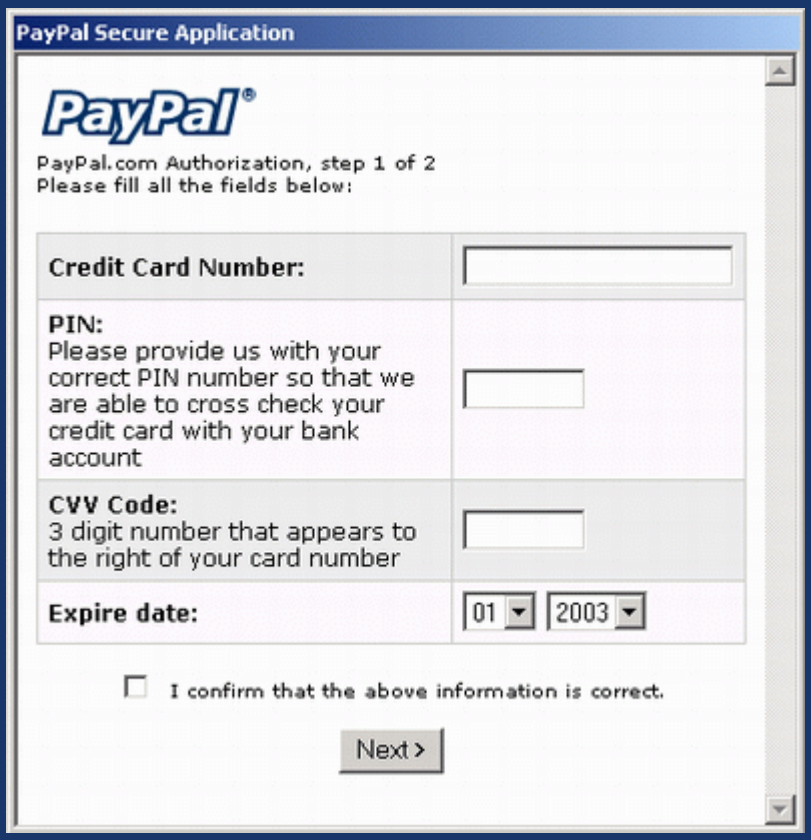
informační
# bulletin
AEC DATA SECURITY COMPANY

(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: Mimail.l a J**
- **Novinky mezi počítačovými viry: Sober**
- **AEC Antivirus Gateway: řešení pro lokální síť**
- **Softwarové novinky od AEC**




**Mezi záplavou škodlivých kód, které se objevily v průběh roku 2003 byl také Mimail.l, který se předstíral, že slouží k ověření informací platebního systému Paypal. Namísto toho ale od důvěřivých uživatelů odcizoval osobní informace (včetně přístupového hesla), díky čemuž neznámý hacker mohl krást peníze.**

AEC DATA SECURITY COMPANY

# Novinky mezi počítačovými viry: Mimail.I a J

V průběhu listopadu 2003 se objevily další dvě nové verze e-mailového červa Mimail. Jejich tvůrce si tentokrát jako maskování vybral motiv on-line platebního systému PayPal, s jehož pomocí se snaží vylákat informace o platební kartě infikovaného uživatele.

E-mailová adresa odesílatele je v obou případech falešná: „PayPal.com“ donotreply@paypal.com. Mimail.I používá předmět zprávy „YOUR PAYPAL.COM ACCOUNT EXPIRES“ a přiložený soubor nese název www.paypal.com.scr. Mimail.J má zase poněkud strohý předmět „IMPORTANT“ a přiložený soubor www.paypal.com.pif. V textu zprávy je vložena e-mailová adresa příjemce, což může u některých uživatelů vzbudit zdání důvěryhodnosti.

Pokud příjemce červa z přiloženého souboru spustí, je mu nejprve zobrazen falešný webový formulář, který imituje grafický styl platebního systému PayPal. Tímto formulářem se červ snaží uživatele přinutit ke vložení údajů o jeho kreditní kartě. Ty jsou zaznamenány do souboru c:\ppinfo.sys, který je později odesílán e-mailem na určité adresy. Dále se červ instaluje do systémového adresáře Windows pod jménem svchost32.exe a registruje klíč v systémovém registru, kterým zajišťuje svoje spuštění při každém startu operačního systému.

E-mailové adresy pro další šíření sbírá ze souborů nalezených na pevném disku infikovaného počítače. Při vyhledávání adres vynechává soubory, jejichž přípona je na jeho zvláštním interním seznamu. Samotné rozesílání provádí pomocí vlastního SMTP motoru, který k nalezení cílového SMTP serveru používá předem definovaný seznam veřejných DNS serverů.

# Novinky mezi počítačovými viry: Sober

Škodlivý kód Sober se objevil v průběhu října 2003. V několika následujících dnech zaznamenaly různé antivirové firmy vzrůstající trend šíření tohoto svými vlastnostmi „klasického“ e-mailového červa.

