MINDENKI TUD VÍRUST ÍRNI

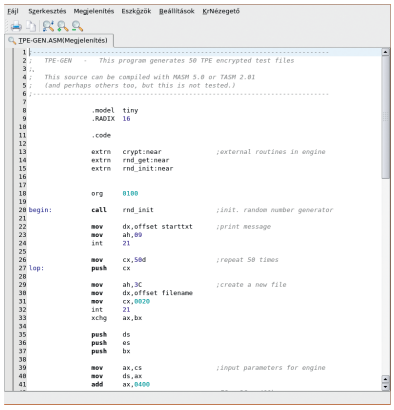
Gépesített hadosztályok a barikád két oldalán

Sorozatunk tizenharmadik epizódjában áttekintjük, mik okozzák az exploitokat és mekkora út vezetett az egyéni, „kézzel írt” vírusoktól a mai, automatikusan generált kártevőkig. Látható, hogy a kódgeneráló kitek, a „tesztelő” segédeszközök és egyéb programkészletek a kártevőellenes csata mindkét résztvevőjénél komoly fejlődésen estek át és jelentős szerepet játszottak/játszanak.

Van a sebezhetőségeknek egy speciális csoportja, amelyet a szakzsargon csak „nulladik napi támadásnak” (0 day exploit) nevez. Ezek olyan, épphogy csak felfedezett friss programhibák, amelyekre még nem létezik javítófolt, sőt néhány esetben a gyártó egyáltalán nem is tud a sebezhetőségről. Az ilyen hibák kihasználása eredménnyel – és ezáltal anyagi haszonnal – kecsegtet a bűnözőknek a javításig, ezért egy-egy jelentősebb Windows Vista nulladik napi hiba technikai leírása és a kihasználására írt kód akár 50 ezer dollárért is gazdát cserélhet a feketepiacon.

Ki csordul, mi csordul

A nem frissített operációs rendszerek és alkalmazások mellett a leggyakoribb veszélyforrás a puffertúlcsordulási hiba. Anélkül, hogy mélyebben érintenénk ennek programozói vetületét, kijelenthetjük, hogy nagyjából arról van szó, hogy egy programban a különféle visszatérő funkciókat ellátó programrészletek (függvények) egy memóriaterületen (verem, angolul stack) adják át egymásnak a paramétereiket. A verem azonban nemcsak ezeket, hanem azokat a memóriacímeket is tárolja, amelyekre a meghívott függvény lefutása után a programnak ugrania kell, azaz amelyekhez vissza kell térnie. Ha a hívóprogram nem végez semmilyen ellenőrzést a verembe töltendő paraméterek hosszát illetően, akkor a túl hosszú adattal a fontos visszatérési címek felülíródhatnak. Számos behatolási kísérletnél használják ezt a módszert, azaz egy megfelelően előkészített adatcsomaggal magára az „adatra” kerül át a vezérlés, ami esetünkben egy kártevő. Így lehet például egy MP3 fájlba vírust helyezni, és mondjuk egy puffertúlcsordulás ellen nem védett zenelejátszóval elindítani a zenébe rejtett károkozót.

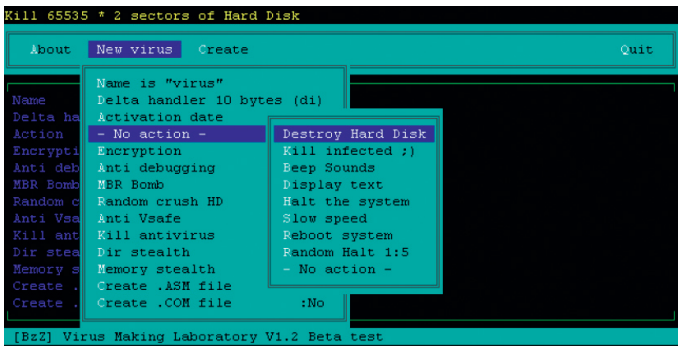


TridenT Polymorphic Engine (TPE) mutációs program igazi nagyágyú volt a maga idejében. Készítője, Masoud Khafir a forráskódot is közkinccsé tette

