AEC
DATA SECURITY COMPANY

Magazín

Milí přátelé!
Vítáme Vás při četbě našeho informačního bulletinu, který má za cíl seznámit Vás s novinkami na poli virů, antivirů a bezpečnosti dat všeobecně.

Z dnešního obsahu vybíráme:

Příjemné počtení a co nejméně potíží s viry a zabezpečením dat přeje Vaše firma AEC, spol. s r.o.

SECURITY 2001 - POD PRAPOREM POČÍTAČOVÉ BEZPEČNOSTI

Již od roku 1992 pořádá společnost AEC konference, věnované problematice počítačových virů, antivirové ochraně a související problematice. Letos si Vás dovolujeme pozvat na již šestý ročník konference zaměřené na ochranu a bezpečnost dat stejně jako na antivirovou problematiku.
Při loňském (pátém) ročníku akce Vás mohla překvapit změna názvu akce (dříve Virus, nyní vzhledem ke stále širšímu záběru bezpečnostní problematiky Security) - také nyní dochází k další radikální změně. Tou je periodicita konference - dosud se konala jen v letech sudých. Ovšem vzhledem k neutuchajícímu zájmu o počítačovou bezpečnost a otázky s ní související a také vzhledem k překotnému vývoji na poli IT security jsme se rozhodli konferenci pořádat každý rok. V souvislosti s tímto jsme obvyklou dvoudenní akci zredukovali do jednoho dne. A tak se i letos setkáme na konferenci Security 2001, a to ve čtvrtek 7. června 2001. Konferenci pořádáme za mediální podpory vydavatelství Vogel Publishing (Chip, Počítač pro každého, IT Net, Level, Media Shop). Těšíme se na setkání v červnu!

Bližší informace lze nalézt na www.security2001.cz

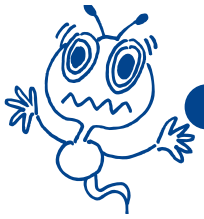
BEZPEČNOST ELEKTRONICKÉHO PODPISU: BOUŘE VE SKLENICI VODY

Začalo to stručným oznámením, pak následovala tisková konference a velké diskuse v tisku často přecházející až téměř do podněcování hysterie okolo základů elektronického podpisu („Elektronický podpis není bezpečný“, „Konec elektronického podpisu v Čechách“ apod.).

Co se tedy za tím vším skutečně skrývá? Nejprve - útok, který pánové Rosa a Klíma popsali, je skutečně reálný a opodstatněný. Týká se způsobu práce se soukromým klíčem v PGP, přesněji postupů jakým je tento klíč uchováván. Existující implementace vychází z doporučení rfc2440, OpenPGP Message Format. Autoři ukázali, že doporučení daná touto normou nejsou z hlediska kryptografické ochrany soukromého klíče dostatečná. Co víc, ukázali, že existující implementace PGP (včetně posledních verzí) nejsou vůči jimi popsaným útokům odolné. Toto se týká podpisů, které jsou v PGP vytvářeny algoritmem DSA. Algoritmus RSA je naštěstí v PGP ošetřen ještě dodatečnou kontrolou integrity datového souboru, ve kterém leží zašifrovaný soukromý klíč a popsaný útok není dle autorů tedy přímo aplikovatelný.

Pro úspěšnost útoku je třeba zabezpečit, aby útočník měl buď přístup k počítači napadeného uživatele, nebo se k němu mohl dostat přes síť, resp. měl přístup k nějakému počítači, ve kterém se vyskytuje exportovaný zašifrovaný soukromý klíč uživatele (ve formátu OpenPGP).

Vůči PGP je to poměrně nepříjemný úder. Analytikové se shodují, že bude třeba připravit příslušné úpravy všech verzí, kterých se to týká.



Logicky se objevují doporučení nevytvářet ukvapená řešení, ale provést hlubokou analýzu protokolu a vytvořit nový (snazší) přístup k formátům, ve kterých jsou soukromé klíče v PGP ukládány spolu s využitím dalších kontrol integrity příslušného souboru dat.

Přes svou rozšířenost je PGP označováno jako proprietární řešení. Je to z celé řady důvodů. Některé okruhy otázek jsou totiž v těchto produktech řešeny postupy, které platí výlučně pro software PGP (namátkou PGP/MIME, koncepce důvěry, zmíněné formáty, atd.). Nemají však pravdu ti, kteří hovoří o tom, že PGP není systém, kterého by se týkal zákon o elektronickém podpisu. Je to jeden z mnoha možných způsobů, kterým lze k využívání elektronického podpisu dospět a např. při existenci odpovídající smlouvy zúčastněných stran má takovýto podpis i všechny náležitosti z hlediska zákonných dopadů.

