Počítačové viry a červi dostaly své pojmenování pro podobnost s tvory reálného světa. Přestože se pohybují ve světě ryze kybernetickém, je velmi pravděpodobné, že se jejich chování i tam začne brzy podobat tomu, co dělají v prostoru živočišném. Nevěříte? Odpověď se skrývá v přenosných zařízeních.

Mobilní svět je ohrožen

Biologické ohrožení se šíří z počítačového světa na mobilní telefony

VOJTĚCH BEDNÁŘ

Počítačový virus je program, který má schopnost se automaticky šířit z jednoho počítače na druhý. Využívá k tomu stejného efektu jako virus z biologické říše. Umí totiž „napadat" jiné programy tak, jako virus napadá organismy, využívá je a bez nich by nemohl existovat.

Naproti tomu hlavním úkolem červa není parazitovat na aplikacích, ale na systémech. Tam, kde virus zneužívá hostitelský program nebo soubor a čeká, až jej někomu zkopírujete, červ je schopen se rozmnožovat s využitím různých technologií sám. Je založen na zneužívání známých vad a vlastností operačních systémů nebo běžně využívaného softwaru.

Krátká historie nebezpečí

Ačkoliv historicky se známými škůdci staly především viry, současnost patří hlavně a zejména červům. Počítače, které byly velmi dlouho vlastně jen jakýmisi osamocenými buňkami, propojenými jen tím, že jste z jednoho do druhého přenesli disketu, se podstatně změnily. V osmdesátých letech spolu s masovým rozvojem strojů typu PC a Mac přišlo první široké a dostupné využívání sítí. V malých sítích bylo několik počítačů, které spolu obvykle sdílely obsah několika adresářů, tiskárnu nebo skener. Na stejném principu pak pracovaly také síťové aplikace.

Viry se v tomto prostředí mohly šířit velmi rychle a i při použití konvenčních metod nakazit celou síť. Jejich soumrak přinesl až masový nástup internetu. V jeho prostředí se konvenční služby již tak masivně nepoužívají, jednotlivé počítače se alokují jinak a virová infekce má v jejich případě výrazně menší šance se rozšířit. Problematická je také otázka šíření virů v moderních operačních systémech. Ty často díky mechanice svého fungování nedávají virům dostatečný prostor, obsahují určitou „pasivní bezpečnost" a jsou odolnější. Nicméně jsou i složitější. A tato složitost jim dává novou vlastnost, zvýšené riziko přicházející od druhého typu škodlivého kódu – od červů.

Současnost nákaz

Červi představují většinu momentálně se šířících škodlivých kódů. Ke svému šíření využívají internet a jsou založeny na známých nedostatcích operačních systémů, především z rodiny Windows. Rodí se jich díky aktivním autorům poměrně veliké množství. Ačkoliv většina z nich „zapadne", nakazí jen několik málo počítačů a pak přestane fungovat, objevují se i takové, kterým se povede dosáhnout masového rozšíření po celém světě. I přes obranná opatření, přes firewally, přes antivirové aplikace. Boj proti červům tak spočívá především v odhalování mezer, které využívají, a v jejich záplatování, znemožňování zneužití. To má pochopitelně dvojí dopad. Kromě toho, že lepení mezer vede k jejich omezování, na druhou stranu se tím autoři červů informují a nové nebezpečné kódy tak vznikají mnohem rychleji, než by vznikaly jinak. Je to věčný souboj a věčné dilema.

Neposkvrněný mobilní svět

Zdálo by se, že svět červů, ochranných aplikací a podobných vymožeností je záležitostí úzce specifickou pro „velký" internet se světem počítačů typu PC. Dlouho tomu tak skutečně bylo. Nicméně v současné době existují obavy, že těžiště jejich nové aktivity se nachází přece jen někde jinde. Tím místem je svět přenosných zařízení a chytrých telefonů.

Vzít si některé informace z počítače s sebou na cestu jinak než je vytisknout nebo uložit na disketu byl dlouhodobý sen mnoha různých lidí z různých oborů. Tento sen se již v devadesátých let úspěšně uskutečňoval díky digitálním diářům, ty ale nebyly skutečnými počítači. Již před začátkem nového století se ale začala objevovat první skutečně chytrá datová mobilní zařízení, vybavená vlastními operačními systémy a s vlastnostmi, které se v mnohem podobaly tradičním velkým stolním zařízením. S přístroji vyzbrojenými platformami Palm OS, Pocket PC nebo Symbian se již můžeme setkávat naprosto běžně, existují i takové, které implementují v snadno přenosném malém těle operační systém Linux.