A kőbaltától a rakétáig

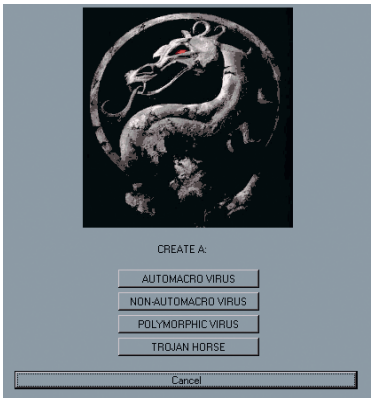
Az első időkben a szakmai tudás, a mély rendszerprogramozási ismeretek játszották a főszerepet, s az Assembler és a C nyelv alapos tudása adta kulcsot víruskódok elkészítéséhez. A tudásanyaghoz többek között a lemezkezelés részletes ismerete tartozott: tehát a boot szektorral, a Master Boot Rekorddal és az adatok tárolására vonatkozó szabályokkal (clusterek, láncolás stb.) kapcsolatos jártasság. Egy valamirevaló vírusíró természetesen a megszakítások (interruptok) kezelésével, működésével is magas szinten tisztában volt. Később már itt is előfordultak olyan vírusváltozatok, variációk, amikor például a péntek 13-i időzítést 12. csütörtökre cserélték: nos, ehhez persze nem szükségeltetett komoly tudás, csak egy szövegszerkesztő vagy egy hexaeditor, plusz némi lelemény.

Kevesen foglalkoztak magas színvonalon vírusírással és vírusirtókból sem volt sok, így sokáig a havi frissítés – a váratlan és rendkívüli eseteket leszámítva – elegendőnek látszott. Egy-egy jelentősebb vírus – például a Whale család polimorfikus, azaz alakváltó kódjának megjelenése – jól fel tudta kavarni a hangulatot. Néha még olyan is előfordult, hogy egy új vírus írója váltságdíjat kívánt kérni nagyobb AV-cégektől, hogy a pénz fejében átadja a víruskódot, amelyet azok beépíthetnek az adatbázisba. Természetesen az antivírusipar elzárkózott az ilyen terrorista akcióktól, sőt a legtöbb helyen még az a szokás is megmaradt, hogy volt, de már jó útra tért vírusírókat nem alkalmaznak, a „rablóból lesz a legjobb pandúr” elv ellenében. Ez a szabály manapság gyengülni látszik, Kínában több esetben is jól fizető IT-biztonsági állást ajánlottak a kártékony kódok készítőinek, a vezető

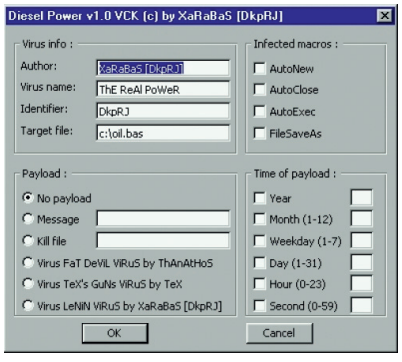


Már a DOS-os időkben is léteztek vírusgenerátorok. Hozzájuk jutni azonban sokkal nehezebb volt, mint manapság, mivel például jelszóval védett privát BBS-ek vettek részt a terjesztésben

Amikor beköszöntött a makróvírusok korszaka, hihetetlen mennyiségben jelentek meg olyan konstrukciós készletek, amelyekkel szakértelem nélkül is lehetett ontani a kártékony kódokat. Itt a Dark Bytes nevű kitet látjuk



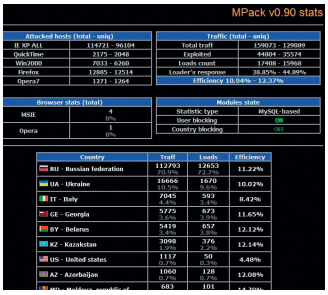
A nagy népszerűség miatt a makróvírusok is bekerültek az univerzális víruskészítő készletekbe. A Demolition Kit (azaz „Pusztító Készlet”) segítségével néhány egérkattintással „eredményt” lehetett produkálni



