MINDEN LUKBA DUGÓ KELL

Mobil kártevők

CD1/DVD
A cikk képei megtalálhatók a lemezmellékleten

Sorozatunk tizedik epizódjában a mobileszközökön futó vírusokról, kémprogramokról és kártevőkről lesz szó. Az evolúció itt is végbement, igaz, a tömeges elterjedés még – és ez a legfontosabb szó ebben a mondatban – nem történt meg. Nyilvánvalóan nem az okos telefonról kell lemondanunk, hanem itt is elkerülhetetlen lesz a megfelelő hozzáállás és az óvatosság.

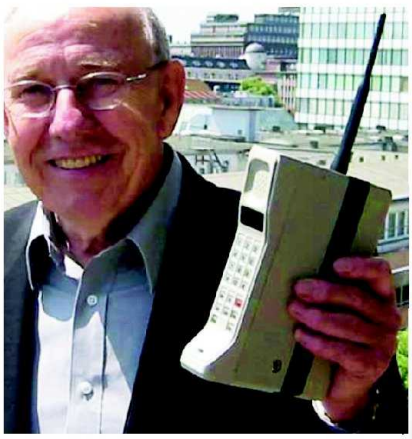
Ha a felütjük a *Galaktika* folyóiratot, vagy belelapozunk gyerekkorunk sci-fi könyveibe – például *Teknős Péter* Jártunk a jövőben című művébe – egyből észrevehetjük, hogy a fantázia világában már a 60-as években létezett egy „cigarettásdoboz méretű" okos kis készülék, amely személyi kommunikátor, televideográf és egyéb neveken szerepelt. Válaszolt kérdéseinkre, segítségével videotelefonálhattunk ismerőseinkkel, térkép helyett útbaigazítást adott, kielemezte a légköri viszonyokat – álmunkban, álomvilágunkban. Aztán mire felnőttünk, elkezdtek megjelenni a valóságban is az újabbnál újabb csodamasinák: ZX81, ZX Spectrum, C64, programozható tudományos kalkulátorok, az első Motorola hordozható telefon, PDA-k, GPS- és Java-támogatással érkező okos telefonok. És azóta a gyártók egyre csak ontják a mind kisebb, okosabb és sokoldalúbb készülékeket.

Első fecskék, néhány érdekes darab

A legegzotikusabb hardver- vagy szoftverplatformra is el szokott készülni előbb vagy utóbb egy kártevő – demonstrációs céllal. Bemutatni a világnak, hogy ezt is lehet. Az ilyen kísérleti kártevőket – amelyek legelső megjelenési formájukban sokszor valójában ártalmatlanok – hívjuk PoC, azaz Proof of Concept kártevőknek. Így volt ez a Palm OS-alapú készülékek idejében, és nincs okunk feltételezni, hogy az újonnan megjelenő mobil rendszereknél ne legyen majd valaki, aki az „első" kísérleti kártevővel megmutatja, ki a legény a gáton.

2004 júniusában igen érdekes jelenségről kaptunk hírt. A Symbian operációst rendszert futtató mobiltelefonok kerültek veszélybe a még kezdetleges Cabir vírus miatt. A zseniális újdonság az volt, hogy a fertőzött készülék a bekapcsolt vezeték nélküli Bluetooth kapcsolaton keresztül igyekezett továbbadni a vírust egy bizonyos hatótávolságban (néhány méter) található másik telefonra. Kiválasztott egy aktív Bluetooth vevővel rendelkező telefont, és ezek után erre az egy készülékre folyamatosan küldte tovább magát. A kártevőt a nemrég megszűnt 29A formáció *ValleZ* nevű tagja készítette demonstrációs célból: valódi „büntetőrutint" nem is tartalmazott, és a forráskódja is elérhető az interneten. Illetve a büntetés tulajdonképpen az volt, hogy a telefon igen hamar lemerült a Bluetooth-kapcsolat miatt. Lenyűgöző, illetve félelmetes. A valamivel később, 2005-ben felbukkant CommWarrior már számos tulajdonságában felülmúlta a Cabirt. Már nemcsak egyetlen készüléket választott ki a fertőzéshez, hanem minden, a hatótávolságában lévő és aktív Bluetooth-kapcsolattal felvértezett telefont igyekezett megfertőzni. Ennél is érdekesebb, hogy saját magát már el is rejtette a feladatkezelőben (szemben a Cabirral, amelyet megtalálása után simán kilőhettünk a FExplorerrel), emiatt sokkal életképesebbnek bizonyult.