Přestože mobilní zařízení mají obvykle nějaké víceméně jasně stanovené poslání mobilního telefonu, čtečky elektronických knih, pokladního přístroje, evidenčního zařízení nebo komunikátoru, prakticky je v jejich možnostech fungovat jako klasický víceúčelový programovatelný počítač. Lze do nich nahrávat aplikace (což v případě digitálních diářů možné nebylo). Je možné tyto aplikace spouštět, a to i na pozadí operačního systému. Některé ze systémů jsou vybaveny multitaskingem, tedy schopností provozovat zároveň více než jednu aplikaci.

Vytvářejí tak prostředí, které je v mnoha ohledech podobné prostředí na PC. Nemluvíme samozřejmě o kompatibilitě aplikací, ale o podobné koncepci. A tam, kde je koncepce, se dříve nebo později objeví i podobné kódy. V našem případě viry a červi.

Škodlivé kódy se mobilnímu světu dlouho úspěšně vyhýbaly, mělo to dva důvody. Jednak naprogramovat virus či červa pro zjednodušený operační systém mobilního zařízení je mnohem obtížnější, než pro „velká" Windows. Druhým důvodem je otázka šíření. V případě PC lze spoléhat na určité pravidelně se opakující jevy. Používaná výměnná média jsou z hlediska systému kompatibilní, využívají stejné přístupové metody. To u malých přístrojů platí v omezenější míře, především při práci s paměťovými kartami typu flash, ale jinak ne. Další příčinou byla nesourodost a nekompatibilita operačních systémů, velké množství různých řešení, která se vyskytují v různých zařízeních, a omezená možnost přenosu kódu v přístrojích na stejné platformě, avšak rozdílné hardwarové konstrukce. A tak bylo možné donedávna používat palmy či chytré telefony relativně bez obav.

Pobláznění telefon

Klasické mobilní telefony typu GSM, jaké najdeme v kapse prakticky každého člověka, vlastně jednou už zažily obavy z šíření nebezpečných kódů. Ačkoliv na starší typ mobilu není možné instalovat další aplikace, naskytla se možnost zneužití vlastností jejich softwaru. Některé Nokie, ale také Ericssony či Siemensy je možné poškodit, „zbláznit" je tak, že na ně odešlete speciálně upravenou textovou zprávu, nebo tak, že je necháte z mobilní sítě přijímat data služeb, které podporují, v jiné podobě, než jak by měla tato data vypadat. To ovšem vyžaduje jednak bez výjimky speciální vybavení na straně útočníka, jednak problém i v GSM síti, která je velmi dobře hlídaná a neustále monitorovaná. Přesto se již koncem devadesátých let objevily úspěšné útoky. Jejich výsledkem byly telefony, které bylo pro další práci nutné restartovat, v horším případě pak svěřit odbornému servisu. Protože ale každý takový útok musel být směřován unikátním způsobem na unikátní typ zařízení, nepředstavovaly (i když vzbudily značný mediální ohlas) nijak signifikantní riziko. Nicméně znamenaly určitý počátek.

Chyba systému

O něco později, v době, kdy nebezpečné textové zprávy již zmizely za plentou jiných, zajímavějších událostí, se objevilo něco, co pomohlo spoluvytvořit obraz skutečného rizika a co se zpočátku jevilo jen jako prostý nedostatek, způsobený výrobci přenosných zařízení. Kombinace určitých telefonů s určitým příslušenstvím vedly k potížím. Ve světě PC bychom to nazvali hardwarovou nebo protokolární nekompatibilitou a velké počítače s tím jednu dobu urputně bojovaly. To, co lze na PC vyřešit s přehledem, však v mobilním světě představuje problém. Přenosná zařízení začala být vybavována technologiemi, které měly usnadnit jejich používání a dodat jim novou funkcionalitu – schopnost komunikovat navzájem. Přišla bezdrátová rozhraní: nejprve v podobě infračervených portů, posléze jako dnes již poměrně rozšířená technologie bezdrátového přenosu Bluetooth. Obojí umožňuje vzájemnou datovou komunikaci mobilního přístroje s jiným mobilním přístrojem nebo s počítačem. Zatímco v případě infračerveného portu musí být obě zařízení tak říkajíc v přímém dosahu, u Bluetoothu tomu tak není. Spolu s komunikačním rozhraním však přichází i jeho chyba. A tak některé mobilní telefony, jsou-li používány s některými bezdrátovými sluchátky, mohou havarovat, některá infračervená rozhraní, přesněji jejich využití způsobuje (či v minulosti způsobovalo) jejich pády nebo dezorientaci a navíc, stále existuje problém možné interference takové komunikace s jinými přístroji. A to je poněkud problematická věc.