A Diesel Power menüszerkezetében mindent beállíthatunk: mikor – év, hónap, nap, óra, perc, másodperc –, milyen állományban, milyen nevű makróban, milyen kísérő üzenettel, milyen pusztítás történjen

Manapság, a szélessáv korában a warezoldalakról vagy a torrentekről csekély keresgéléssel bárki bármihez hozzájuthat, legyen az trójaigenerátor, vírus forráskódja vagy épp hackereszköz

A Multi AVs Fixer megkönnyíti a vírusírók életét: segítségével gyorsan és hatékonyan tesztelhetik új kártevőjüket, hogy lehetőleg minél kevesebb antivírusprogram ismerje azt fel.



Egy idő után a bűnözők már nemcsak a konstrukciós kiteket bocsátották áruba, hanem valódi supportot is nyújtottak: az ár már tartalmazta a technikai támogatást és a statisztikát is

nagyhatalmak pedig hackereket toboroznak honvédelmi célokra.

Megnyomom a gombot, és vírus terem

Amit már egyszer felfedeztek, megfejtettek, arra már lehetett a továbbiakban építeni (mint a C vagy Pascal nyelvű könyvtárrutinok esetében), így például az alacsony szintű lemezkezeléshez már senkinek nem kellett újra feltalálni a spanyolviaszt. Természetesen a szakmai tudást az első víruskorszak után is a szükséges hozzávalók közt említjük, de elkezdődött az egyedi, szeretve dédelgetett kódok világa után a sorozatgyártás, a konstrukciós kitek, a csekély ismeretekkel rendelkezők számára néhány gombnyomásra vagy egérkattintásra kész vírust készítő csomagok, technikák kora. Ebben már nemcsak a gyorsabb kódkészítés, az alacsonyabb rendű kulimunkák megspórolása játszott szerepet, hanem elkezdett árucikké válni az univerzális víruskészítő programkészlet is, amely iránt fizetőképes kereslet mutatkozott a feketepiacon.

Az automatikus vírus-, illetve féregkészítő készleteknek komoly hagyománya van a mai Oroszország (a volt Szovjetunió) területén. Szürkeállományban gazdag, de erkölcsi gátlásoktól mentes, pénzéhes programozók minden technikai nehézséget legyőzve csak úgy ontották a rafináltabbnál rafináltabb készleteket. Persze készültek ilyenek máshol is: Németország, USA, Ausztrália sem szégyenkezhet. Nézzünk meg ezek közül egy-két érdekesebb darabot.

Mutációkészítő kézi készülék

1993-ban a TridenT, egy holland vírusíró csoport elkészítette a TridenT Polymorphic Engine (TPE) programot. Írója, *Masoud Khafir* több, igen fejlett vírust hozott létre, ezek között vannak az első Windows-vírusok, a Win_Vir, a Cruncher sorozat és az egyik legelterjedtebb – amely a MtE mutációs algoritmust is használja –, a MtE.Pogue vírus. A szerző igen alapos ismeretekkel rendelkezett a titkosításban, programja pedig igazi mérföldkőnek számított. A kezdeti, 1.1-es változat néhány processzortípussal nem működött megfelelően, ezért a hibák kijavítása miatt több – utoljára az 1.4-es – verzió is napvilágot látott. További korai kortárs volt még a Virus Constructions Set (VCS), a Virus Creation Library (VCL), a Next Generation Virus Construktion Kit (NGVC), a NuKE's Randomic Life Generator (NRLG) stb.