Minden felhasználói alkalmazás ikonja helyébe egy koponyát kapunk a Skull-lal fertőzött készüléken


A világ legelső hordozható mobiltelefonja a Motorola DynaTAC 800x. A kisebb táskányi készülék megjelenésekor még nem is sejtettük, hogy sokkal kisebb, sokkal okosabb testvérei pár év múlva már az átlagember farzsebében lapulnak majd, megfizethető áron

De térjünk vissza 2004-be! Ebben az évben egy újabb kártevőverzió tette próbára a felhasználókat. Megjelent a Skulls, azaz Koponyák nevű kód, amely szintén Symbian-alapú mobiltelefonokat tudott megtámadni. Nem volt benne kifejezett büntetőrutin, hanem azt használta ki, hogy a rendszer automatikusan bemásolta a rendszerfájlok nevével egyező nevű fájlokat a telefonba. Települése után megfertőzte a készülékeket, és ez nemcsak abban nyilvánult meg, hogy minden ikont egy koponyával helyettesített, hanem az alkalmazásokat is elérhetetlenné tette. Ilyenkor két eset közül választhattunk: vagy leformáztuk a telefont – ekkor elve-

Egyelőre még mindig az ember a leggyengébb láncszem. És ha kíváncsiságból kattintani fog, utána jól megnézheti magát...

A CommWarrior Q a telefonkönyvben szereplő számokra MMS-üzeneteket küld, emellett a beérkező SMS- és MMS-üzenetekre automatikusan egy fertőzött MMS kiküldésével válaszol. Nemcsak a telefon, hanem a benne lévő memóriakártya is megfertőződhet

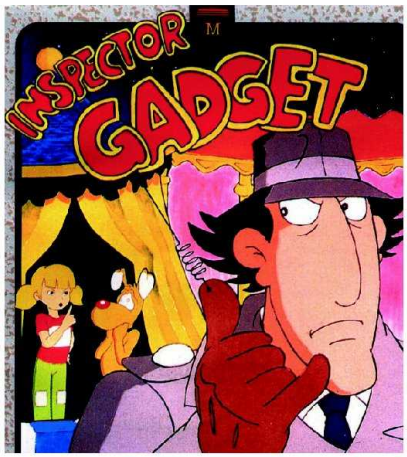
szett minden személyes adatunk, vagy szervizbe kellett menni vele. A Skulls féreg mérete igen változatos volt – pár tíz kilobájttól egészen az 1-2 megabájtos SIS-csomagig –, és gyakran a Cabir, később a CommWarrior kódját is magában hordozhatta.

Voltak még apróbb-nagyobb kellemetlenséget okozó próbálkozások, például a Fontal nevezetű kártevő, amely az alapértelmezett fontkészletet cserélte le zagyvaságra, ily módon kezelhetetlenné téve a telefont.

És hogy egy friss történet is szerepeljen: 2008 februárjában bukkant fel a Windows Mobile rendszerre íródott InfoHijack. Ez a Kínában terjedő károkozó kikapcsolja a Windows CE telepítéssel kapcsolatos biztonsági beállítását, és a megfertőzött készülék gyári sorozatszámát, a futó operációs rendszer adatait, valamint egyéb információkat küld el a kártevő szerzőjének. Az így manipulált eszközök a későbbiekben védtelenek maradnak káros kódok letöltésénél, hiszen a biztonsági figyelmeztetések már nem jelennek meg.

