

30 éves a Brain vírus

Két pakisztáni srác 1986-ban megváltoztatta a számítógépek világát

A számítógépes vírusok történelmében a jelképes nulla kilométerkövet a PC MS-DOS (MicroSoft Disk Operating System) rendszerű gépeket támadó pakisztáni eredetű Brain képviseli, megjelenését az 1986. január 19. dátumhoz kötik. A 80-as évek végén, de még a 90-es évek elején is elenyészően csekély, pár ezres nagyságrendű volt azon kártevők száma, amelyek számát ma már hozzávetőlegesen 350 millióra becsülnék a vírusvédelmi szakemberek. Az ESET biztonságtechnológiai cég a születésnap alkalmából összefoglalta az elmúlt időszak változásait.

A vírusok megjelenése, és napjaink tömeges terjedése miatt a felhasználóknak is megváltozott az élete, így a biztonságos munkavégzéshez, játékhoz, vagy internetezéshez már alaphelyzetben is hozzátartozik a korszerű vírusvédelem. De ugyanígy új kihívás elé kerültek a számítógép-programozók is, hiszen míg korábban elég volt a kódolásnál a jó végeredményre és a gyors működésre koncentrálni, addig ma már a biztonságos programozás is nélkülözhetetlen eleme lett a szakmának.

Bár a legeslegelső vírust jóval korábbra datálhatjuk - ez az 1971-ben megjelent Creeper volt, de a PC számítógépeken széles körben tömegesen elterjedő vírusok úttörőjének mégis az 1986-os Brain számít. A Lahore-i (Punjab) illetőségű testvérpár, Basit Farooq Alvi és Amjad Farooq Alvi orvosi szoftvereket árultak floppy lemezen, és az illegális programmásolást akarták vele büntetni. A program készítői érdekes módon teljes nevüket, címüket és telefonszámukat is beleírták a vírus kódjába.



Az IBM PC-re írt vírus emellett egyben az egyik első olyan kód, amely lopakodó mechanizmust használt. A pakisztáni Brain az 5 1/4 collos floppy lemezekben a boot rekordot fertőzte meg felülírással, az eredeti adatokat pedig elmentette, és egy hét leforgása alatt szétterjedt a világon. A Brain vírus rezidens volt, azaz egy állandóan a tárban maradó résszel is rendelkezett, és mivel a megszakításvektorokat önmagára irányította, egy lemezeditorral végzett bootszektor-vizsgálatot is képes volt átverni: ilyenkor trükkösen az eredeti, elmentett részt jelenítette meg: „tartotta a táblát”. Későbbi változatai aztán már nem csak a hajlékony, de a merevlemez is képesek voltak fertőzni.

A vírusvédelmi szakemberek szemében ezek igazi hősi idők voltak, például a vírusok száma a 80-as évek végén, de még a 90-es évek elején is elenyészően csekély, pár ezres nagyságrend volt a mai hozzávetőlegesen 350 millióra saccolt egyedi kártevő kóddal szemben. De a világ is még másként működött, nem volt még grafikus felületű Windows illetve egér, hanem jobbra csak karakteres PC DOS felület. A legtöbb munkahelyen monokróm Hercules monitorok üzemeltek, AUTOEXEC.BAT és CONFIG.SYS konfigurációs beállító fájlokban dőlt el sok minden. A letöltés őse pedig a BBS, azaz Bulletin Board System nevű helyekről, betárcsázós telefonvonalon, 1200-3600 baud sebességű modemekkel történt. A kezdetekkor az adatbázis frissítések is jóval ritkábbak voltak - 1-2 havonta jött csak ki új szignatúra, az új vírusokkal vagy kártevő variánsokkal, a mai naponkénti, vagy még gyakoribb automatikus frissítési megoldásokkal szemben.

Szinte ugyanilyen régóta védelmezi az ESET is a felhasználók millióinak a számítógépeit. Az 1987-ben megjelent ESET NOD32 Antivirus világső az elnyert Virus Bulletin "VB100" tesztelési díjak számát tekintve, illetve a vizsgálatok 1998-as fennállása óta eddig minden szabadon terjedő vírust vagy férget észlelt és kivédett. Az ESET NOD32 Antivirus, ESET Smart Security és az ESET Cyber Security (biztonsági megoldás Mac-re), valamint a mobiltelefonok és táblagépek védelmét biztosító ESET Mobile Security a legajánlottabb biztonsági megoldások közé tartoznak, a termékekben milliók bíznak meg világszerte.

