informační
bulletin
AEC DATA SECURITY COMPANY

(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: MyDoom.M a S***
- ***Novinky mezi počítačovými viry: Bagle.AI***
- ***AEC i nadále s certifikátem ISO 9001***
- ***Softwarové novinky z laboratoří AEC***
- ***Proč se počítače záplatují?***

V rámci veletrhu informačních technologií Invex se ve středu 13. října 2004 uskuteční tradiční konference „Viry a antiviry“ pořádaná pod záštitou vydavatelství Vogel Burda Communications. Na konferenci vystoupí také přednášející z AEC – mezi nimi i ing. Petr Nádeníček (na snímku z konference o antivirové ochraně v Českých Budějovicích).

AEC DATA SECURITY COMPANY

Novinky mezi počítačovými viry: MyDoom.M a S

V průběhu letošních prázdnin se objevilo několik nových variant e-mailového červa Mydoom.

První z nich se stal Mydoom.M (některé antivirové společnosti jej ovšem detekují jako Mydoom.O, Mydoom.L a Mydoom.R). Podobně jako předchozí varianty provádí generování a rozesílání infikovaných e-mailů pomocí vlastního SMTP motoru, e-mailové adresy čerpá z různých typů souborů nalezených na disku infikovaného počítače, falšuje adresu odesílatele a snaží se šířit i prostřednictvím výměnných P2P sítí. Text v těle zprávy je vygenerován z různých součástí, které si červ nese s sebou. Od svých „příbuzných“ se odlišuje také tím, že může rozesílat také nezavirované soubory (o velikosti 1 – 2 kB).

Jako zdroj e-mailových adres červ používá také různé vyhledávače. Podle dostupných informací došlo v této souvislosti ke krátkodobému narušení činnosti vyhledávače www.google.com.

Pokud je Mydoom.M spuštěn vytvoří v adresáři Windows svůj soubor JAVA.EXE (např. C:\WINDOWS\JAVA.EXE) a SERVICES.EXE. Spouštění při každém startu systému si zajišťuje vytvořením příslušných klíčů v registru. Na infikovaném počítači otevírá na TCP portu 1034 zadní vrátka, která mohou být následně zneužita k útoku na infikovaný systém.

Za zmínku stojí také další varianta: Mydoom.S. Tento červ je také někdy označován jako Ratos.A. Infikovaná zpráva rozesílaná červem Mydoom.S vypadá následovně:

```
Předmět : photos
Text : LOL!;))))
Přiložený soubor : photos_arc.exe
```

Adresy pro další šíření extrahuje z některých typů souborů, které vyhledává na disku infikovaného počítače. Adresa odesílatele je jako obyčejně falšována. Vyhýbá se adresám, které obsahují některý z určených výrazů.

Ke svému spuštění z infikovaného e-mailu červ potřebuje aktivní spolupráci uživatele. Pokud je aktivován, nainstaluje se do adresáře WINDOWS jako rasor38a.DLL a do adresáře SYSTEM jako winpsd.exe. Kromě toho vytváří také několik klíčů v systémovém registru.

Snaží se také o stažení a instalaci dalšího škodlivého kódu zadních vrátek ze dvou různých webových serverů.

AEC
DATA SECURITY COMPANY

Novinky mezi počítačovými viry: Bagle.AI

Do světa byl vypuštěn další e-mailový červ z rodiny Bagle (tentokrát je to verze AI). Stejně jako několik dalších nedávno objevených variant má podle antivirových odborníků poměrně velkou šanci se šířit „In the Wild“.

Bagle.AI svůj původ nezapře. Podobně jako většina jeho příbuzných se šíří v infikovaných e-mailech jako soubor s různými názvy a příponami EXE, SCR, COM, CPL nebo ZIP. Ten může být navíc šifrovaný. V tomto případě je heslo potřebné k dešifrování uvedeno v e-mailu jako text nebo formou obrázku.

E-mailové adresy potřebné k dalšímu šíření čerpá z různých typů souborů nalezených na disku infikovaného počítače. K rozesílání využívá vlastní SMTP motor. Stejně jako většina dnešních červů falšuje adresu odesílatele. Kromě šíření e-mailem se kopíruje také do složek sdílených do P2P sítí

V počítači se usazuje v systémovém adresáři Windows System jako WinXP.exe. Ve stejném adresáři vytváří ještě několik dalších souborů. Svoje spuštění při každém startu systému zajišťuje pomocí klíče v registru. Jako pojistku proti vícenásobné infekci červ používá mutex.

Aktivně bojuje proti některým dalším červům a bezpečnostním programům Ukončuje jejich spuštěné procesy (podle velmi dlouhého vlastního interního seznamu – 275 položek) a maže klíče ze systémového registru. Kromě toho na infikovaném počítači otevírá zadní vrátka na TCP portu 1080 a UDP portu 1040.

AEC i nadále s certifikátem ISO 9001

Systém managementu jakosti společnosti AEC uspěl v pravidelném kontrolním auditu Lloyd´S Register Quality Assurance a může se i nadále honosit certifikací podle normy ISO 9001:2000.