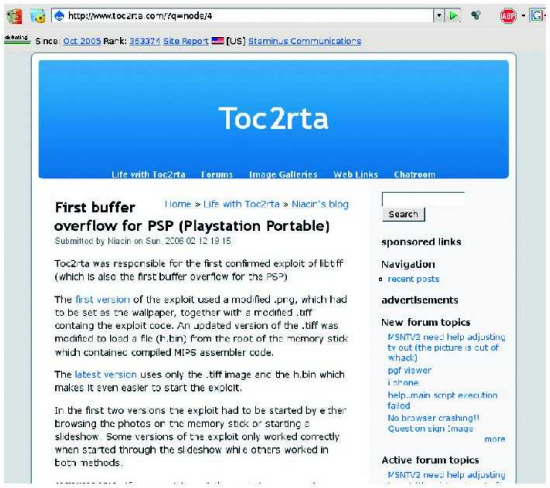
Egy kis séta a mobil operációs rendszerek világában

Számos különféle, mobileszközökben használt platform létezett, illetve létezik manapság is. A vírusok szempontjából a legjelentősebb a Symbian S60 R2, amely 60 százalékos arányával a legelterjedtebb volt a piacon – egyebek mellett a Nokia okostelefonok népszerűsége révén. Szerencsére a fejlesztők időközben kiadták az S60 R3 jelű, illetve a Symbian 9.0 verziókat, amelyek számos jelentős, a biztonság szempontjából kulcsfontosságú változtatást tartalmaztak. A legfontosabb változás az, hogy már csak a Symbian és a hozzá tartozó szoftverházak partnerei által digitálisan aláírt csomagokat lehet telepíteni. Mivel az S60 R2 és R3 csomagok szerkezete binárisan inkompatibilis, ezért a korábbi, bizonytalan eredetű SIS-csomagokat már nem lehet telepíteni az új rendszert futtató készülékekre. További biztonságot igyekeztek elérni a kriptográfiai házirend bevezetésével, amely nagyjából azt jelenti, hogy egy megbízható alkalmazásnak alapból nincs jogosultsága olyan kritikus funkciókhoz való hozzáférésre, mint például az SMS-üzenetek küldése, a Bluetooth ki-, illetve bekapcsolása, e-mail küldés stb., hanem minden kényes funkcióhoz külön részletezett jogköröket kell kérni a hiteles aláírás igénylésekor. Így megerősítve már igen nehéz vírust írni, esetleg csak tanúsítványhamisítással lehetne próbálkozni.



És ezt tudja lovon és trapézon is

A Windows Mobile platform egészen az 5.0-s verzióig szintén kedvelt célpontja volt a víruskészítőknek. A 6.0-s változattal aztán a fejlesztők végre igyekeztek a biztonságot szolgáló újításokat is bevezetni: ilyen például a biztonságos C könyvtárak használata, az elkülönített kernel- és felhasználói-memória-terület, a WPA2 Wi-Fi és IPv6 támogatása, a rendszerbetöltés biztonságossá tétele stb. Mindazonáltal ha valaki készítene, és egy webszerveren elhelyezne egy olyan vírust, amely valamely azonnali üzenetküldő kliensnek hazudná magát, biztosak lehetünk abban, hogy előbb-utóbb lenne, aki letöltené és futtatná. Ekkor a kártevőnek elég lenne elküldeni magát a felhasználó összes címére, hogy „új változatú XY instant messenger kliens jelent meg, töltsd le”, és az ilyen emberi megtévesztéssel – ahol ugye felhasználói interakció, kattintás szükséges – is könnyen lehetne kárt okozni.



A Sony Playstation Portable rendszerre már 2006 elején napvilágot látott PNG- és TIF-állományokkal kapcsolatos sebezhetőségről szóló információ

Ilyen is volt kereskedelmi forgalomban: tartsunk totális ellenőrzés alatt egy másik mobiltelefont S60, Symbian 9.x vagy Windows Mobile rendszer alatt! A 250 eurós programmal titokban belehallgathatunk családtagjaink, kollégáink beszélgetéseibe, minden fogadott, illetve küldött SMS-, MMS- és e-mail üzenetből másolatot kaphatunk. Kérdés, hogy mindez mennyire törvényes?

