# 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 dat přeje Vaše firma

AEC, spol. s r.o.

## *Stačí otevřít e-mail – a máte virus!*

Již několikrát byl v minulosti vypracovaný teoretický „obraz“ viru, který by se mohl aktivovat pouhým OTEVŘENÍM e-mailové zprávy. Dosud všechny e-mailové viry vyžadovaly ke své činnosti spuštění souboru na příloze, ať již měl koncovku EXE, DOC či jakoukoliv jinou. Nikdo však vir aktivující se pouhým otevřením zprávy nedokázal reálně vytvořit – to platilo až do poloviny listopadu.

Neznámý „autor“ využil známou bezpečnostní chybu a vytvořil první e-mailový virus, který se aktivuje pouhým otevřením zprávy. V případě, že máte v poštovním klientovi nastavené automatické prohlížení, virus se aktivuje dokonce pouhým PŘIJETÍM zprávy! Na první pohled vize minimálně hrůzostrašná. Proto se podívejme na virus BubbleBoy, jak se nový prográmek nazývá, poněkud podrobněji. Není to totiž takový zázrak, jak se na první pohled může zdát, neb využívá již dlouho známých chyb v některých programech a spoléhá na pohodlnost uživatelů, kteří si ještě nestihli „záplatovat“ své systémy.

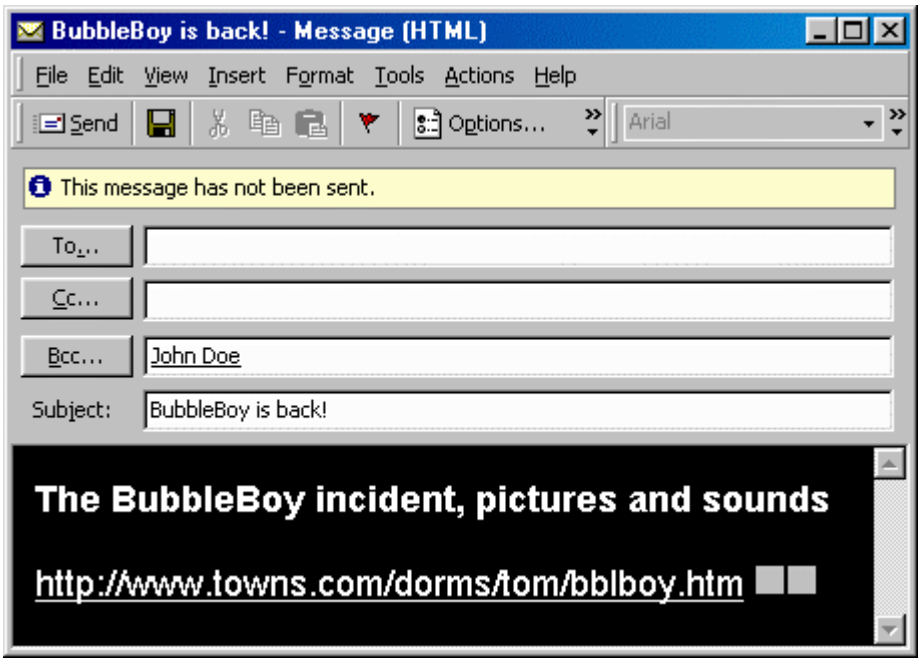
Bubbleboy se šíří jen pod MS Outlookem 98, Outlookem 2000 a Outlook Expressem, který přichází s Internet Explorerem verze 5. Nešíří se pod Windows NT. Využívá známou bezpečnostní „díru“ v Outlooku, pomocí níž vytváří HTA soubor ve složce

```
C:/WINDOWS/START MENU/PROGRAMS/START UP
```

Jedná se o soubor UPDATE.HTA, který po restartu počítače či při přihlášení nového uživatele změní údaje o vlastníkovi počítače na „BubbleBoy“ a společnost na „Vandelay Industries“. Navíc sám sebe rozešle na všechny adresy v adresáři Outlooku.

Infikovaný e-mail přitom má následující atributy:

```
Od: [jméno infikovaného uživatele]
Předmět: BubbleBoy is back!
Text zprávy: The BubbleBoy incident, pictures and sounds
```




Pokud si chcete být stoprocentně jisti, že se setkání s virem Bubbleboy vyhnete, nainstalujte si následující „záplatu“:

```
http://www.microsoft.com/security/Bulletins/ms99-032.asp
```

Resumé? Viru BubbleBoy se není zapotřebí vůbec obávat. Je však vysoce zdviženým varovným prstem. Pokud bychom jej nebrali vážně, mohlo by se nám to jednou v budoucnu ošklivě nevyplatit.

## *Pozor na počítačový virus FunLove!*

Antivirová společnost Kaspersky Lab (výrobce programu AVP) hlásí objev nového viru šířícího se v prostředí Windows. Jmenuje se Win32.FunLove. Jedná se přitom o velmi kvalitní „produkt“, který se úspěšně šíří po počítačích na celém světě.