Na druhou stranu je nutné říci, že profesionální řešení, která jsou připravována pro řešení elektronického podpisu (ve světě ale i u nás) vychází v daném ohledu z jiných principů a doporučení. Takováto řešení jsou připravována pro využití i v ČR (ať už ve státní či soukromé sféře).

Není tedy naprosto žádný důvod propadat jakékoliv panice.

Z WINDOWS DO LINUXU - A ZASE ZPÁTKY

Světlo světa spatřil první multiplatformní virus, který se cítí „jako doma“ nejen v systémech

Windows 9x/NT/2000, ale také v prostředí Linuxu. Jeho jméno je Winux (některé antivirové programy jsou ovšem schopné detekovat jej pod mírně odlišnými názvy).

Winux ukázkou zajímavé možnosti řešení daného problému. Tomuto tvrzení nahrává i skutečnost, že neprovádí žádné destruktivní činnosti. Faktem však zůstává, že jakmile se jednou nalezne (leč neškodné, ale fungující) řešení, je jen otázkou času, kdy z něj někdy v budoucnosti vznikne daleko nebezpečnější škodlivý kód.

Winux se může šířit v prostředích Windows 95/98/Me/NT/2000 a Linux a napadat nejen spustitelné PE EXE soubory (Windows), ale i ELF soubory (Linux). Jeho šíření probíhá prostřednictvím sdíleného prostoru mezi Windows a Linux počítači.

Metoda napadení souboru je celkem primitivní. Virus "pouze" přepíše *.reloc sekci *.EXE souboru. Pokud je pro něj příliš malá, zůstane soubor nákazy ušetřen. Činnost viru nepoškozuje data, ale pouze snižuje výkon napadeného počítače. *.ELF soubor je taktéž napaden tímto způsobem. Pokud je napadený soubor spuštěn, virus převezme kontrolu, rozšíří se a vrátí kontrolu zpět hostitelskému souboru. V těle *.ELF souboru je virus uložen na jeho konci.

Winux.Linux ve svém těle obsahuje následující text:

[Win32/Linux.Winux] multi-platform virus byBenny/29A" and "This GNU program is covered by GPL.

MAGISTR - DALŠÍ NEBEZPEČÍ V E-MAILU

Magistr se šíří prostřednictvím e-mailu a pomocí sdílení přes lokální sítě. Podle dostupných informací se "narodil" ve Švédsku v dílně hackera známého pod pseudonymem "The Judges Disemboleweler" (podle komentáře nalezeného v těle viru). Červ používá široký repertoár technik sloužících k zakrytí jeho existence a činnosti.

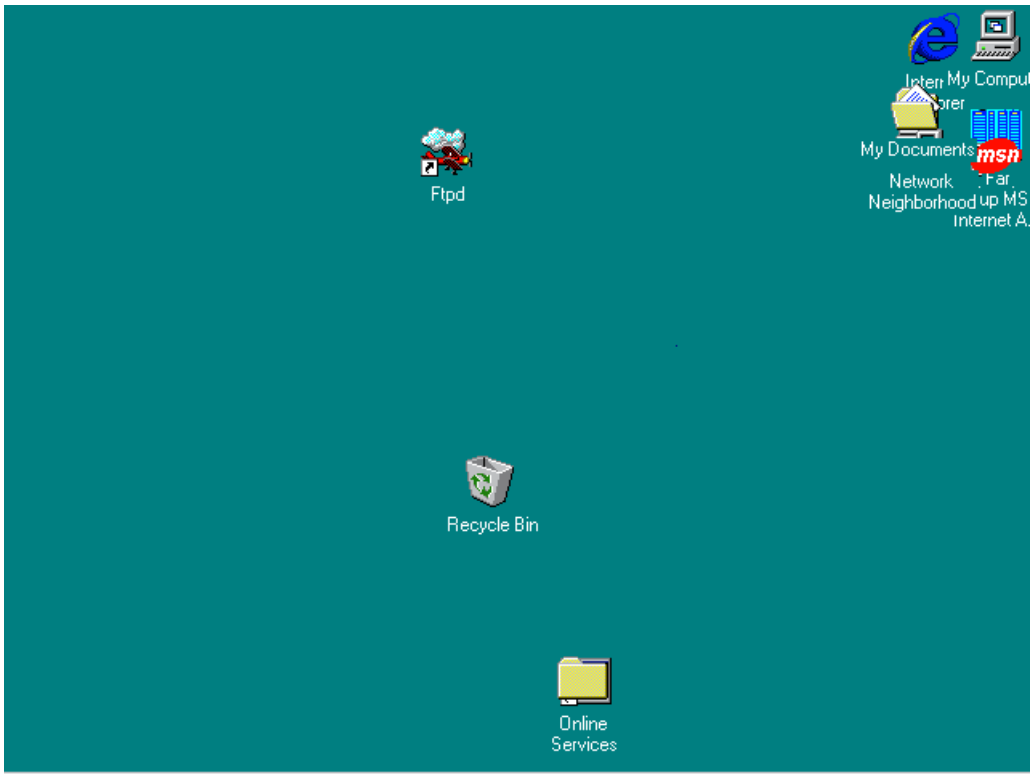
Jakmile je soubor napadený Magistrem spuštěn, virus začne běžet na pozadí, a po krátkém čekání spustí svoje vykonávací rutiny: lokální a síťovou infekci Win32 exe souborů, samošíření pomocí e-mailu atd. Červ zajišťuje svoji rezidentnost prostřednictvím součásti systému Windows explorer.exe. Při prvním spuštění také napadne (většinou první) soubor v adresáři Windows, který infikuje a zaregistruje ho v auto-run registru a ve win.ini. Tím si zajistí svoji aktivaci při každém restartu počítače. Vložená procedura v napadeném programu není spuštěna, pokud před tím červ neprovedl výše popsané úkoly. V opačném případě je aplikace zrušena a místo ní se spustí virus. Tím se vyhne vedlejším účinkům svého spuštění a zbytečně na sebe neupozorní.