Mi van a többi polcon?

A J2ME, vagyis a Java 2.0 Micro Edition megjelenésével talán azt remélhetnénk, hogy a mobil operációs rendszerek fejlesztői igyekeztek tanulni az elődök hibáiból, és mind nagyobb hangsúlyt fektetnek a biztonságra. Sajnos nem teljesen így fest a kép, itt ugyanis tetszőleges program képes elérni a saját könyvtárán kívül eső, a rendszer fastruktúrájában elhelyezkedő állományt, például a digitálisan aláírt

IRODALOMJEGYZÉK

Dr. Vesselin Bontsev: Virusability of modern mobile environments, 2007

Mivel érdekes piaci megfontolásból sok országban nem használhatnánk telefonálásra a különféle szolgáltatóknál az Apple iPhone készülékét, így szinte mindenki a feltört szoftver letöltését választja. Azon már kevesebben gondolkodnak el, hogy az ismeretlen forrásból letöltött csomagokban mi minden lapulhat még

J2ME MIDlet eszközkészletet. Bár a felhasználó megkapja a felugró ablakot, miszerint a MIDlet éppen készül valamire, mivel látszólag megbízhatónak tűnik a dolog, ezért biztosan igennel fog válaszolni a *Mehet-e* kérdésre.

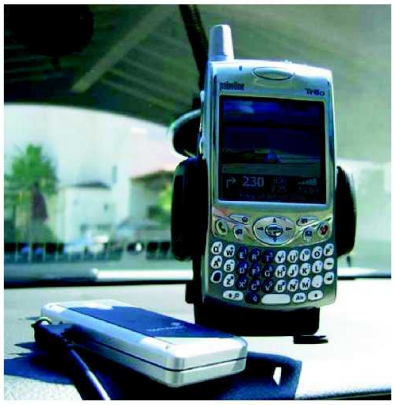
Szintén a versenyzők között indul még a Sony PSP – nem telefon, de nagyon népszerű kézi játékkonzol –, amely alkalmas webböngészésre és moziállományok lejátszására is. Különféle puffertúlcsordulás típusú hibákról sajnos itt is több ízben olvashattunk már. Ugyancsak sokan használnak BlackBerry készülékeket is. Itt már egy fokkal érdekesebb a helyzet, hiszen a levelek mellékletében már engedélyezett a DOC, PDF, TXT, WPD, XLS és PPT kiterjesztésű állományok használata. Szerencsére a HTML-alapú levelek és weboldalak esetén a szkriptelés nem engedélyezett, így legalább ezzel a veszélyforrással nem kell számolni.

Említhetjük még a szintén elterjedt iPodot és az Apple nagyágyúját, az iPhone telefont: ezekkel kapcsolatosan jelenleg szintén a sérülékenységek (exploit kódok) kiaknázása van terjedőben. Sokan azt jósolják, hogy ezek a UNIX-alapokon nyugvó rendszerek már idén a hackerek célpontjává válnak, de ez egyelőre erős túlzásnak tűnik.

És végül, de nem utolsósorban az összes operációs rendszer felett áll az az eset, amikor egy kártékony program folyamatosan jóváhagyást kérő ablakokkal bombázza szerencsétlen felhasználót. Aki az első pár alkalommal talán még óvatos, de a tizedik után már türelmetlenül és lemondóan csak megnyomja azt a fránya igen gombot.

