AEC Magazín – Viry, antiviry a bezpečnost

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:

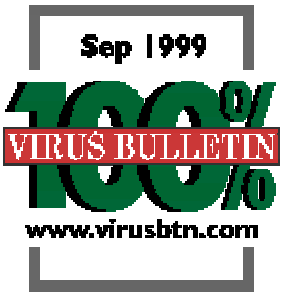
Příjemné počtení a co nejméně potíží s viry a zabezpečením Vašich dat přeje AEC, spol. s r.o.

„Flotila“ antivirových programů AEC, spol. s r.o. se rozrůstá: Norman

V rámci rozšíření a vylepšení našeho portfolia antivirových programů přicházíme v krátké době (po produktu AVP) s další novinkou na český trh. Je jí antivirový program NORMAN Virus Control (dále jen Norman).

Nejedná se ovšem o novinku úplně novou, ale spíše staronovou. Pro toto vysvětlení se musíme podívat trochu do historie. Předpokládáme, že antivirový program ThnderByte vám zní povědomě. V průběhu února 1998 zakoupila ThunderByte Antivirus právě firma NORMAN, a od té doby probíhaly usilovné práce techniků a programátorů této firmy o co nejúspěšnější sladění těch nejlepších vlastností dvou, do té doby různých antivirových produktů – Norman Virus Control a ThunderBYTE Antivirus.

Dílo se zadařilo: Nový Norman Virus Control je certifikován ICSA, a v poslední době byl několikrát vyhodnocen časopisem Virus Bulletin jako jeden z nejlepších antivirových produktů (Virus Bulletin 100% Award).



Buddylst.zip: Varování před virem, který neexistuje

Někdy v průběhu října 1998 (tedy více než před rokem!) se ve Spojených státech objevil hoax (e-mailová zpráva varující před virem, který ve skutečnosti neexistuje), který upozorňoval na „smrtelně“ nebezpečný počítačový virus šířící se v souborech Buddylst.zip. Zároveň vyzýval k tomu, aby příjemce zprávy co nejdříve varoval co největší množství osob.

A právě toto „lavinovité“ šíření je jediným cílem hoaxů. Vir Buddylst.zip totiž nikdo nikdy neviděl. Jedná se o zprávu s jediným cílem: Vyvolat paniku mezi nicnetušícími uživateli počítačů.

A počátkem letošního října se kterýsi „dobrodinec“ rozhodl více než rok staré varování přeložit do jazyka českého a rozeslat jej na všechny strany. Způsobil tak paniku nevídanou.

Hoax Buddylst.zip má následující podobu (samozřejmě s atributem „Důležitost“ nastaveným na hodnotu „Velká!“):

> Pečlivě si prosím přečtěte následující informaci. Možná by Vám mohla býti nápomocna v nezmaření Vaší práce.
>
> Tato informace přišla včera ráno od Microsoftu. Prosím předejte ji každému, o kom víte, že má přístup k Internetu. Možná dostanete zdánlivě neškodný šetřič obtazovky „Budweiser“ nazvaný „BUDDYLST.ZIP“. Jestliže ano, V ŽÁDNÉM PŘÍPADĚ JEJ NEOTEVÍREJTE, ale okamžitě jej vymažte. Jestliže jej otevřete, ztratíte všechno, co máte na Vašem PC.
>
> Harddisk bude úplně zničen a osoba, která Vám poslala zprávu, bude mít přístup k Vašemu jménu a heslu přes Internet. Pokud je nám známo, virus se dostal do oběhu včera ráno. Je to nový virus a mimořádně nebezpečný. Prosím, okopírujte tuto zprávu a pošlete ji e-mailem každému, koho máte ve svém adresáři.
>
> Musíme udělat vše, abychom tento virus zastavili. AOL potvrdil, jak je tento viru nebezpečný a neexistuje žádný antivirový program, který by jej zničil. Prosím podnikněte veškerá opatření a předejte tuto informaci Vašim přátelům, známým a kolegům v práci.

