AEC Virus Eye

Obsah:

www.aec.cz

Pro PC WORLD připravuje Tomáš Přibyl - tomas.pribyl@aec.cz

AEC ROADSHOW 2004

Stejně jako v uplynulých letech se také letos v září se bude konat úspěšná akce „AEC roadshow", jejímž cílem je především zpřístupnit problematiku IT bezpečnosti také zájemcům mimo tradiční oblasti. Inu, je to tak – konference a semináře v největších městech dnes pořádá kdekdo, ale ostatní lokality bývají (neprávem) stranou pozornosti. A tak i letos dostanou příležitost seznámit se s nejnovějšími trendy informační bezpečnosti, tipy, triky, návody, moderními bezpečnostními programy či postupy zájemci v Brně (úterý 14. září), Pardubicích (středa 15. září), Českých Budějovicích (čtvrtek 16. září), Liberci (úterý 21. září), Mostě (středa 22. září) a ve Zlíně (čtvrtek 23. září).

Na AEC roadshow 2004 zazní přednášky věnující se následující problematice:

- Škodlivé kódy včera, dnes a zítra.
- Metodika zavádění elektronického podpisu.
- Seznámení s řešením elektronické podatelny.
- Představení produktů a služeb společnosti AEC.
- Antivirová programy z nabídky F-Secure.

Semináře jsou po předchozí registraci na webu roadshow.aec.cz ZDARMA.

- AEC si vyhrazuje právo odmítnout přihlášku na seminář bez udání důvodu.
- Počet účastníků ZDARMA je omezen na dvě osoby z jedné firmy/organizace (v případě většího počtu zájemců nás prosím neváhejte kontaktovat na e-mailu tomas.pribyl@aec.cz).
- Vstup ZDARMA platí pouze pro osoby, které se předem zaregistrovaly na webu roadshow.aec.cz a při příchodu na akci se prokáží planým registračním číslem.

Pořadatel si vyhrazuje právo změny místa konání, programu nebo termínu – pro nejnovější informace sledujte ROADSHOW.AEC.CZ

AEC roadshow 2004 společně připravila společnost AEC Data Security Company (www.aec.cz), redakce měsíčníku PC World (www.pcworld.cz) a finská společnost F-Secure (www.f-secure.com).

CABIR: PRVNÍ ČERV VYUŽÍVAJÍCÍ BLUETOOTH

Antivirové firmy hlásí výskyt prvního červa, který se dokáže šířit prostřednictvím bluetooth po zařízeních s operačním systémem Symbian EPOC Series 60.

Tento červ, který je označován jako Cabir, byl podle dostupných informací vytvořen členy známé skupiny pisatelů virů „29A". Tato skupina se zabývá tvorbou tzv. „proof-of-concept" škodlivých kódů, které se sice většinou nešíří „In-the-Wild", ale snaží se ukázat technologie a postupy zneužitelné v „ostrých" virech.

Cabir se šíří ve formě SIS souboru, který se na další zařízení přenáší pomocí bluetooth spojení. Snaží se přitom maskovat jako utilita Caribe Security Manager, která je součástí bezpečnostního software systému Symbian. Pokud uživatel následně SIS soubor s červem nainstaluje, spustí tím červa, který se snaží z infikovaného zařízení šířit dále.

Činnost červa se může projevovat také snižováním kapacity baterie, která je více zatěžována častým používáním bluetooth. Manuální dezinfekci můžete provést vymazáním souborů červa z paměti zařízení.

DUTS: PRVNÍ VIRUS PRO WINDOWS CE

V pátek 17. července 2004 světové antivirové firmy zaznamenaly existenci prvního počítačového viru pro platformu Windows CE (resp. Pocket PC). Jeho šíření „In the Wild" se však neočekává.

Duts je parazitický infektor, který infikuje všechny EXE soubory vyskytující se v adresáři, kde byl spuštěn. Přidává do nich svůj kód, čímž se jejich velikost zvětší asi o 1,5 kB. Vícenásobné infekci zabraňuje vytvořením příznaku v jeho hlavičce.

Protože se jedná o tzv. „hodný virus", žádá před zahájením infekční rutiny uživatele o svolení prostřednictvím dialogového okna.

Duts ve svém kódu virus obsahuje vzkazy od autora:

This code arose from the dust of Permutation City
This is proof of concept code. Also i wanted to make avers happy. The situation when Pocket PC antiviruses detect only EICAR had to end...

ŠKODLIVÉ KÓDY A MOBILNÍ ZAŘÍZENÍ

Mobilní telefon má dnes prakticky každý. Výrobci se předhánějí v nabídce přístrojů – v jejich rozmanitosti, tvarech a především v množství funkcí. Vzhledem k tomu, že mobilní zařízení se staly prostředkem masové komunikace, je celkem logické, že se k nim upřela i pozornost tvůrců škodlivých kódů. Byť „zavirovat" současný mobil je stejně vyloučeno jako zavirovat kapesní kalkulátor nebo digitální hodinky, situace na tomto poli se do budoucna s příchodem sofistikovanějších přístrojů s pokročilým rozhraním rozhodně změní. A rozhodně ne k lepšímu.