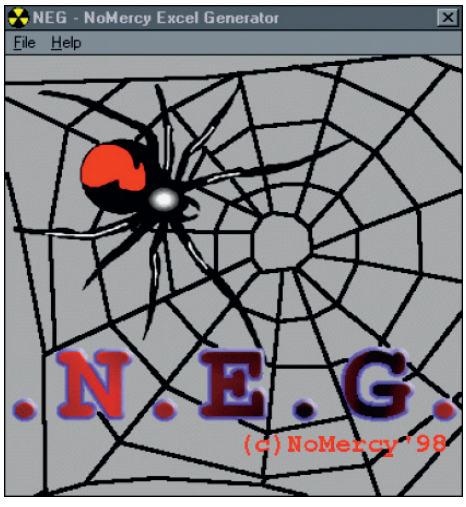
MPack csomag, a svájci bicska

Az MPack kit már friss darab, így a kor igényeinek megfelelően különféle exploitokkal képes támadni. Egy PHP-szoftverkomponenseket összegyűjtő és adatbázissal felszerelt készletről van szó, amely egy PHP-szerveren futva fejti ki tevékenységét. A terméket forgalmazó orosz bűnbanda szoftverkövetést, supportot, valamint teljes körű statisztikát is ad a program mellé. Magát a konstrukciós programot körülbelül 1000 amerikai dollárért hirdetik a feketepiacon. Különböző exploitok segítségével a Windows platformon futtatott Internet Explorer, Firefox és régebbi Opera böngészőkliensek használóit hozhatja nehéz helyzetbe, ha nem frissítenek vagy upgrade-elnek időben. Ezenkívül további híres-hírhedt darabok is léteznek, ezekről helyhiány miatt éppen csak említést teszünk – így érdekes volt még a Shark, a Metasploit, az Icepack platinum stb. A Pinch II Pro nevű, adatlopásra tervezett vírus-, trójai- és kémprogramkészítő készletet pedig a *Vírusok Varázslatos Világa 2. részében* részletesen is bemutattuk, kipróbáltuk.

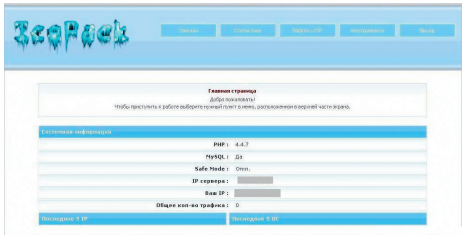
Utolsó simítások a víruskódon – Multi AV-szkennerek

Amikor még a „munkapadon" van a kártevő, de már teljesen működőképes, a terjesztőnek az az érdeke, hogy teremtménye minél észrevétlenebb lehessen. Ezért érdemes megvizsgálnia több, különböző antivírusprogrammal, hogy csökkenjen a lebukás veszélye. Nem meglepetés, hogy erre is vannak automata eszközök. Az egyik ilyen a Multi AV Fixer. Segítségével nagyságrendekkel gyorsabban és olajozottabban lehet próbálkozni a cél érdekében – azaz annak érdekében, hogy minél kevesebb antivírus jelezzen az új programra.

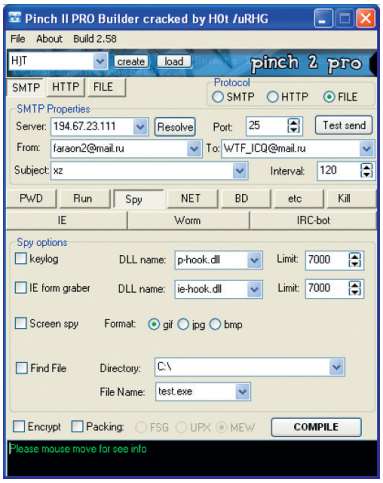
Nagyon macerás viszont több antivírusrendszert is feltelepíte-



Természetesen az egyéb makrózható Office állományok sem kerülhették el a sorsukat. Képünkön a NoMercy (Nincs kegyelem) Excel Generator nyitóképernyője. Nomen est omen



Az egyik leghírhedtebb konstrukciós támadó készlet az Icepack Platinum. Többek közt az Internet Explorer, Firefox, Opera, Windows Media Player, QuickTime, WinZip tucatnyi sebezhetőségét tudta kihasználni és ezeken keresztül kártevőket telepíteni. Az eredeti cirill betűs, orosz nyelvű változata mellett kínaira fordított verziója is létezik



A Pinch II Pro menüjében minden részlet aprólékosan beállítható. Sok kereskedelmi programot lepipál a kényelmes kezelőfelület. Cikksorozatunk 2. részében mi is teszteltük a képességeit