Magistr prohledává všechny lokální a sdílené síťové disky, pátrá po adresářích WINNT, WINDOWS,WIN95, WIN98 a následně jejich obsah popsaným způsobem infikuje. Pro vlastní použití vytváří soubor *.dat. Jméno a umístění tohoto souboru záleží na jménu sítě nebo počítače.

Pro hromadné rozesílání sebe sama virus používá databáze emailových adres (Outlook Express, Netscape Messenger, Internet Mail and News). Vygenerovaný e-mail neobsahuje žádnou zprávu (toto není absolutním pravidlem, Magistr se někdy šíří v elektronické poště s textovou zprávou). Předmět zprávy je náhodně zvolen z implementovaného seznamu. Jméno přiloženého souboru je různé. Červ vyhledá *.exe soubor, který infikuje a připojí k emailu.

V závislosti na svém vnitřním počítadle se virus připomíná zásahy do Windows desktopu a hrátky s ikonami.

Měsíc po infikování počítače spustí virus svoji destrukční rutinu, která přepíše soubory na lokálních a síťových discích textem „YOUARESHIT“. V systému Windows 9x navíc smaže CMOS Flash a data na disku. A poté ještě zobrazí vzkaz s vulgárním obsahem.



PRODUKT MCAFEE WEBSHIELD ZÍSKAL CERTIFIKACI ICSA

Antivirové řešení pro Internet gateway - WebShield SMTP, získalo certifikaci ICSA (ICSA Lab's je celosvětově uznávaná odborná společnost působící v oblasti internetové bezpečnosti).

Antivirová ochrana bran do Internetu je stále více rozhodující otázkou v oblasti ochrany sítí. McAfee svým produktem WebShield poskytuje vysokou úroveň ochrany lokálních sítí, zejména svou schopností úspěšně zasahovat proti nejnovějším počítačovým virům, e-mailovým červům a ostatním škodlivým kódům.

McAfee WebShield SMTP, který je součástí skupiny programů pro ochranu bran do Internetu, je také jednou z hlavních součástí nového zařízení Webshield e50, které je spojením výkonného hardware a kvalitního software McAfee. Zařízení Webshield e50 je určeno k nasazení především k ochraně malých a středních sítí na vstupních internetových branách.

NORMAN VIRUS CONTROL - VIRUS BULLETIN 100 PROCENT PODRUHÉ ZA SEBOU

Norman ASA dnes (4. dubna 2001) oznámil, že jeho antivirový produkt Norman Virus Control v5 pro platformy NT/2000 opět získal ocenění Virus Bulletin 100 procent, tentokrát za měsíc duben.

Virus Bulletin, který je na poli antivirů respektovanou autoritou, provádí testování antivirových produktů všech hlavních světových výrobců již od roku 1998. V současné době zveřejňuje výsledky testu vždy každý druhý měsíc a poskytuje tak uživatelům kvalitní službu pro orientaci mezi produkty jednotlivých výrobců.

Pro uživatele Norman Virus Control a dalších uživatelů, jejichž antivir používá stejný engine (skenovací motor), je zpráva o opětovném udělení zmiňované ceny ujištěním o kvalitě produktu, který používají.

O FIRMĚ
AEC, SPOL. S R.O.

Firma AEC, spol. s r.o. byla založena v roce 1991. Dnes je jedním z předních poskytovatelů software a služeb pro komplexní zabezpečení osobních počítačů jak z hlediska utajení informací, tak antivirové ochrany. Za své produkty obdržela několik prestižních ocenění a také certifikace ISO-9001 a TickIT. V současnosti disponuje prodejní sítí, pokrývající Českou republiku i Slovensko s kancelářemi v Praze, Brně a Bratislavě.