AEC
DATA SECURITY COMPANY

informační
bulletin

(Připravuje AEC Data Security Company – jakékoliv připomínky, náměty či dotazy posílejte na e-mailové adresy tomas.pribyl@aec.cz nebo petr.nadenicek@aec.cz)

Počítačové viry, antivirové technologie, elektronický podpis, šifrování dat – prostě ochrana datových informací vůbec.

Dnes přinášíme:

- **Novinky mezi počítačovými viry: Lovgate**
- **Počítačové viry „šité“ na míru**
- **F-Secure Policy Manager pro Linux**
- **Kurzy a semináře AEC v květnu 2003**

Závěrečná děkovačka divadelní hry „Byl to pták“ v pražském Divadle Bez Zábradlí dne 21. března 2003. Společnosti AEC Data Security Company zde pořádala své tradiční každoroční setkání s obchodními partnery, novináři a dalšími přáteli.

Novinky mezi počítačovými viry: Lovgate

Lovegate je e-mailový a síťový červ, který navíc disponuje zadními vrátky a snímačem stisknutých kláves. Za zemi jeho pravděpodobného původu je označována Čína.

Kromě „klasického“ šíření pomocí e-mailu umí Lovegate zneužívat i nalezená síťová sdílení. Disponuje vlastním SMTP enginem, který se za účelem rozeslání infikovaných e-mailů připojuje na server smtp.163.com, který pravděpodobně patří jednomu čínskému portálu. Na všechny e-maily nalezené v INBOXu odpovídá infikovanou zprávou. Její text může vypadat např. takto:

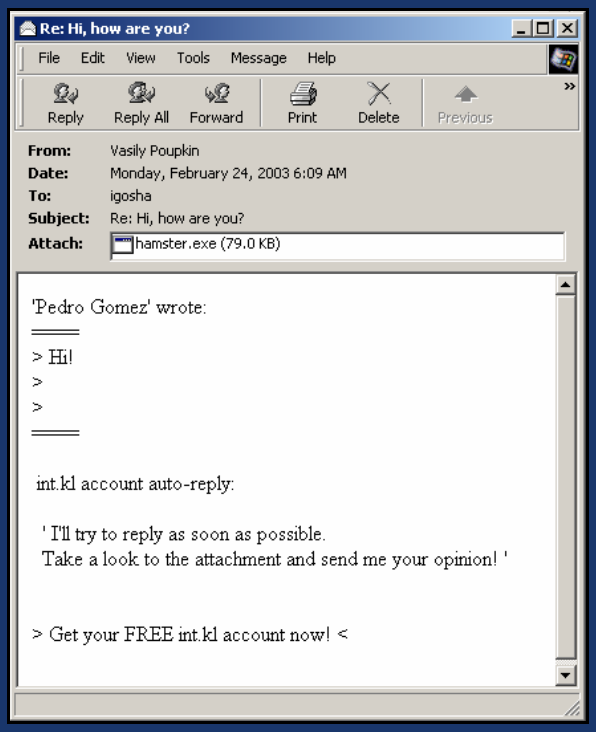
Wherever.com account auto-reply:
I"ll try to reply as soon as possible.
Take a look at the attachment and send me your opinion!

>Get your Free wherever.com account now! <

Červ kopíruje svoje soubory do systémového adresáře Windows pod různými jmény a v různých konfiguračních souborech a systémových registrech pro sebe vytváří rozmanité položky. Díky jedné provedené modifikaci dochází ke spuštění červa při každém pokusu o otevření textového souboru. Kromě toho je však soubor v Notepadu opravdu otevřen, takže uživatel nic nepozná.

Kromě toho obsahuje i zadní vrátka, která komunikují na portu 10168 a čekají na pokyny zvenčí. Případnému hackerovi dovolují provádět různé akce. Kromě toho obsahuje i tzv. keylogger (nástroj na snímání stisknutých kláves). Tyto komponenty používají několik DLL souborů, které červ kopíruje do infikovaného systému. O jejich úspěšné instalaci je autor červa informován e-mailem.

Lovegate se vyskytuje ve verzích „B“ a „C“, přičemž druhá se od první odlišuje zejména absencí keyloggeru, používanými jmény souborů a možnými texty infikovaných e-mailů.



AEC
DATA SECURITY COMPANY

Počítačové viry „šité“ na míru

Cest, kterými se počítačové viry a další škodlivé kódy budou v nejbližší době ubírat, je několik. V jedné z nich se ovšem odborníci shodují: Budoucnost patří virům, které budou navrhované za konkrétním cílem. Jejich úkolem bude napadnout konkrétní cíl a vykonat zde určitou činnost.