Dostanete-li tudíž e-mail mající podobné příznaky, neposílejte jej dále a ignorujte jej, případně upozorněte jeho odesílatele na to, že se nechal napálit. Budete-li mít přesto nějaké pochybnosti, zkuste před bezhlavým šíření této zprávy kontaktovat některou z antivirových firem (teď jsem si asi vysloužil kletby všech pracovníků antivirových firem držících hot-line). Ve většině případů bude stačit třeba i jen pohled na webovskou stránku některé z antivirových firem, protože o události podobného typu budou určitě informovat. Na některých najdete určitě i odkazy na typické falešné poplašné zprávy, které v současnosti nejvíce zaplavují Internet nebo na historii některých z nejznámějších. Pravdou je, že ještě donedávna byly tyto zprávy výhradně v angličtině a jejich rozšíření mezi českými uživateli Internetu bylo hodně malé.

Vypadá to, že českých uživatelů Internetu již je takové množství, že se „pachatelům“ podobných varování bude stále častěji vyplácet jejich lokalizace…

Cholera se šíří po Internetu!

Na Internetu se šíří Cholera. Nemusíte si sice po každé práci s počítačem umývat ruce a ihnalovat dezinfekční chlór, leč opatrnosti nikdy není dosti. Dokonalou souhru představuje symbióza „červa“ jménem W32.Cholera a viru W32.CTX.

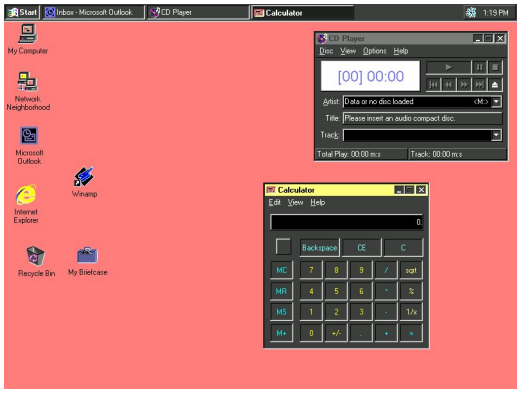
Cholera se šíří pomocí Internetu a přes lokální sítě. Nejčastěji se do počítače dostává jako soubor SETUP.EXE, což je příloha e-mailových zpráv, které mají v poli „Předmět“ jen strohé konstatování „Ok…“. Trojský kůň je napsaný v jazyku Microsoft C++ a je dlouhý 40 kilobajtů. největší část jeho velikosti přitom zabírá knihovna C++, pouze asi 7000 bajtů tvoří vlastní kód Cholery.

Aby uživatel nepojal jakékoliv podezření, zobrazí Cholera po svém spuštění následující hlášení:

```
Setup
Cannot open file: it does not appear to be a valid archive.
If you downloaded this file, try downloading the file again.
[ OK ]
```

Jak již bylo uvedeno, Cholera v sobě „nese“ i vir: CTX. Je to poměrně neškodný parazitický polymorfní virus, který vyhledává PE (Portable Executable) soubory v aktuálním adresáři a také v adresářích WINDOWS a WINDOWS/SYSTEM. CTX se projevuje v okamžiku, když spustíte napadený soubor přesně půl roku po infikování (s přesností na hodiny). Tehdy dojde k invertování barev pracovní plochy a vir se „zacyklí“ v nekonečné smyčce.

Na viru CTX je také zajímavá jeho kompatibilita s operačním systémem Windows 2000. Obratně se totiž vyhýbá antivirové ochraně Windows 2000 založené na SFC (System File Check). CTX si zajistí přístup do knihovny SFC.DLL a každý soubor si před napadením „prověří“. Pokud je chráněný, ignoruje jej a za cíl útoku si vybírá nějaký jiný soubor.



Viry také v obrázcích JPG?

Ne, nebojte se, obrázky formátu JPEG jsou (a vždy budou) před viry bezpečné. Pouze neznámý „vtipálek“

„Vir ve formátu JPEG“ využívá jedné bezpečnostní díry v produktu Mirabilis Software, který zobrazuje pouze prvních dvanáct znaků z názvu souboru! A tak se může stát, že zatímco bude zopbrazen pouze soubor „********.jpg“ (kde „********“ je zcela libovolná sekvence znaků), ve skutečnosti jde o soubor „********.jpg.exe“ (díky zmíněné chybě uživatel nevidí jeho skutečnou koncovku).

Jedná se o trojského koně ICQpws.gen (někdy se můžeme setkat i s označením Trojan.PSW.Coced). Aby maskoval svou činnost, zobrazí po svém spuštění obrázek a současně vytváří v adresáři WINDOWS/SYSTEM soubor mswim32.exe, který zajistí při příštím restartování počítače odeslání uživatelova hesla a dalších identifikačních znaků na přednastavenou e-mailovou adresu.