Potencionálních problémů v oblasti mobilních komunikací je přitom hned několik. Především je zde riziko, že si uživatelé ze současné generace mobilních zařízení zapamatují právě skutečnost, že jsou bezpečné. A s příchodem složitějších strojů a vznikem nových typů útoků si budou na změněnou situaci těžko zvykat.

Současné škodlivé kódy potřebují k šíření z počítače do počítače znát „adresu" – potřebují vědět, kam se mají vydat. Viry a podobná „havěť" na mobilních telefonech se přitom bez podobné informace vcelku obejdou, neboť jim bude stačit náhodně generovat čísla (náhodně generovat e-mailové adresy jde asi dost těžko). Jinými slovy, záběr „mobilních" počítačových virů bude poněkud širší než těch současných počítačových. (Ostatně, stačí si vzpomenout na léto 2001 a případ škodlivého kódu CodeRed, který se šířil výhradně po počítačových serverech, díky čemuž si mohl dovolit náhodně generovat IP adresy. Šířil se jako mor na všechny strany rychlostí nevídanou…)

Jak už bylo jednou uvedeno, škodlivé kódy se zatím prakticky netýkají mobilních zařízení (i když první průkopníci se již objevili – viz níže). Na druhé straně je ovšem třeba si uvědomit, že tato situace nebude trvat věčně. Je jen otázkou, zdali ke změně dojde za dva či čtyři roky.

A jak to tedy vypadá se „stavem škodlivých kódů" pro mobilní aplikace? Možná to zní až neskutečně, ale skutečně už se objevily první větší útoky na mobilní zařízení, včetně nejrozšířenějších mobilních telefonů.

V roce 2000 způsobil poměrně velký rozruch virus **Timofonica.** Šlo o škodlivý kód, který byl napsaný v jazyce VBS (Visual Basic Script) stejně jako např. slavný Iloveyou. Timofonica se šíří e-mailovou zprávou, přičemž využívá bezpečnostních slabin aplikace MS Outlook a naivity uživatelů. Virus je v příloze e-mailové zprávy (ta má předmět „Timofonica" a španělsky psaný text), která se jmenuje TIMOFONICA.TXT.vbs.

Pokud dojde k nejhoršímu a uživatel připojený soubor spustí, Timofonica rozešle své kopie na všechny adresy ze seznamu MS Outlooku. Po každé odeslané zprávě navíc vygeneruje náhodné číslo a na e-mailovou adresu (náhodné číslo)@correo.movistar.net odešle zprávu „informa que: Telefănica te estˇ engaáando.” Adresa correo.movistar.net je přitom SMS bránou, která distribuuje uživatelům mobilních telefonů e-mailové zprávy. A tak dochází k tomu, že Timofonica spamuje (tedy obtěžuje nevyžádanou poštou) uživatele mobilních telefonů.

Známe již také první virus pro Palm OS pojmenovaný **Phage**, který napadá a infikuje aplikace (resp. PRC soubory). Pokud je infikovaná aplikace spuštěna, je displej Palmu pokryt šedými čtverečky a jsou infiltrovány všechny ostatní aplikace. Infikování probíhá tak, že virus přepíše první sekci hostitelova PRC souboru svým vlastním kódem. Uživateli nezbývá než napadený Palm „natvrdo“ restartovat a obnovit celý obsah ze zálohy na osobním počítači pomocí HotSync. Jak je tedy vidět, i tak jednoduchá platforma, jako je Palm OS, se může stát cílem virového útoku.

Dalším škodlivým kódem pro Palm OS je trojský kůň **Liberty**, který se objevil v srpnu roku 2000. Skrývá se v souboru vydávajícím se za crack na Liberty Gameboy emulator 1.1. Na displeji se zobrazuje jako ikona aplikace s názvem „Crack 1.1“. Pokud je škodlivý kód spuštěn, vymaže všechny instalované aplikace a zařízení restartuje. Přes jeho výraznou škodlivou rutinu jej nelze označit za virus v pravém smyslu slova, protože nesplňuje základní podmínku – svoji replikaci a šíření.

Mírnější účinky na systém kapesního počítače má trojský kůň **Vapor**, který v systému Palm OS nastavuje všechny aplikace jako skryté, takže nejsou jejich ikony vidět na displeji. Kromě možné paniky uživatele nepůsobí další škody.

Jiným trojským koněm, tentokrát pro platformu EPOC, je prográmek **Lights**. Jeho projevy jsou spíše humorné. Nepodniká nic jiného, než že rozsvěcuje a zhasíná podsvětlení displeje a snaží se tak vybíjet baterie. Dalším humorným prográmkem, který ale rozhodně nelze považovat za virus ani trojského koně, je program nazvaný **Disowner**, který v systému EPOC mění informace o uživateli na „Some fool owns this“.