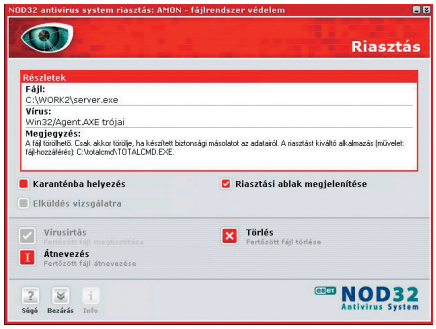
Nem csak konstrukciós kitek és trükkös segédprogramok léteznek ám. Ennek az oldalnak segítségével MD5 hash értékekből nyerhetjük vissza a jelszót. Arra is felhívja a figyelmet, hogy ne ringassuk magunkat hamis illúziókba vélelmezett biztonságunkat illetően

ni egy gépre, ráadásul a rezidens részt mindegyikben ki is kell kapcsolni, hogy össze ne akadjanak. Nos, erre jó a **Virusscan.Jotti.org** vagy a **VirusTotal.com** weboldal. Az előbbi 20, míg az utóbbi oldal immár 37 különböző gyártó keresőmotorjával vizsgál párhuzamosan. Korábban a VirusTotal kínált egy olyan lehetőséget, amikor a vizsgálandó mintáknál azt is kiválaszthattuk, ne küldjék el automatikusan az állományt a víruslaborokba, de éppen a vírusírók effajta, kiadás előtti tesztelése miatt ezt az opciót később megszüntették.

Eladó az egész világ

Ma már minden feladatra létezik hatékony eszköz, legyen az Office dokumentumok vagy egyéb jelszavak feltörése, MD5 hash kódok visszafejtése, WiFi-titkosítás megfejtése, vagy éppen friss exploit kódok felhajtása. Aki az interneten keres, az talál – sosem volt még ez ilyen egyszerű. Rengeteg esetben akár egy nyilvános weblapon is lelhetünk olyan eszközöket vagy információkat, amelyek gyakorlati útmutatót adnak a kártevőkészítők kezébe. Nehéz megítélni, hogy az információk közzététele jó vagy rossz, de talán inkább hasznos, ha mindenki tud róla.

Az új sérülékenységek esetében azonban a dolog kétoldalú. Gondoljunk csak a legutóbbi, nagy port felverő DNS-poisoning sebezhetőségre, amely esetében a csepegtetett blog-információkból végül csak összerakták a mozaikot, és beindult a támadási hullám. A megfelelően etikus felfedezőtől azt várnánk el, hogy először a gyártókkal és a fejlesztőkkel vegye fel a kapcsolatot, és addig ne adjon ki részletes információkat vagy demonstrációs támadókódot. Néha azonban a fejlesztőcégek tagadják a felfedezett rést, nem hajlandók elismerni a hibájukat, vagy épp némaságba burkolóznak, szinte kiprovokálva ezzel a hiba felfedezőjétől a részletek nyilvánosságra hozását. És persze azt sem szabad figyelmen kívül hagyni, hogy egy új nulladik napi sebezhetőség felfedezése a jó oldalon „csak” hírnevünket fényesítheti, míg a rossz oldalnál (eléggé el nem ítélhető módon) bőkezűen készpénzben honorálják az ilyen jellegű konkrét információkat.



A Shark konstrukciós kittel még a legkevésbé hozzáértő is tud vírust írni. Az azért megnyugtató, hogy a tesztelés során a NOD32 minden ilyen, futószalagon készült vírust szépen felismert

Ha harc, hát legyen harc!

Ha már a sötét oldal ilyen automatákkal operál, illogikus volna, ha a hatékony védekezés és tesztelés miatt a „jók” nem tennének hasonlóképpen. Fontos az operációs rendszer és az azon futó alkalmazói programok frissítéseinek rendszeres naprakészen tartása. Ebben, valamint például a sebezhetőségek vizsgálatában is számos hasznos eszköz áll rendelkezésre. A Secunia Inspector (**secunia.com/software_inspector**/), a Microsoft Baseline Security Analyzer (**technet.microsoft.com/en-us/security/cc184924.aspx**), és még jó néhány program is hozzájárul ahhoz, hogy gyorsan leellenőrizhessük a problémákat. Az említett eszközök hatásosan és alaposan feltárják a gyenge, elavult komponenseket, ráadásul a frissítéshez konkrét letöltési linkkel, esetenként pedig részletes útmutatóval is szolgálnak.