E-mailové zprávy, ve kterých se Sober šíří, mohou být v anglické nebo německé jazykové verzi. Červ se pokouší zneužívat sociálního inženýrství, takže se může v některých případech vydávat např. za update chránící před novým smyšleným červem apod. Pro svůj soubor přiložený k e-mailu používá jména jako anti_virusdoc.pif, check-patch.bat nebo např. playme.exe.

Pro rozesílání infikovaných zpráv používá vlastní SMTP motor. Adresy čerpá z různých souborů nacházejících se na pevném disku infikovaného počítače (htt, rtf, doc, xls, ini, mdb, txt, htm, html, wab, pst, fdb, cfg, ldb, eml, abc, ldif, nab, adp, mdw, mda, mde, ade, sln, dsw, dsp, vap, php, asp, shtml, shtm, dbx, hlp, mht, nfo). Všechny nalezené kontakty ukládá do speciálně vytvořeného souboru MEDIA.DLL v adresáři %SysDir%\MACROMED\HELP\.

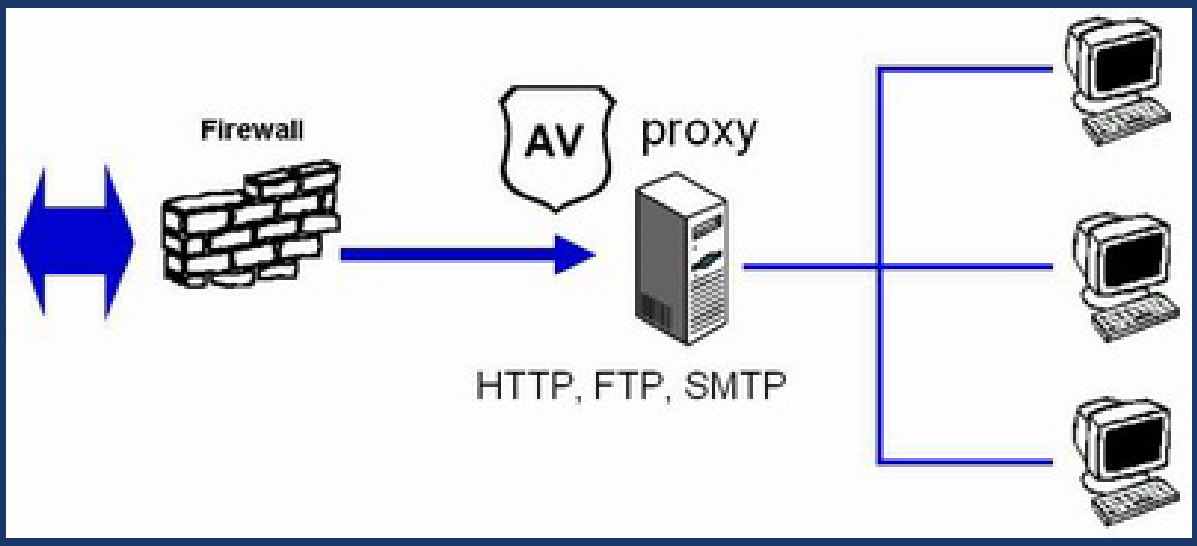
Při své instalaci do systému zobrazuje falešné chybové hlášení s textem: *"Error. File not complete!"* Na disk se kopíruje do systémového adresáře Windows jako SIMILARE.EXE. Kromě toho vytváří ještě další dva soubory s náhodně zvoleným názvem, které se starají o to, aby proces červa nebyl přerušen zvenčí. V takovém případě jej spouští znovu ze záložní kopie.

AEC
DATA SECURITY COMPANY

# AEC Antivirus Gateway: řešení pro lokální síť

**Pokud právě přemýšlíte, jak dokonale ochránit lokální podnikovou síť před e-mailovými červy, škodlivými kódy a dalším smetím, které dnes a denně přichází z internetu a nemáte chuť ani čas nic složitě instalovat a nastavovat, máme pro Vás dokonalé řešení. Společnost AEC v těchto dnech uvádí na český trh nové antivirové zařízení pro centrální ochranu podnikových sítí.**

**AEC Antivirus Gateway splňuje všechny požadavky moderní antivirové ochrany internetových vstupních bran. Jedná se o komplexní řešení, které dokáže spolehlivě zastavit veškeré nebezpečné virové infekce ještě před tím, než se mohou dostat do vnitřní sítě na poštovní server nebo k uživatelům. Kromě samotné základní funkce antivirové ochrany tak efektivně zabraňuje také případným výpadkům sítí a dalším incidentům spojeným s masivními epidemiemi internetových červů.**