Jak vidno, mobilní platformy se už staly středem zájmu hackerů a pisatelů škodlivých kódů. Proto se podívejme jen na několik nejběžnějších nebezpečí, se kterými má běžný smrtelník možnost se nejvíce setkávat.

Rozhodně se nikdy nepodaří zcela eliminovat možnost „hardwarové příhody". Sem patří nejen odcizení či poškození hardware (vhodně převržený šálek kávy či váza rozhodně udělá své), ale třeba i jeho opotřebování časem. Ač se tyto hrozby dají eliminovat, nikdy se je nepodaří vyloučit zcela. Na všechny (i níže uvedené) je přitom zaručený a odzkoušený recept: Zálohování, zálohování a zase zálohování.

Velmi jednoduchou metodou útoku je použití sociálního inženýrství. Nevyžaduje žádné zvláštní znalosti, stačí jen dobrý nápad na který se nicnetušící člověk chytí. V českých krajích zatím (naštěstí) ještě ne, ale v zahraničí jsou běžné SMS zprávy „Dobře tě znám a mám tě rád/a, ale stydím se ti zavolat, abych ti to řekl přímo. Zavolej mi, lásko, na toto číslo…" Uvedené číslo ale znamená spojení na drahou telefonní linku, nezřídka do zahraničí.

Jinak se dá předpokládat, že mobilní škodlivé kódy budou mít podobné projevy a cíl útoků jako v současnosti rozšířené počítačové viry. Škodlivé kódy budou data likvidovat, zneužívat či modifikovat. V těchto útocích je přitom velká síla i nebezpečí zároveň – když někdo něco odcizí v reálném světě, jsou následky konání ihned viditelné. V kybernetickém prostoru lze donekonečna kopírovat data – a miliónta kopie přitom stále vypadá absolutně stejně jako originál. Jen s tím rozdílem, že originál jaksi nikomu nechybí.

Velice často zmiňované nebezpečí představují bezdrátové přenosy. Třeba viry, které budou „přeskakovat" z jednoho kapesního počítače na druhý pomocí infračerveného přenosu. Bude stačit jen se projít po nějakém veletrhu. To už budou skutečné „viry", jak je známe z biologického světa („majitelům citlivějších PDA se dnes doporučuje nevycházet a omezit pohyb mezi lidmi, neboť se objevila epidemie viru však-víš-který"). Sci-fi? Ale kdeže! Stačí i v současné době se projít po kancelářských budovách s trošičku citlivějším přijímačem a posbíráte neuvěřitelné množství zajímavých informací. Bezdráty jsou v módě – tiskárny, klávesnice, myši… A s nějakým stíněním nebo zabezpečením se zatím nikdo neobtěžuje.

A jaká je tedy v případě mobilních zařízení obrana a ochrana? Samozřejmě, že různé hrozby (některé jsou v současné době spíše tušené) vyžadují různá řešení a různé „odpovědi". Ještě jednou bychom ale připomněli nezbytnost zálohování. Bez něj můžete přijít o více, než si dokážete představit (zkuste na chvíli zavřít oči, představit si, že se váš osobní počítač najednou „vypaří" – kde máte zálohy? Jak dlouho by trvalo obnovení dat? Podařily by se všechny informace vrátit bezezbytku do původní podoby?)

Druhou poměrně univerzální radou je **šifrování** dat. Šifrování zajistí, že k datům bude mít přístup pouze oprávněná osoba (resp. okruh oprávněných osob) – majitel dešifrovacího klíče a hesla. Data jsou pak chráněna i v případě odcizení nebo ztráty příslušného mobilního zařízení.

Elektronický podpis (ač v plenkách i ve světě „běžných" počítačů) také dokáže zabránit mnoha nepříjemnostem. Bezpečně určí původce zprávy či autora dokumentu, takže následně může odpadat zdlouhavé a náročné dokazování a dohledávání. Stejně tak může být elektronický podpis použit jako zbraň proti počítačovým/mobilním virům. Zpráva elektronicky podepsaná má samozřejmě vyšší stupeň důvěryhodnosti – a navíc je zřejmé, že nebyla vygenerována škodlivým kódem.

Stejně tak se dříve či později stane nezbytností **antivirový program** – ostatně, jako se tomu stalo v případě běžných počítačů. Škodlivé kódy se rozhodně budou do mobilních zařízení tlačit ještě agresivněji než do počítačů.
Podtrženo, sečteno – i v oblasti mobilních komunikačních zařízení se slovíčko „bezpečnost" stává frekventovaným a uznávaným pojmem. A časem rozhodně nebude ztrácet na významu.

[KONEC magazínu AEC VIRUS EYE]