1_0 = config.get
        local l_1_1 = flame_props.FLAME_ID_CONFIG_KEY
        return l_1_0(l_1_1)
```

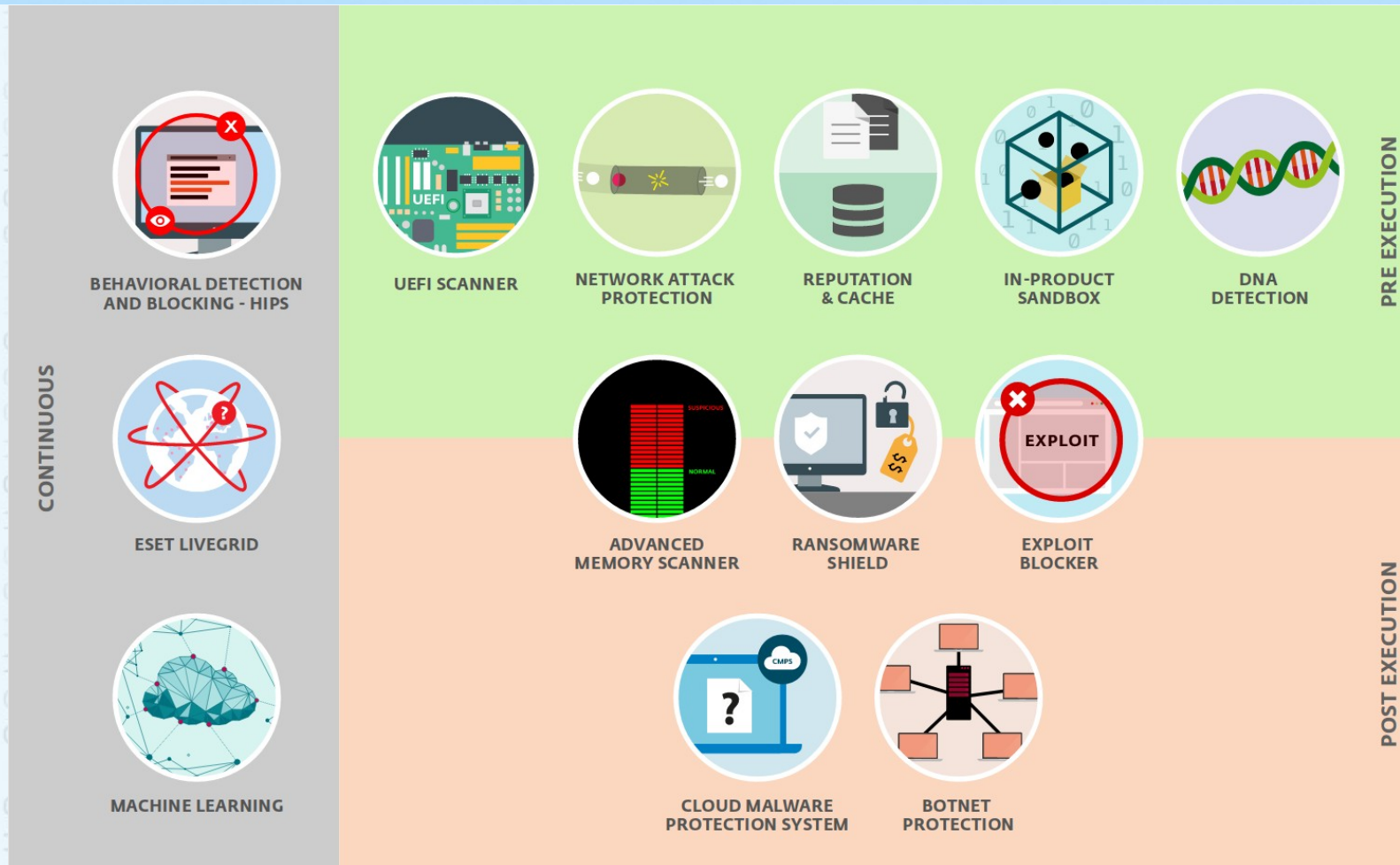
AP



- 2010. Stuxnet – Irán
- 2013. Adobe hack
- 2018. Spectre és Meltdown - Intel x86
- 2019. Unencrypted data: Tesla, Facebook, etc.
- 123456, password, query



- automatizált eszközök
- teljes feketepiaci infrastruktúra a darkweben
- bérelhető botnet for dummies, 7/24 support, nyelvi támogatás
- RaaS - Ransomware as a Service
- sokféle támadó: script kiddie, hacktivist, állami kártevők, ransomware, ipari kémkedés, stb.