Virus připravený pro určité prostředí (uvědomme si, že každý počítač je svým způsobem unikátní kombinací hardware i software nejrůznějších verzí, jazykových mutací, aktualizací, nastavení, „záplat“ apod.) má totiž mnohem větší šanci na úspěch, než jeho „univerzální“ kolega. A tak může mnohem snadněji „proklouznout“ přes nejrůznější antivirové „nástrahy“ a opatření.

Že se jedná o vizi z nějaké nepovedené sci-fi? Nikolivěk. První virus, který byl „ušitý na míru“ už totiž spatřil světlo světa. Antivirové společnosti jej pojmenovaly Iloveyou.BD (šlo totiž o skriptovací virus ne nepodobný proslulému viru Iloveyou alias „Láska“, který napadl počítače celého světa letos v květnu). Virus byl naprogramovaný pro použití v United Bank of Switzerland.

Nejprve začaly zaměstnancům této banky chodit e-mailové zprávy s názvem „Resume“, k nimž byl připojený soubor resume.txt.vbs. Pokud se pokusili soubor spustit (např. dvojitým poklikáním kurzoru myši), zobrazila se seriózně vypadající žádost uchazeče o zaměstnání. To ale samozřejmě nebyl jediný projev viru, ale pouze jakýsi zastírací manévr, aby uživatel nepojal žádné podezření.

Virus se totiž snaží stáhnout a spustit z Internetu soubor, který obsahuje jednoduchou programovou rutinu sloužící ke zcizování hesel. Nejprve se pokusí na počítačích dotyčné banky lokalizovat datové soubory a poté co je nalezne, je odesílá na tři předdefinované e-mailové adresy.

Zatím se jedná pouze o prvotní a spíše neohrabaný pokus o vytvoření počítačového viru pro konkrétní prostředí, ale příklad škodlivého kódu Iloveyou.BD nechť je pro nás dostatečně zdviženým varovným prstem.

Bránit se před podobnými útoky v budoucnu nebude jednoduché, ale ne nemožné. Nejlepší obranou v takovýchto případech je prevence. Pokud budete svá data šifrovat, pak případný útočník může získat informace – ale pouze v zašifrované podobě. A s nimi nenadělá vůbec nic…

AEC

DATA SECURITY COMPANY

F-Secure Policy Manager pro Linux

Finská společnost F-Secure, jeden z předních světových výrobců antivirových a bezpečnostních řešení, oznámila, že uvedla na trh novou verzi svého řešení pro centrální správu F-Secure Policy Manager určenou pro instalaci na operační systém Linux.

Tímto krokem vyšla společnost F-Secure vstříc všem, kdo místo Windows na svých serverech raději preferují Linux a chtějí dosáhnout větší bezpečnosti, dostupnosti a spravovatelnosti centrální správy. Společnost F-Secure se tímto stává jediným výrobcem na světovém antivirovém trhu, který svým zákazníkům nabízí účinné bezpečnostní řešení pro linuxové platformy včetně kvalitní centrální správy. To je navíc zákazníkům F-Secure k dispozici zcela zdarma.

F-Secure Policy Manager for Linux je postaven na technologii Apache web serveru, který je na linuxových platformách známý svou stabilitou. Všechny instalační komponenty jsou distribuovány v podobě tzv. RPM balíčků. Celý systém může být nainstalován do pouhých pěti minut. F-Secure Policy Manager for Linux umí bez problémů spolupracovat mimo jiné i s antivirovým řešením F-Secure Anti-Virus for Firewalls instalovaným taktéž na Linuxu. Díky tomu může uživatel „vystačit“ pouze s linuxovými servery. Instalace administrátorské konzole však může být umístěna jak na platformě Windows, tak i na Linuxu. Záleží pouze na „vkusu“ administrátora.

Kurzy a semináře AEC v květnu 2003

V průběhu měsíce května 2003 pořádá Centrum vzdělávání AEC následující kurz:

- **ZABEZPEČENÍ SOFTWAROVÝMI PROSTŘEDKY, AUTENTIZACE A ŠIFROVÁNÍ, ZABEZPEČENÍ HARDWAROVÝMI PROSTŘEDKY, KRYPTOGRAFIE A ELEKTRONICKÝ PODPIS (29. května – Praha) – K nástrojům ochrany dat patří nejen antivirová ochrana dat, ale také jejich zabezpečení pomocí moderní symetrické nebo asymetrické šifry a autentizačních mechanizmů. Přehled kryptografických algoritmù, způsoby bezpečné komunikace pomocí šifrovacích prostředkù, využití čipových karet, tokenů a jiných hardwarových prostředkù,které především souvisí s elektronickým podpisem,budou v kurzu prezentovány - a to jak z hlediska teorie,tak i praktického nasazení.**

Bližší informace ke kurzům Centra vzdělávání AEC naleznete na http://vzdelavani.aec.cz, dotazy lze směrovat na e-mailovou adresu kurzy@aec.cz

AEC
DATA SECURITY COMPANY