Kényelem vs. biztonság

A kényelmi és automatikus funkciók szintén okozhatnak problémákat. Például a Nokia E90 telefonja, amely a Symbian 9 operációst rendszert futtatja, alaphelyzetben úgy van beállítva, hogy automatikusan WLAN-t keres, és arra külön kérdezés nélkül azonnal csatlakozik is. Az csak egy dolog, hogy ezzel mondjuk meríti az akkumulátort, de bizonyos, hogy lesznek olyan ezt kihasználható exploit kódok, amelyek segítségével már manipulálhatókká válnak e telefonok. Érdemes lehet például ezt a funkciót kikapcsolni.



Manapság már egyáltalán nem ritkaság, hogy GPS is legyen a kézi számítógépen

Amennyiben kényes adatokat is tárolnunk kell, célszerű valamilyen titkosítóprogramot bevetni: például Symbian alatt a Best Crypto 3DES-t (www.smartphoneware.com), amely bizalmas jegyzeteinket, a belépési

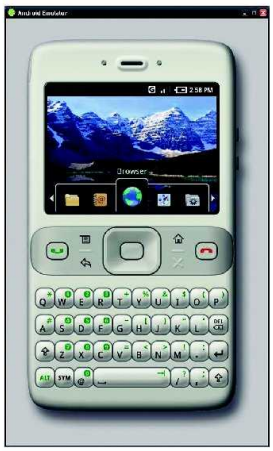
Ha a mobil kártevő éppen egy sima PC-s könyvtárban található, a vírusirtó korrektül felismeri

és PIN-kódjainkat tartalmazó szövegfájlt biztosan jobban megvédi, mint ha sima szövegként tárolnánk. Ennél is rafináltabb megoldás lehet még, ha a bizalmas adatok microSD-kártyáját, mondjuk egy olcsó 128 megabájtosat, nem is tartjuk állandóan a telefonban, hanem bérlettokban, pénztárcában. Így ha a telefont esetleg el is veszítjük, vagy ellopják, az adatok nem kerülnek veszélybe automatikusan.

A mobil már a statisztikák szerint is vonzó célpont

Ausztráliában a mobilok száma (21,26 millió) már meghaladja a lakosság számát. Kínában pedig 2007 óta a legnagyobb, China Mobile nevű mobilszolgáltatónak több ügyfele van, mint az USA teljes, 300 milliós népessége. A növekedés minden országban folyamatos, és egy biztos: a mobilokban és egyéb, online hozzáférésű „kütyükön" tárolt adatokra és az előfizetett szolgáltatásokra a jövőben fokozottan kell majd vigyáznunk. Amíg emberek kritikus (bizalmas, értékes, személyes) adataikat zömmel titkosítatlanul tárolják ilyen eszközökön, addig ezek ellopása, elvesztése, illetéktelen kezekbe kerülése, illetve az emelt díjas vagy más módon történő, pénzügyi kárt okozó machináció veszélye is fennáll. Ha veszélyekről hallunk, nem okvetlenül vírusként terjedő programokra, hanem a social engineering megtévesztő módszereit is bevető csalárd trójai programokra, hamis szoftverfrissítésekre, adathalász támadásokra, kéretlen reklámprogramokra, kémprogramokra, továbbá egy sor, csak mobileszközökön jellemző csalásra, például a Smishingre (valótlan tartalmú SMS-üzenettel kártékony weboldalakra csalogatják a címzettet) kell gondolnunk. Ha valamiben biztosak lehetünk, az az, hogy a rossz fiúk egyre újabb próbálkozásai a mobileszközök frontján sem maradnak el.

Különösen izgató nagyságúra fog nőni a mézesbödön a csalók számára azzal, hogy már hazánkban is napirenden van a mobillal való fizetés különféle szolgáltatások igénybevételekor, illetve akár áruvásárláskor is. A parkolócédulától a színes tévéig bármit vásárolhatnak a mi mobilunkkal mások is, ha online elérik. Szeretnénk?



A szép reményű Google Android széles körű elterjedése a jövőben a kártevőkészítők figyelmét is felkeltheti

***

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

www.eset.eu
bigyo.blog.hu
antivirus.blog.hu/2008/02/28/trojai_a_keziszamitogepen
www.freewareppc.com
www.symbian.com