Tento detail, tedy obyčejná nekompatibilita, se stal předlohou k asi největšímu ohrožení, jakému mobilní inteligentní přístroje zatím čelily, a je velmi pravděpodobné, že mu v budoucnu budou čelit ještě více. Vyřešily se tím totiž obě problematické otázky spojené se škodlivými kódy. Tedy jak je naprogramovat a jak je rozšířit.

První vzorky

První antivirové aplikace pro mobilní přístroje se objevily v okamžiku, kdy začalo být zřejmé, že se platformy, na nichž tyto přístroje pracují, začínají čím dále tím více homogenizovat. V současnosti existují pro přenosné přístroje tři vysoce a celosvětově rozšířené operační systémy. Prvním z nich je platforma Windows Mobile (Pocket PC alias Windows CE) od společnosti Microsoft. Za ní následuje systém Palm OS. Posledním je pak systém Symbian, vyvíjený konsorciem jeho dodavatelů. První dva systémy se hojně vyskytují v přenosných počítačích a v chytrých telefonech, i když první použití je pro ně typické. Symbian je naproti tomu v současné době jednoznačným králem inteligentních mobilních telefonů. Ty jsou stále více a více rozšířené spolu s tím, jak klesají jejich ceny. Inteligentní telefon je po technické stránce velice podobný zařízení typu PDA, pouze mu chybí některé jejich typické znaky a má navíc to nejdůležitější – schopnost telefonovat. I když většina uživatelů asi příliš dodatečných aplikací například do dnes již zastaralé Nokie 7650 instalovat nebude a zda použije Bluetooth či infračervený port, je také sporné, nemění to nic na faktu, že tento mobil (a mnoho dalších typu i výrobců) je vlastně počítačem. Se všemi riziky s tím spojenými.

I přes existenci antivirových programů chyběl o dlouho to nejdůležitější – tedy virus. Existovaly, pravda, viry či červi napsané za účelem testování, ale pokud se na PDA nebo smartphonech nějaký skutečný škodlivý kód objevil, jednalo se obvykle o trojského koně. Trojský kůň je program, který dělá něco jiného, než má. Nedávno rozčeřil hladinu zájmu program pro Symbian, cracknutá pirátská verze hry Mosquitos. Pirátská hra totiž kromě toho, že funguje, také odesílá textové zprávy na velmi vysoce zpoplatněné číslo ve Velké Británii. Výsledkem je, že majitel si sice zahraje zadarmo, ale přijde o spoustu peněz. Jiný trojský kůň se objevil (byl slavně objeven nedávno) pro Palm

OS. Opět zatímco hrajete hru, tato hra vám z vašeho kapesního počítače maže uložená data. A to je také velmi nepříjemné.

Poslední zmíněná platforma, Windows CE, již byla napadena také, autorem prvního funkčního červa byl podle všeho Čech. Přestože červ se „pouze šířil" a navíc na sebe majitele zasaženého handheldu upozornil, aniž by něco vymazal, je i toto určitá hrozba. To vše jsou ovšem jen první vzorky, po nichž může následovat větší pohroma.