Ředitelka společnosti Ing. Alena Řezníčková k této události řekla: „Kvalitu v AEC chápeme především jako kvalitu našich služeb a spokojenost našich zákazníků. Jsme rádi, že i tento kontrolní audit potvrdil úspěšnost naší snahu v prosazování jakosti do všech činností firmy.“

AEC
DATA SECURITY
COMPANY

Softwarové novinky z laboratoří AEC

Brány vývojového oddělení společnosti AEC opustily nové verze programů TrustPort® Disk Protection, TrustPort® DataShredder a TrustPort® Personal Firewall. Kromě toho byl uveden také zcela nový nástroj pro vytváření prezentací TrustPort® Run Manager.

TrustPort® Disk Protection slouží k on-line šifrování dat na virtuální diskové jednotce. Poslední verze TrustPort® Disk Protection 3.5.1.454 přináší některá drobná vylepšení a je k dispozici v anglické i české jazykové mutaci. Novinky jsou mimo jiné následující:

- Podpora MS Windows NT.
- Možnost připojení diskového obrazu fyzicky umístěného na serveru v síti.
- Možnost definování klávesové zkratky rychlého odpojení disků.
- Podpora automatické instalace bez účasti uživatele.
- Nové parametry pro použití programu z příkazové řádky.

TrustPort® DataShredder slouží ke skartaci dat na pevném disku počítače. Uživatel ho může využít k bezpečnému smazání jednotlivých souborů, adresářů, volného místa a dalších položek vytvářených systémem a internetovým prohlížečem. Nová verze TrustPort® DataShredder 2.5.1.454 obsahuje některá drobná vylepšení a opravy, zejména následující:

- Optimalizované a výkonnější skartovací jádro.
- Mazání historie navštívených stránek v adresním řádku aplikace Internet Explorer.
- Možnost skartování z příkazové řádky.

Kromě toho společnost AEC vydává také dlouho očekávanou anglickou a českou verzi svého TrustPort® Personal Firewallu. Anglická verze TrustPort® Personal Firewall 3.5.0.454 a česká TrustPort® Personal Firewall 3.5.0.459 přináší zejména následující novinky:

- Přesnější definici pravidel pro filtrování provozu.
- Možnost zobrazení statistik přenosu paketů a počtu bytů.
- Klasifikaci pravidel do logických skupin.
- Vytváření pravidel podle zpráv ze souboru událostí.
- Funkci pro prohlížení externích souborů událostí.

Na trh byl taktéž uvolněn další zajímavý produkt AEC - TrustPort® Run Manager 3.5.0.457, který je určen k vytváření menu např. prezentačních nebo instalačních CD. Uživatel si může jednoduše v XML formátu navrhnout vlastní menu (např. firemní prezentace na CD disku) včetně textu, grafiky, tlačítek a dalšího obsahu. Program obsahuje řadu užitečných funkcí pro práci se soubory, profily apod.

AEC
DATA SECURITY COMPANY

Proč se počítače záplatují?

Záplatujte, záplatujte, záplatujte… Možná, že i k Vám se donesla tato poučka bezpečné práce s počítači. Proč záplatovat? Jak to provádět? Na tyto a další otázky se pokusíme odpovědět na následujících řádcích.

Není tomu tak dávno, co softwarové firmy vydávaly své produkty za zcela bezchybné a bezproblémové. Přestože se chyby a problémy evidentně vyskytovaly, vždy se sváděly na „objektivní příčiny“ nebo na cokoliv jiného. Situace se ale změnila, většina výrobců software zcela bez uzardění připouští, že jejich programy mohou obsahovat chyby. Ostatně, není se ani čemu divit – každý počítač na světě je unikátní kombinací software, hardware a jejich nastavení, přičemž testování programů probíhá pouze na velmi úzkém vzorku strojů.

Výrobci software si navíc uvědomili, že v případě zaujímání pozice „mrtvého brouka“ k těmto nedostatkům se jim to může jednoho krásného dne šeredně nevyplatit. Např. v podobě žalob poškozeného klienta nebo ztráty důvěry významných zákazníků. I z tohoto pohledu se jeví jako přijatelnější řešení připustit možnost existence chyb, tyto pravidelně opravovat (hle, služba zákazníkům!) a přenést tak zodpovědnost právě na uživatele.

Samozřejmě, že není možné chtít, aby si uživatelé po každé vydané opravě celý program nebo rovnou operační systém přeinstalovali. A tak vznikly právě patche – záplaty. Jedná se o menší programy, které mají za cíl po aplikaci na příslušném počítači upravit zdrojové kódy mateřského programu a jeho konfiguraci tak, aby se odstranily známé problémy. Ty mohou být několikerého rázu – kolize příslušného programu s jiným, špatná funkce v některých případech, nechtěná vlastnost, kterou mohou využít hackeři nebo viry apod.

Vlastní proces „záplatování“ – tedy aplikace příslušné záplaty – se liší program od programu. Někdy může mít „záplata“ podobu doporučení ke změně nastavení některých položek v programu. Jindy mám podobu spustitelného EXE souboru, který je zapotřebí na počítač nahrát a spustit. Jindy záplata přichází v podobně datových souborů, které je potřeba uložit do příslušného adresáře apod.

Podtrženo, sečteno – ač se „záplatování“ může zdát zbytečné a uživatele obtěžující, ve skutečnosti tomu tak není. Odměnou za jeho aplikaci bude stabilnější a bezpečnější chod příslušné aplikace.

AEC
DATA SECURITY COMPANY