A [ESET infografikáján](#) pedig bemutatjuk a számítógépes kártevők rövid történetét a Brain vírustól kezdődően egészen napjaink botnetes kártevőig. Az összefoglalóból kiderül, hogy a kezdeti híres, hírhedt vírusokon, a világjárványt okozó férgek át hogyan jutottunk el a rejtett kémprogramokig, banki kártevőig.

Az ESET-ről:

A több mint 25 éves, díjnyertes NOD32 technológiát kifejlesztő ESET a proaktív védelem úttörője, az üzleti és otthoni biztonságtechnikai szoftvermegoldások nemzetközi szállítója. A vállalat piacvezető a fenyegetések észlelésében és megelőzésében. Az 1987-ben megjelent ESET NOD32 Antivirus világső az elnyert Virus Bulletin "VB100" díjak számát tekintve, illetve a vizsgálatok 1998-as fennállása óta eddig minden szabadon terjedő vírust vagy férget észlelt és kivédett. Az ESET NOD32 Antivirus, ESET Smart Security és az ESET Cyber Security (biztonsági megoldás Mac-re), valamint a mobiltelefonok és táblagépek védelmét biztosító ESET Mobile Security a legajánlottabb biztonsági megoldások közé tartoznak, a termékekben milliók bíznak meg világszerte. A vállalat központja Szlovákiában, Pozsonyban található, regionális terjesztési központokkal rendelkezik San Diegóban (USA), Buenos Airesben (Argentína) és Szingapúrban, valamint irodái vannak São Paulóban (Brazília) és Prágában (Csehország). Az ESET több mint 180 országban, köztük Magyarországon, rendelkezik kiterjedt partneri hálózattal. További információ: www.eset.hu

A Sicontactról:

A Sicontact Kft. az egyik legjelentősebb, IT biztonsággal foglalkozó hazai szoftverdisztribútor. Mottója és küldetése, ami köré termékportfólióját kialakította: „biztonság a digitális világban”. A Sicontact Kft. Magyarországon az ESET NOD32 technológiára épülő termékeivel mind a lakossági, mind a vállalati szegmensben meghatározó piaci szereplő. A cég 2007-ben megszerezte az ESET ausztriai képviselétét, így azóta regionális piaci szereplőként tevékenykedik. A Sicontact kizárólagos magyarországi disztribútora a Unified Threat Management (UTM) hálózatzbiztonsági eszközök terén piacvezető Cyberoam termékeinek, valamint portfóliójában megtalálható a helyi és távoli rendszerdiagnosztika, a hálózatzfigyelés, a távvezérlés és a licenccmenedzsment terén kiemelkedő képességekkel rendelkező AIDA64 szoftver is.

Sicontact Kft. 1023 Budapest Sajka u. 4. tel: 1/346 7040 fax: 1/346 7050 www.sicontact.hu



A Sicontact Kft. több ízben elnyerte a kitüntető Business Superbrands díjat. Az ESET Smart Security programcsomagot többször is az év antivírus megoldásának választották. A Sicontact Kft. az ESET szoftvereit a lehető legrugalmasabb konstrukciókban kínálja. Az ESET biztonsági szoftverek licencelése során a gyorsan változó körülményeket is figyelembe veszi, így például az ESET szoftverek a licencidőszak alatt bármikor újratelepíthetők az adott számítógépre, továbbá az unilicenc konstrukció keretében a munkaállomásokon a megvásárolt ESET licenccel egyaránt használhatók a Windows, Linux és Mac operációs rendszerre fejlesztett ESET termékek, így az operációs rendszer cseréje esetén nem szükséges új licencet vásárolni. A Sicontact Kft. az ESET szoftverekhez és a Cyberoam termékeihez díjmentes terméktámogatást és távsegítséget biztosít, mind az otthoni, mind a vállalati felhasználók számára, így az ügyfelek jelentős időt és pénzt takarítanak meg.

Sicontact Kft. 1023 Budapest Sajka u. 4. tel: 1/346 7040 fax: 1/346 7050 www.sicontact.hu