Experiment

Student jedné české vysoké školy, který se nechce stát známým, a tak jej nebudeme jmenovat, naprogramoval svou vlastní verzi piškvorek, rovněž pro operační systém Symbian. Piškvorky se dají hrát tak, jako každé jiné – liší se v jediném. A tím je schopnost automaticky se šířit na další kompatibilní zařízení. Využívají k tomu vlastností použitého operačního systému. A tak pokud máte telefon se Symbianem a zapnutý Bluetooth, může se vám stát, že po náhodném setkání s člověkem, který má tyto piškvorky ve svém telefonu, aniž byste onoho člověka znali či s ním vůbec promluvili, zjistíte, že máte o jednu hru navíc. Právě zde začíná doba, kdy se čistě kybernetický kód začíná přibližovat biologickému. Mobilní telefon totiž na kompatibilního kolegu hru doslova kýchne. Používá k tomu funkci, kterou se běžně posílají z jednoho přístroje na druhý vizitky. Této technice se říká útok na Bluetooth, tedy bluejacking. Existuje reálná hrozba, že právě tímto směrem se v budoucnu bude ubírat vývoj mobilních škodlivých kódů. Bohužel.

Jeden na všechny?

Problém mnoha různých platforem a jejich vzájemné nekompatibility má poněkud překvapivé řešení. Je totiž možné naprogramovat například červa, který bude na kapesním počítači fungovat stejně, jako na jiném zařízení s odlišným operačním systémem. Všechny přístroje umožňují ukládat prakticky jakákoliv data (pokud jsou správně zabalená) a umí odlišit, co je datový soubor, například obrázek, od toho, co je programem a má být spuštěno. Když vytvoříme dva identicky fungující programy pro dvě různé platformy a zabalíme je tak, že vždy ta část, která je určena pro jinou platformu než je aktuální, se bude chovat jako datový soubor, máme vyhráno. Jeden červ by se tak mohl šířit napříč platformami, využívat toho, že takřka všechna zařízení jsou na komunikační úrovni kompatibilní. Vytvořit hybridní program je sice obtížnější, než udělat mobilního červa, nicméně to není nemožné a zdá se, že i v tomto případě se jedná spíše o nastupující skutečnost než o hudbu středně až velmi vzdálené budoucnosti.

Jsem nezranitelný!

Obranná opatření jsou zatím v případě mobilních zařízení v zárodcích. Konvenční antiviry sice existují, ale je obtížné posoudit, zda jsou v tomto případě vůbec použitelné. To je otázka, na kterou nikdo nezná uspokojivou odpověď. Komunikační rozhraní mobilních přístrojů jsou, podobně jako systémy, v mnoha případech vybavena obrannými mechanismy. Aplikace pro některé systémy (Symbian, Windows CE) mohou být digitálně podepsány a podpis je známkou jejich vydavatele zajišťující bezpečnost. Komunikace pomocí bezdrátového rozhraní je možná pouze za předpokladu, že si přístroje vyměnily speciální autorizační klíče, což požaduje obvykle zásah uživatele. Ze všech těchto postupů ale existují ryze praktické výjimky. A škodlivé kódy se budou ubírat cestou těchto výjimek, díky nimž mohou fungovat například i ty periferie, u nichž by to jinak nebylo za přesného dodržení daných standardů možné.

Tak, jak se operační systémy staly homogenními, univerzálnějšími a kompatibilnějšími, staly se i zranitelnějšími. Stejně jako lze ve Windows najít mnoho bezpečnostních nedostatků, založených na běžných jevech (přetečení zásobníku), lze je hledat i u Pocket PC nebo u Palm OS. Stačí k tomu pouze mít dost času. Zatímco záplatování „velkých" systémů je přinejmenším technicky možné poměrně snadno a také je vyzkoušené, stejná činnost u kapesních přístrojů se snadno změní v noční můru. Jejich operační prostředí je uloženo v paměti typu Flash, nezřídka dokonce v ROM a podstatný update nepřipadá proto vůbec v úvahu. Antivirus pak zabírá místo, kterého je v přenosném přístroji vždy jedině málo, navíc vyžaduje speciální údržbu a péči. A především potřebuje zájem ze strany uživatele. Většina lidí, kteří používají například již zmíněnou Nokii 7650, se přitom o cokoliv dalšího, na rozdíl od PC, starat nechce. Žádají, aby to fungovalo a otevírají tak cestu potenciálním útočníkům. Jak to může vypadat?