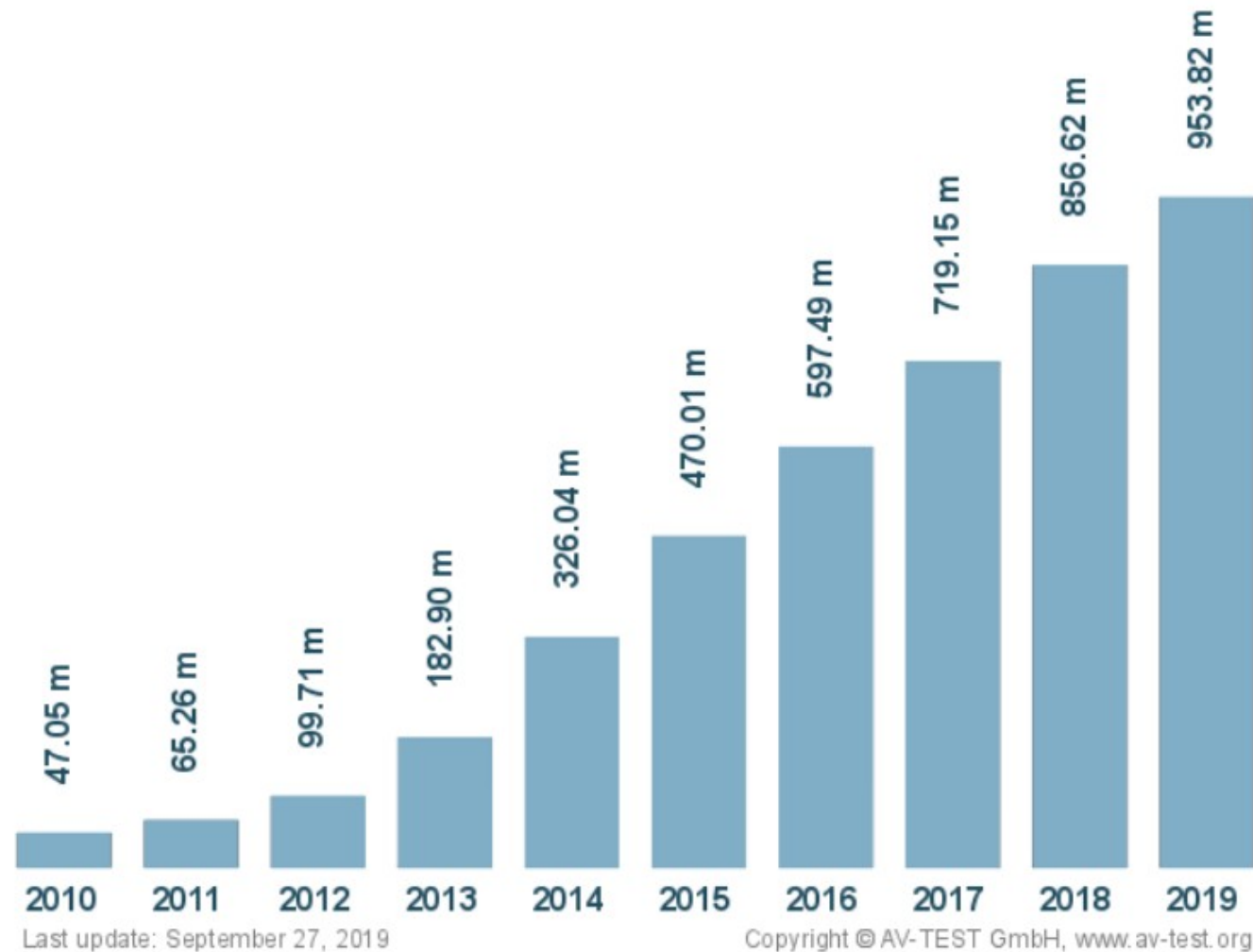


- A vírusirtó nem halott
- Live Grid, SysInspector, Exploit Blocker, Botnet Protection, Hálózati védelem, Antiransomware, UEFI Scanner, stb.
- 1989. óta adatgyűjtés-osztályozás, 1995. óta gépi tanulás, a védelmi munkában 7 féle AI
- ESET Dynamic Threat Defense: 3 külön gépi tanulási modell, utána sandbox (új ransomware)



- AVTest.org: >953m egyedi kártevő
- 4.53 mrd netező (World Internet Users)
- 26.66 mrd netes eszköz (Statista, 2025-re 75 mrd)

Total malware

AVTEST

BREAKOUT TIME BY ADVERSARY FOR 2018

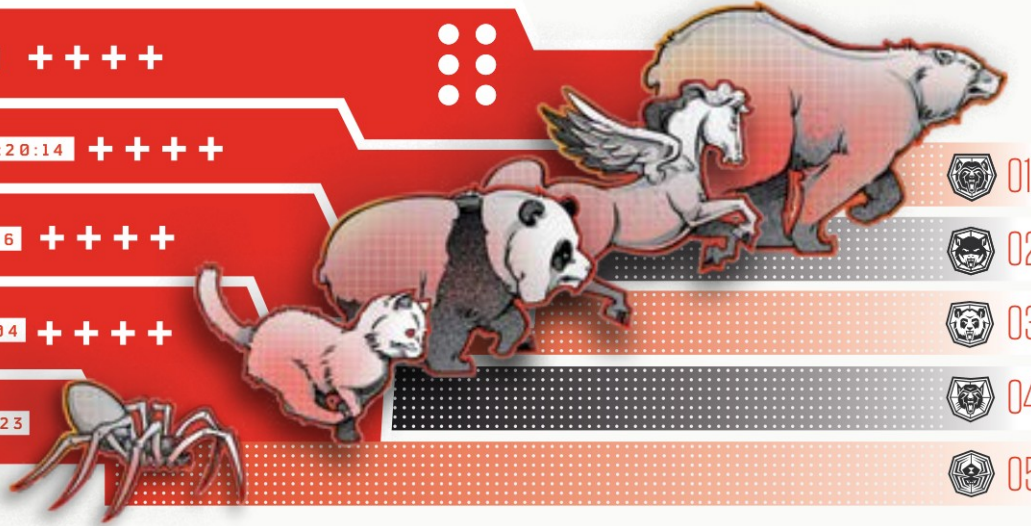
BEAR 00:18:49 + + + +

CHOLLIMA 02:20:14 + + + +

PANDA 04:00:26 + + + +

KITTEN 05:09:04 + + + +

SPIDER 09:42:23



- Lappangási idő 101 nap (iparági átlag FireEye 2017.)
- Meghackelési idők a behatolást követően: 18 perctől - 5 óra (CrowdStrike Global Threat Report, 2019.) (Oroszország, Észak-Korea, Kína, Irán)
- Egyre több (nem csodafegyver) AI lesz mindkét oldalon



32 éve szolgálunk és védünk!

Köszönöm a figyelmet!

info@sicontact.hu