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: Bugbear.B**
- **Novinky mezi počítačovými viry: Sobig**
- **Potvrzená důvěra a kvalita**
- **S AEC bezpečně na zemi ve vzduchu…**

CERTIFIKÁT SYSTÉMU MANAGEMENTU JAKOSTI

Potvrzujeme, že systém managementu jakosti společnosti:

AEC, spol. s r. o.
Brno
Česká republika

byl schválen společností Lloyd's Register Quality Assurance podle následujících standardů systému managementu jakosti:

ISO 9001:2000
BS EN ISO 9001:2000
DIN EN ISO 9001:2000
ČSN EN ISO 9001:2001

Systém managementu jakosti zahrnuje činnosti:

Vývoj a dodávka software a systémové integrace včetně souvisejících služeb, konzultací a školení.

Certifikát č.: PRA 280117

První certifikát vystaven: 6. června 2003
Současný certifikát vystaven: 6. června 2003
Platnost certifikátu do: 30. června 2006

Vystaveno v LRQA Praha

UKAS 004

Tento dokument je vystaven za podmínek uvedených na zadní straně.

Společnost AEC obhájila při nedávném auditu svůj systém managementu jakosti a získala certifikát dle normy ISO 9001:2000.

Novinky mezi počítačovými viry: Bugbear.B

V průběhu čtvrtka 5. června se objevila nová verze již dříve „úspěšného“ červa Bugbear. Jeho původní varianta se poměrně masivně šířila na přelomu loňského září a října, kdy přidal vrásky na čelo nejednoho administrátora.

Stejně jako původní červ, představuje Bugbear.B nadmíru komplexní škodlivý kód, který v sobě kombinuje „dovednosti“ e-mailového a síťového červa, keyloggeru, trojského koně a polymorfního viru infikujícího spustitelné soubory. Dokáže také ukončovat spuštěné procesy bezpečnostních a antivirových programů.

Červ se snaží o šíření na všechny adresy nalezené na infikovaném systému. E-mailová adresa odesílatele je falešná a neshoduje se s adresou infikovaného uživatele. Adresy umí vytahovat z INBOXu a ze souborů: .DBX, .EML, INBOX, .MBX, .MMF, .NCH, .ODS a .TBB. K samotnému odesílání červ zneužívá uživatelův default SMTP server, jehož nastavení si zjišťuje z klíče Internet Account Manageru.

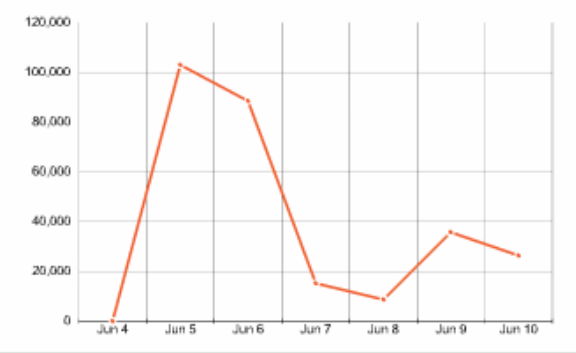
I když má ve svém kódu zabudovány seznamy různých předmětů, textů a názvů přiložených souborů, pro generování infikovaných e-mailů většinou využívá přímo části existujících zpráv a názvy souborů nacházejících se na disku infikovaného počítače. Přiložený soubor je samozřejmě opatřen dvojitou příponou .exe, .pif nebo .scr (např. .doc.pif). Infikované e-maily mohou v některých případech (ale ne vždy) obsahovat kód zneužívající známou Iframe bezpečnostní díru, která může způsobit spuštění přiloženého souboru červa při pouhém otevření zprávy.

Do systému se instaluje pod náhodně vygenerovaným jménem do „START UP“ adresáře, což zajišťuje jeho spuštění při každém startu systému. Do stejného umístění se snaží nakopírovat i na ostatní počítače přes sdílení v lokální síti. S touto šířící rutinou však nevyrukuje ihned po infikování systému, ale nějakou dobu s ní počká.

Do počítače instaluje také keylogger (snímač stisknutých kláves) na bázi DLL, který ukládá do adresáře SYSTEM. Název jeho souboru obsahuje celkem sedm náhodně zvolených znaků. Na stejné místo kopíruje ještě dva další podobné soubory, které obsahují zachycené informace v zašifrované podobě. Obsahuje také trojského koně, který může být potencionálním hackerem ovládán prostřednictvím TCP portu 1080 a zneužit pro získání přístupu do systému.