Prognóza

Uvedený příběh byl samozřejmě smyšlený, ale není daleko doba, kdy se něco podobného může stát. Stačí k tomu poměrně málo. Hlavně ve velkých městech s hustou veřejnou dopravou a velkým počtem míst, kde je hodně lidí v blízkém kontaktu, je poměrně běžné, že se snadno šíří přenosné choroby, jako je chřipka. A v budoucnu je možné i to, aby se stejným způsobem šířily přenosné choroby mobilních zařízení. Pokud jde o chřipku, jistě jste si již položili otázku, odkud se bere. Kdo se nakazil jako první? A odkud? Odpovědí na tuto otázku může být mnoho a stejně tak je tomu i v případě elektronických infekcí. Červi mohou být šířeni záměrně svými autory nebo roznašeči. Mohou se do zařízení dostat společně s nevinně se tvářícími programy u uživatelů, kteří instalaci aplikací pravidelně používají. Stejně tak je možné i zavlečení z internetu. Mnoho mobilních zařízení je využíváno například ke čtení elektronické pošty. A tak jako se automatičtí červi šíří ve světě Windows a PC například útokem na otevřené porty počítačů, mohou se šířit i mobilní kódy analogickým útokem na kapesní přístroje. Přestože to vypadá na první pohled poněkud fantasticky, éra bioelektronických infekcí se blíží. Nebo dokonce je již zde, jen o tom prozatím nevíme. 4 0499/FEL ❑

Příběh jednoho týdne

Byla neděle a měli jsme firemní oslavu. Takovou párty v hospůdce u příležitosti dokončení velké zakázky. Šéf rozléval jako divý a já jsem jako divý konzumoval, což jsem neměl dělat.

V pondělí ráno jsem se probudil, jako každý den. Bolela mne hlava, kýchal jsem, tušil zvýšenou teplotu a beznadějně použitý kapesník po mém boku jasně říkal, že chřipka je zde. Tak jsem se omluvil z práce a vydal se k lékaři. Po krátké jízdě tramvají a chůzi přeplněným městem jsem dorazil do čekárny. Byla plná podobně chorých lidí.

Lékař mne prohlédl, pokýval hlavou a vypsal recept. Došel jsem domů, vzal si léky a jal se potit pod dekou. Neměl jsem chuť vůbec na nic.

V úterý mi bylo už o něco lépe. Televize mne nebavila, knihu se mi číst nechtělo, a tak jsem vzal do ruky mobil, že si zahraji hru. Byl nějaký divný. Menu šlo pomalu, střílení kuliček bylo také zaseklé, asi nemám špatný den jenom já, ale i ta hromádka elektroniky. Nechal jsem toho.

Ve středu jsem chodil po bytě a díval se na televizi. Můj telefon úplně přestal reagovat. Ani když jsem ho vypnul a zase zapnul. Volal jsem z pevné linky šéfovi, ale celé dopoledne ho nešlo sehnat. Nechal jsem mu vzkaz v hlasové schránce, ale stejně je to nějaké divné, náš boss si mobil nikdy nevypíná a žertovali jsme, že ho má v posteli místo medvídka.

Čtvrtek. Cítím se díky lékům docela dobře, ale nesmím se moc hýbat. Mobil je mrtev, ale volal mi šéf. Má podobný telefon a stalo se mu přesně to samé. A co hůře, jeho bratrovi, který má Siemens, jakbysmet. Vůbec tomu nerozumím.

Pátek. Byl jsem na kontrole a vypadá to, že v pondělí můžu zase do práce. Doktor si mi postěžoval, že se mu pokazil telefon. No tohle není náhoda. Já vážně nevím.

Rozuměli jste tomuto příběhu? Jeho hrdina dostal jednotýdenní chřipku, ale jeho mobil také. Na firemním večírku se pomocí technologie Bluetooth „nakazil" od telefonu nadřízeného. Když bylo našemu hrdinovi v pondělí špatně, podělil se o mobilního červa s lékařem, který jej vyšetřoval. V následujících dnech začal červ působit. Nejdříve odešel ten telefon, který byl nakažen jako první, a hned po něm všechny ostatní. Tedy v pořadí šéfův bratr – šéf – hrdina příběhu – lékař. Aby toho nebylo dost, nakazil se aktér tohoto příběhu ještě i klasickou chřipkou, což mu způsobilo týdenní dovolenou. Život je někdy ironický.