Jedná se o virus napadající PE.EXE (Portable Executable) soubory na lokálních a síťových discích. Přitom díky svým schopnostem dokáže FunLove napadnout všechny síťové disky z jednoho infikovaného počítače – pokud to nastavení sítě umožňuje.

Jak získal virus své jméno? Celkem jednoduše. Všechny napadené soubory nesou ve svém těle následující text: ~Fun Loving Criminal~ (jedná se o jméno populární rockové skupiny).

Jakmile je infikovaný soubor spuštěn, vytváří soubor FLCSS.EXE v systémovém adresáři Windows. Do něj nejprve zapíše svůj kód – a poté jej spustí. Pod operačním systémem Win

95/98 se chová jako skrytá aplikace, pod NT jako aplikace servisní. Nepodaří-li se z jakéhokoliv důvodu viru vytvořit soubor FLCSS.EXE, spouští se infekční rutina přímo.

Infekční rutina postupně napadá všechny lokální pevné disky od C: do Z:, poté se ještě pokouší dostat na síť. „Pracuje“ tak, že prohledává všechny adresáře a podadresáře, kde napadá soubory s koncovkou OCX, SCR a EXE. Při útoku virus vepisuje svůj kód na konec souboru a do hlavičky vkládá „odskakovací“ rutinu – ta zajišťuje že v okamžiku spuštění souboru je vykonán programový kód viru. Délka napadeného souboru vzrůstá pod Win 95/98 o 4099 bajtů, pod NT minimálně o tuto hodnotu, zpravidla však ještě více.

Přestože FunLove nenese žádný nebezpečný „náklad“, jednu nepříjemnou vlastnost přece jen má. V prostředí NT totiž „ruší“ bezpečnostní nastavení a dovoluje tak přístup „všem všude“. Jinými slovy – kterýkoliv uživatel může nahlédnout do soukromých souborů kohokoliv jiného, což jistě není příjemné.

FunLove je velmi opatrný, nenapadá soubory ALER*, AMON*, _AVP*, AVP3*, AVPM*, F-PR*, NAVW*, SCAN*, SMSS*, DDHE*, DPLA*, MPLA* (jde většinou o antivirové programy).

Závěrem: Nebojte se na tento vir (i na kterýkoliv jiný) „nasadit“ některý z antivirových programů v nabídce AEC, spol. s r.o.: AVP, F-Secure AntiVirus, Norman Virus Control i VirusScan.


## *AEC, spol. s r.o. míří se svými programy do Austrálie*

„Záběr“ brněnské antivirové a bezpečnostní firmy AEC, spol. s r.o. se rozšiřuje. Před několika dny došlo k podpisu dohody o prodeji vlastního bezpečnostního software **IronWare® Security Suite** (dále jen IW Security Suite) do Austrálie. Dohoda zajišťuje prodej a podporu tohoto původního českého programu světových parametrů na australském kontinentě.

Partnerem AEC, spol. s r.o. v Austrálii se stala firma Support Solutions (Sales) Pty Ltd. se sídlem v Sydney, přední dodavatel systémů pro podporu managementu. Pro bezpečnostní program IW Security Suite se rozhodla, neboť otázka bezpečnosti a zabezpečení dat i informací se stále častěji stává v informačních systémech tématem číslo 1. Navíc se jedná o kvalitní mezinárodně uznávaný produkt, splňující veškeré požadavky na zajištění bezpečnosti informačních systémů.

Systém IW Security Suite je modulární, centrálně řízený bezpečnostní systém pro zabezpečení dat v LAN/WAN založený na Complex-PKI (dále jen C-PKI), které zajišťuje centrální správu šifrovacích klíčů a nejmodernější šifrovací algoritmy. C-PKI je srdcem systému IW Security Suite, jehož jednotlivé aplikační moduly se připojují k C-PKI přes otevřené standardizované rozhraní. Díky tomu je systém otevřen i pro speciální bezpečnostní moduly vyvinuté podle požadavků zákazníka.

## *Problém „Vir 2000“*

V souvislosti s nadcházející změnou koncového dvoujčíslí letopočtu z „99“ na „00“ se často hovoří o „problému viru roku 2000“. To je terminologicky poněkud zavádějící, problém roku 2000 (aka Y2K) totiž v žádném případě nesouvisí s žádným virem.

Proč? Protože problém roku 2000 souvisí s něčím zcela jiným než s počítačovými viry. Ovšem na druhé straně si musíme uvědomit, že počítačové viry nejsou mýtické bytosti z neznámé planety, ale „jen“ počítačové prográmky, které stvořili lidé z masa a kostí. A tito lidé si samozřejmě vyberou i čas a způsob projevu daného viru. Pokud je některých z „programátorů“ fascinovaný datem 1. ledna 2000, pak si jej samozřejmě vybere jako „rozbušku“ svého viru.