We brakes for nobody!

Az automatizált eszközök a harc mindkét résztvevőjénél megjelentek. A rossz oldal a profit növelése érdekében a támadó kódok hatékonyságát egyszerre több szóba jöhető sebezhetőség kihasználásával erősíti, ezenkívül a kártevőkészítő és -terjesztő kitek drága árucikké válása révén húz hasznot a dologból. Nem is beszélve az egyre sokasodó ellopott banki adatokról, jelszavakról, amelyeknek szintén külön piaca van.

A jó oldalon – ahol a csatában az időfaktorral is keményen küzdeni kell – a kényszer szülte a megoldásokat. Automatizált vírusminta-feldolgozás nélkül például ma már egy víruslabor sem tudna lépést tartani a fenyegetésekkel és egyetlen rendszergazda vagy cég sem lenne képes rendszereit a sebezhetőségek automatikus vizsgálata (Secunia, fuzzerek stb.) nélkül naprakészen tartani.

A kártevőkészítők közül egy-egy háttérbe húzódott magányos lángelme időnként még tud zavart okozni – gondoljunk csak a legújabb, 1024 bites titkosító kulccsal operáló Gpcode vírus esetére –, ez azonban ma már inkább ritka kivétel, a tendencia az iparszerű, egészpályás letámadás a specializált és automatizált eszközökkel mindenki ellen.

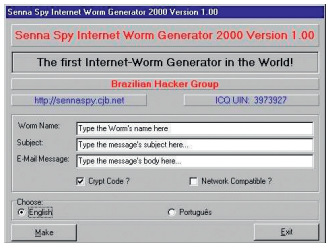
***

Kérjük kedves olvasóinkat, ha a témában kérdésük, hozzászólásuk van, juttassák el hozzánk (**velemeny@pcworld.hu**).

Csizmazia István,
vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete
antivirus.blog.hu

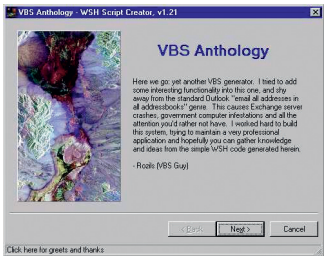
KAPCSOLÓDÓ WEBOLDALAK

ESET víruslexikon: **www.eset.hu/virus**
Secunia: **www.secunia.com**
VX Heavens: **vx.netlux.org**

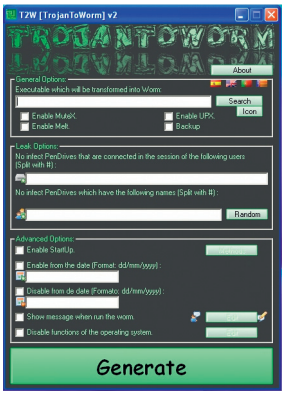


Szintén a hírhedt programok közé tartozott a Sennaspy is, segítségével bárki egyszerűen készíthetett internetes férgeket

Érdekes és veszélyes csoport volt a szkriptvírusok csoportja is. VBS, Perl és egyéb nyelveken sok leleményes kód született. A WISK segítségével IRC alá lehetett fertőző férgeket konstruálni



A VBS Anthology költői neve ellenére sem lesz a barátunk. A forráskódban terjedő férgek 1998 környékén kezdtek megjelenni. Mivel az Outlook képes a beérkező levelekben lévő VBScript és JavaScript programkódot automatikusan végrehajtani, ez által igen hatékonyan lehetett kárt okozni, főleg állományokat töröltetni



Nem szükséges sok szakismeret a Trojan2Worm használatához, kattintunk, legördülőből választunk, és ennyi. Egy tetszőleges ártalmatlan alkalmazást töltünk be, így a kit segítségével egy saját magát terjesztő trójait kreálhatunk