Pokouší se o infikování určitých konkrétních souborů a snaží se ukončovat běžící procesy patřící bezpečnostním a antivirovým programům.

Nástup e-mailového červa Bugbear.B dle www.messagelabs.com:



AEC
DATA SECURITY COMPANY

Novinky mezi počítačovými viry: Sobig.D

Ve středu 18. června 2003 se objevila další (v pořadí již čtvrtá) varianta červa Sobig. Její autor opět neprojevil příliš mnoho invence, takže i tato verze je velmi podobná předchozím.

Stejně jako u verzí „B“ a „C“ je i šíření Sobig.D časově omezeno – tentokrát do 2. července. Šířit se umí e-mailem a také po lokální síti. Ke svému spuštění červa z infikovaného e-mailu je třeba aktivní účasti uživatele, který musí přiložený soubor manuálně spustit. Sobig potom kopíruje do systémového adresáře Windows svoje dva soubory cftrb32.exe (červ) a rssp32.dat (konfigurační soubor). Do systémových registrů přidává nové klíče, které zajišťují jeho spuštění při každém startu systému.

Sobig.D používá při sestavování infikovaných e-mailů stejné metody a předdefinované komponenty jako předchozí verze Sobig.C. Používá buď náhodně vybranou adresu odesílatele nalezenou na infikovaném počítači nebo adresu admin@support.com. Text zprávy je vždy stejný: „See the attached file for details.“ E-mailové adresy vybírá ze souborů : .wab, .dbx, .htm, .html, .eml a .txt.

Přes dostupná síťová sdílení se šíří tak, že se snaží kopírovat do adresáře *„Windows\All Users\Start Menu\Programs\Startup“*\ nebo *„Documents and Settings\All Users\Start Menu\Programs\Startup“*.

AEC: potvrzená důvěra a kvalita

Brněnská společnost zabývající se ochranou počítačových dat AEC při nedávném auditu prováděném britskou Lloyd´S Register Quality Assurance Ltd. obhájila svůj systém managementu jakosti a získala jeho certifikaci dle normy ISO 9001:2000.

„Naši zákazníci tuto skutečnost nepochybně ocení. Certifikace firemního systému jakosti představuje zejména potvrzení vysoké úrovně našich služeb a dodávaných produktů“, prohlásila Ing. Alena Řezníčková, ředitelka společnosti AEC.

Společnost AEC byla držitelem certifikátu ISO 9001:1994 již od roku 1998. I tehdy byla certifikace provedena renomovanou britskou organizací Lloyd´S Register Quality Assurance Ltd. Vzhledem k tomu, že certifikát není udělován „doživotně“, ale je nutné jej v pravidelných intervalech obhajovat, proběhl počátkem června 2003 nezbytný proces recertifikace. Dlužno podotknouti, že úspěšně a AEC je tak i nadále hrdým vlastníkem certifikátu ISO 9001:2000 systému managementu jakosti, který zahrnuje činnosti: „Vývoj a dodávka software a systémové integrace včetně souvisejících služeb, konzultací a školení.“

AEC

DATA SECURITY COMPANY

S AEC bezpečně na zemi i ve vzduchu

AEC zve všechny příznivce na Mistrovství České republiky v plachtění 2003. Tuto akci, kterou naše společnost podporuje, pořádá Aeroklub Křižanov ve dnech 17. až 30. srpna tohoto roku.

Společnost AEC nepůsobí pouze v úzkém oboru informační bezpečnosti, ale čas od času podporuje i některé sportovní a kulturní aktivity. A protože není dobré se stále držet při zemi, ale občas se i vznést do nadoblačných výšin, podporuje naše společnost letošní Mistrovství České republiky v plachtění, které se bude konat na letišti křižanovského aeroklubu ve druhé polovině srpna.

Pokud jste tedy fandové letectví, přijďte se v uvedených dnech podívat, jak si piloti poradí se svými bezmotorovými „miláčky“. Křižanovské letiště se nachází v překrásném prostředí Českomoravské vrchoviny s řadou lesů a rybníků, která kromě plachtění poskytuje ideální podmínky např. pro turistiku a spoustu dalších forem vyžití.

2003 PLACHTAŘSKÉ MISTROVSTVÍ ČESKÉ REPUBLIKY
KŘIŽANOV
17. - 30. SRPEN

AEC
DATA SECURITY COMPANY