V současné době je známo několik virů, které „udeří“ v kritických datech na konci letošního a počátku příštího roku:

**25. prosince:**

- Sarampo
- W97M/Opey.A
- ***W97M/Opey.C***
- W32/Kriz
- W97M/Class.AZ

**31. prosince:**

- ***Chinese Fish***
- W97M/Caligula
- W97M/Chack.H

**1.ledna:**

- Chinese Fish
- November_17$^{th}$.800.A
- W97M/Marker.A

Mimo těchto virů mohou Vaše data a počítače ohrozit také následující „záškodníci“, kteří udeří v prvních pracovních dnech nového roku 2000:

**3.ledna:**

- Helper.F
- Buero
- Alien.H

**4.ledna:**

- Helper.D
- Buero
- Pathogen

V seznamu jsou uvedeny pouze viry, které jsou „In the Wild“, tedy ty, které se běžně šíří a vyskytují mezi uživateli. Jak výše uvedený seznam dokládá, přelom starého a nového roku je obdobím, kdy se více než kdy jindy vyplatí dbát na bezpečnost dat. K tomu může pomoci i

některý z antivirových programů AEC, spol.s r.o.: AVP, F-Secure AntiVirus, Norman Virus Control i VirusScan.

## *Šifruji, šifruješ, šifrujeme…*

Dnes představujeme další část bezpečnostního a šifrovacího programu IronWare® Security Suite, a to část věnovanou šifrování adresářových struktur a šifrování celých disků.

### Šifrování adresářových struktur

Nastavená šifrovací pravidla pro adresář se vždy aplikují i na nově zakládané soubory v těchto adresářích nebo na soubory, které jsou do nich přesouvány nebo kopírovány. Při kopírování souboru do šifrovaného adresáře se tady soubor automaticky zašifruje a při jeho zpětném kopírování do nešifrovaného adresáře automaticky rozšifruje. Všechny funkce pro nastavení šifrování jsou soustředěny ve standardním dialogovém okně vlastností adresáře, které lze vyvolat například pomocí pravého tlačítka myši. Jednotlivé adresáře (nebo celé stromové struktury) lze zašifrovat buď jedním tajným klíčem nebo jedním sdíleným klíčem. U adresářů, které není vhodné přiřazovat k šifrování (adresáře s operačním systémem apod.), lze šifrování zakázat. Praktický význam všech možností je shrnut v následujících bodech:

- **Šifrování tajným klíčem** – soubory v takto nastaveném adresáři jsou zašifrovány klíčem, který vlastní pouze jediný uživatel. V praxi se toto nastavení používá pro přidělení adresářů se soukromými daty jednotlivých uživatelů – např. domácí adresáře na souborovém serveru či stromové struktury s dokumenty na lokálním pevném disku.
- **Šifrování sdíleným klíčem** – soubory v tomto adresáři jsou zašifrovány klíčem, který je sdílen více uživateli. V praxi se používá např. pro nastavení adresáře, jehož obsah je nutné sdílet mezi pracovníky např. určitého oddělení. Konkrétně se může jednat např. o databázi zákazníků sdílenou obchodním oddělením nebo data účetního software používaná účetním oddělením.
- **Vyhrazení adresářů** - takovýto adresář nemůže být přidělen k šifrování. V praxi se používá např. pro adresáře obsahující operační systém nebo některé části programů. Pokud bude k šifrování přidělen adresář nadřazený takto označenému podadresáři, bude tento podadresář při šifrování vynechán („obtečen“ ).

Z bezpečnostního hlediska jsou takto zajištěné soubory účinně chráněny proti porušení důvěrnosti před každým, kdo nepatří mezi jejich vlastníky (tedy jak proti ostatním zaměstnancům, tak proti vnějšímu narušiteli). Významnou vlastností je, že soubory jsou vždy rozšifrovány až v operační paměti koncové stanice – tj. až těsně před předáním dat koncové aplikaci. Díky tomu jsou data účinně chráněna proti odposlechu při přenosu jakoukoli sítí (LAN či WAN).

IW FileProtect počítá i s možností přegenerování klíčů v IW KeyManageru. Poté nově zakládané soubory šifruje novým klíčem, ale soubory původní dešifruje stále původním klíčem. Na požádání je možné všechny soubory přešifrovat novým klíčem. Tuto akci může provést pouze uživatel, který má k novému klíči přístup.

**Šifrování celých disků**

Protože v praxi obvykle používá jeden počítač pouze jediný uživatel (tj. data na lokálním disku není třeba diferencovat pro různé uživatele a jediným nebezpečím je tedy vnější narušitel – což platí zejména pro notebooky), ukázalo se výhodné provádět nastavení takovýchto stanic následujícím způsobem:

Pevný disk je rozdělen na dva logické oddíly – C: obsahuje operační systém a programy,
D: obsahuje cenná data.

Po takovém rozdělení nastavíme šifrování na kořenový adresář disku D: (s aktivovanou volbou včetně podadresářů). Šifrování provedeme tajným klíčem uživatele počítače. Pokud je příliš obtížné rozdělit disk na dva logické disky a přesunout data na druhou část, můžeme zvolit i jinou strategii. Na stávajícím disku C: nastavíme adresáře obsahující Windows a adresáře obsahující programy (standardně adresář Program Files včetně podadresářů) jako vyhrazené, ve kterých se nebude šifrovat a poté necháme zašifrovat všechny ostatní adresáře tajným klíčem uživatele.

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