Pokud si nejste jisti, zdali nemáte v počítači „nevítaného hosta“ v podobě ICQpws.gen, prostě spusťte ICQ. A pak se podívejte do „Spuštěných úkolů“ (například pomocí klasické kombinace kláves Ctrl-Atl-Del). Pokud zde mezi běžícími úkoly najdete i „MSWIN32“, je více než pravděpodobné, že vaše identifikační znaky již zná i někdo jiný.

Bezpečné mazání obsahu pevného disku: IronWare® Shredder

Protože běžné operační systémy na bázi Windows neumožňují neobnovitelné smazání dokumentu, vznikl v bezpečnostním systému IronWare® Security Suite modul IW Shredder sloužící k neobnovitelnému mazání souborů nebo disků. Běžný operační systém soubory maže tím způsobem, že poupraví pouze hlavičku souboru ve FAT nebo NTFS a označí místo, které soubor zabíral za volné místo. Soubor ale fyzicky stále leží na disku - a pokud útočník poopraví hlavičku zpět, je soubor obnoven. Princip neobnovitelného smazání souborů spočívá v několikanásobném přepsání obsahu souborů, jeho zkrácení na nulovou délku a teprve poté smazáním operačním systémem. Několikanásobné přepisování se provádí kvůli rezistenci magnetických médií (magnetické médium umožňuje obnovování i přepsaných záznamů pomocí měření zbytkových magnetických proudů). Soubory jsou proto přepisovány několikrát (až desetkrát). Počet přepsání i řetězec, který bude použit pro přepisování dat, lze v programu nastavit, nebo je generován náhodně.

Modul je složen z následujících částí:

- **IW Shredder** – po instalaci do kontextového menu, které se standardně aktivuje na pravé tlačítko myši přibude funkce skartace vybraného souboru nebo adresáře. Po zvolení této akce jsou vybrané soubory nebo adresáře skartovány.
- **IW Fast Clean** – funkce pro skartování určitých souborů na požádání. Na jednotlivých discích lze nastavit okamžitou jednorázovou skartaci odkládacích a dočasných souborů SWP a TMP, skartaci standardního koše Windows nebo volného místa na disku. Lze nastavit smazání určitého konkrétního seznamu souborů a adresářů pro skartaci, skartaci historie

otevíraných souborů, dočasných souborů systému Windows nebo internetových prohlížečů WWW.

- **IW Panic Shredder** – umožňuje nastavení seznamu souborů, souborových masek nebo celých adresářů, které budou bezpečně smazány při každém stisku určité kombinace kláves.

Modul IW Shredder je možné instalovat a využívat i samostatně bez využití celého systému IronWare® Security Suite.

Více informací o systému IronWare® Security Suite naleznete na našich webovských stránkách, na e-mailové adrese info@aec.cz nebo na kontaktní adrese na konci tohoto „AEC Magazínu".

O firmě AEC, spol. s r.o.

AEC, spol. s r.o. je jedním z předních poskytovatelů a výrobců software pro komplexní zabezpečení osobních počítačů jak z hlediska utajení informací, tak antivirové ochrany. Za své produkty obdržela několik prestižních ocenění a také certifikací ISO-9001 a TickIT. Společnost byla založena v roce 1991. Jedná se o ryze českou firmu bez účasti zahraničního kapitálu. V současnosti disponuje prodejní sítí, pokrývající ČR i SR s kancelářemi v Praze, Brně a Bratislavě. Důkazem toho, že Slovensko není jediným zahraničím, ve kterém AEC, spol. s r.o. působí, je distribuční síť v Belgii, Holandsku, Kanadě, Lucembursku, Maďarsku, Německu a v dalších zemích.

Kontakty:

AEC, spol. s r.o.
Bayerova 30, 602 00 Brno
Tel.: 05 / 4123 5466-7
Fax: 05 / 4123 5038
e-mail: info@aec.cz

AEC, spol. s r.o.
Vinohradská 184, 130 52 PRAHA 3
Tel./fax: 02 / 6731 4326 nebo 1402
e-mail: praha@aec.cz

AEC Bratislava, spol. s r. o.
POB 79, Pribinova 25, 810 11
BRATISLAVA, SK
Tel.: +421 (0)7 50633 027
Fax: +421 (0)7 50633 029
e-mail: bratislava@aec.sk

Autorem „AEC Magazínu" je Tomáš Přibyl: tomas.pribyl@aec.cz