



*(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:

AEC roadshow 2004

Bagle tady, Bagle tam, Bagle kam se podívám

První virus pro Windows CE

NAI se mění na McAfee



První škodlivý kód pro platformu Windows CE (resp. Pocket PC) už je na světě. Jmenuje se Duts. Naštěstí není nebezpečný, nicméně jedná se o jasný a pádný důkaz faktu, že napsání viry pro tuto čím dále rozšířenější platformu je možné.



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. Společnost AEC si ale dobře uvědomuje, že otázku informační bezpečnosti je třeba řešit globálně (a nikoliv pouze lokálně – i když je to bezesporu na první pohled komerčně zajímavější). 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 roadshow 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





Bagle tady, Bagle tam, Bagle kam se podívám

Počátek letošního léta přinesl několik nových variant škodlivého kódu Bagle.

Jednou z „novinek“ byla verze Bagle.AF, která se vyznačuje následujícími vlastnostmi:

- Disponuje vlastním SMTP motorem, který využívá ke generování a rozesílání dalších infikovaných e-mailů.
- Další adresy dokáže extrahovat z určitých typů souborů nalezených na disku infikovaného počítače.
- Dokáže falšovat adresu odesílatele – dosazuje za ni některou z nalezených.
- V příloze infikované zprávy může být „obyčejný“ spustitelný soubor nebo ZIP archiv, který může být navíc šifrován (heslo je uvedeno v textu ,případně ve formě obrázku).
- Na infikovaný počítač červ instaluje zadní vrátka na TCP portu 1080 umožňující jeho zneužití na dálku a informuje o jejich otevření.
- Kopíruje se do složek sdílených do P2P sítí.
- Používá mutex zabráňující jeho vícenásobnou instalaci a také mutexy stejné jako u variant červa Netsky, čímž se snaží bránit infikování již obsazeného systému konkurenčním škodlivým kódem.
- Ukončuje procesy některých bezpečnostních programů a dalších červů a maže jejich klíče ze systémového registru.

Pokud je červ spuštěn, nakopíruje do systémového adresáře Windows svůj soubor s názvem sysxp.exe. Ve stejném adresáři ještě vytváří soubory sysxp.exeopen a sysxp.exeopenopen. Spuštění při každém startu systému zajišťuje vytvořením klíče v registru.

V závěsu za červem Bagle.AF se zjevila další varianta v podobě Bagle.AG. Charakteristiky varianty Bagle.AG jsou velice podobné těm předchozím. Stejně jako ony má vlastní SMTP motor, adresy extrahuje ze souborů nalezených na disku, falšuje adresu odesílatele infikovaného e-mailu a v příloze může nést zašifrovaný ZIP. Jako další kanál pro svoje šíření využívá P2P síť. Kromě toho na infikovaném PC otevírá na TCP portu 1080 zadní vrátka, která ho umožňují na dálku zneužít k různým nekalým účelům.



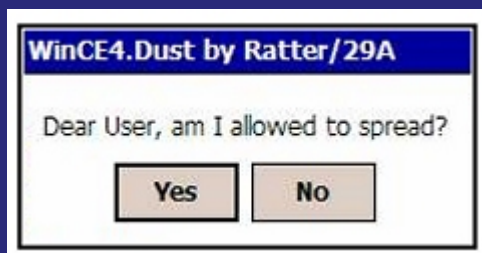
První virus pro Windows CE

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.

Autorem je Ratter ze známé skupiny 29A, jejíž členové se tvorbou „proof of concept“ virů zabývají.

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 tohoto 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...



NAI se mění na McAfee

Známý americký výrobce antivirového a bezpečnostního software společnost Network Associates mění od 1. července 2004 svůj název na McAfee Inc. Tento krok je součástí dalších probíhajících změn. NAI v odprodává svoje divize Magic Solutions (help desk technologie) a Sniffer Technologies (řešení pro správu sítě). Nová společnost McAfee Inc. se úzce zaměří na poskytování řešení pro antivirovou ochranu a prevenci nežádoucího vniknutí (IDS/IPS). Od změny jména si společnost slibuje zejména posílení svého image vedoucí společnosti v oboru. Značka McAfee je díky známá po celém světě.

Další zajímavou novinkou je brzké uvedení nové verze programu McAfee VirusScan Enterprise 8.0i. Jeho hlavním trumfem je kromě zabudovaného personálního firewallu především unikátní funkce pro prevenci narušení systému (IPS).

McAfee VirusScan Enterprise 8.0i poskytuje pracovním stanicím i serverům pokročilou proaktivní ochranu před škodlivými kódy. Detekuje, identifikuje, hlásí, čistí, maže a brání známým i neznámým škodlivým kódům a zlomyslným aktivitám infikovat počítače a servery v síti. Posouvá význam antivirového programu z oblasti reaktivních bezpečnostních opatření k uceleným proaktivním přístupům v ochraně před útoky hackerů a zneužití zranitelností operačních systémů a aplikací.

Klíčové vlastnosti:

- Integrovaný personální firewall a technologie IPS.
- Ochrana proti řadě dalších současných hrozeb jako je např. spyware nebo buffer overflow útoky proti určitým aplikacím."
- Zvýšená ochrana během reakce na novou nákazu (než jsou k dispozici nové DAT soubory).
- Osvědčený skenovací motor McAfee, který provádí kontrolu přímo v paměti.
- Centrální správa a reportování pomocí McAfee ePolicy Orchestratoru a ProtectionPilotu.
- Ochrana proti útoku typu buffer overflow.
- Detekce a likvidace nechtěného software (Spyware, Adware apod.).
- Odezva na nákazu včetně identifikace zdroje infekce.
- Kontrola skriptů (JavaScript a VBScript).
- Plug-in do klienta Lotus Notes.