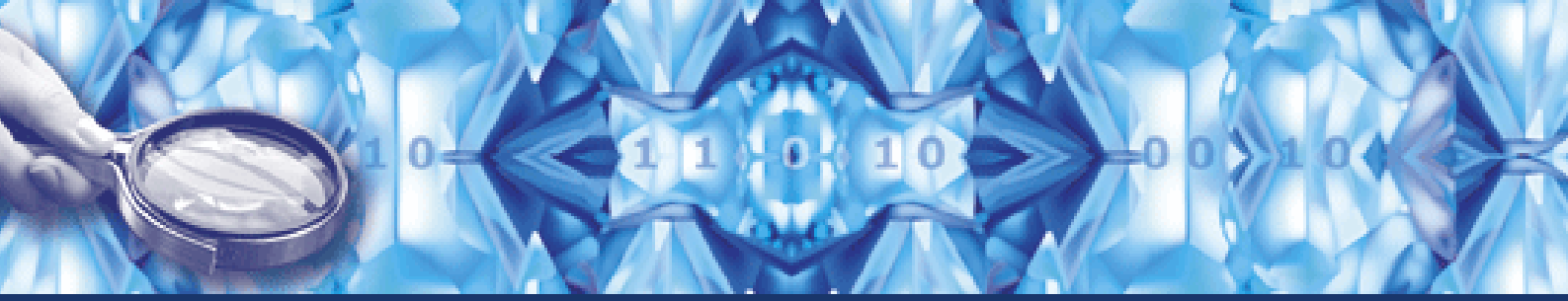



**AEC Antivirus Gateway funguje na principu tzv. antivirového proxy, které se umisťuje do vnitřní sítě přímo za podnikový firewall, kde vytváří virtuální bránu zabraňující vstupu infikovaného datového provozu. Zařízení samo o sobě je kombinací silného a spolehlivého hardware a speciálně odladěného antivirového software F-Secure Internet Gatekeeper. Ten kontroluje datový provoz na protokolech SMTP, HTTP a FTP (přes HTTP). Řešení je nezávislé na firewallu a samotném poštovním serveru. Program lze jednoduše vzdáleně spravovat pomocí nástrojů F-Secure Policy Manageru, který je k produktům F-Secure dodáván zdarma.**

**Výhodou AEC Antivirus Gateway je kromě dalších vlastností především vysoká rychlost skenování, kterou uživatelé ocení zejména při kontrole HTTP provozu. Spolehlivě zvládá přenosové kapacity linky 12 MB/s. Dokáže účinně blokovat závadný e-mailový (např. různé druhy přiložených souborů) a webový provoz (např. zvukové a video soubory). Administrátor dostává do rukou efektivní nástroje pro kontrolu dat stahovaných z webu jednotlivými uživateli.**

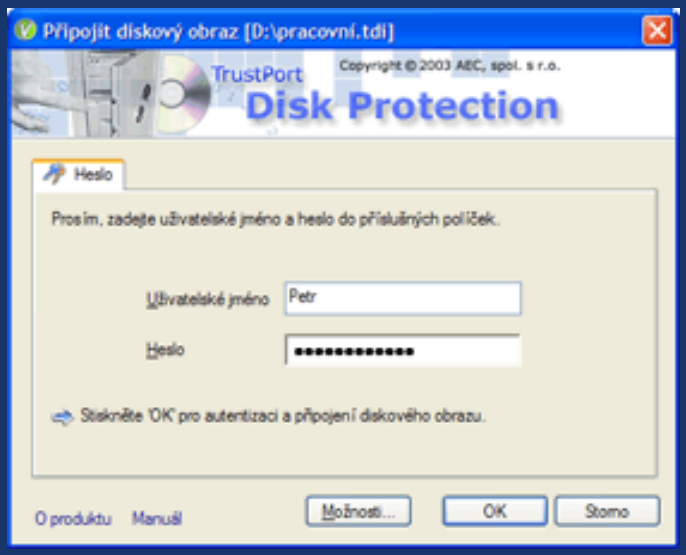
**Nedílnou součástí AEC Antivirus Gateway jsou kromě hardware a software i služby spojené s instalací zařízení do sítě, nastavením a celkovým zprovozněním. Samozřejmostí je technická podpora na nadstandardní úrovni.**

AEC
DATA SECURITY COMPANY



# Softwarové novinky od AEC

**Během posledních několika měsíců jste si mohli všimnout několika stěžejních softwarových novinek, které opustily vývojového oddělení společnosti AEC.**




**První významnou událostí je uvedení nové aplikace pro transparentní on-line šifrování TrustPort® Disk Protection. Nejprve samozřejmě spatřila světlo světa anglická verze tohoto programu. V nedávných dnech však byla vydána i verze česká. Připomeňme jen, že program vytváří virtuální diskové jednotky, jejichž obsah je při ukládání automaticky šifrován. S obrazy šifrovaných disků lze velice jednoduše manipulovat - např. vypálit na CD a uchovávat tak zálohy dat v šifrované podobě...**

**Další netrpělivě očekávanou novinkou byla první verze nového TrustPort® Personal Firewallu. Jedná se o řešení vhodné jak pro pokročilé uživatele, kteří disponují znalostmi síťových protokolů a služeb, tak i pro ty, kterým vyhovuje použití předpřipravených sad konfiguračních pravidel. Personální firewall vytváří na chráněném počítači bezpečnou bránu, kterou procházejí veškerá síťová připojení. Brána umožňuje pomocí definovaných pravidel povolovat nebo zakazovat určité druhy komunikace s okolní sítí. Jednotlivé sady pravidel je možno přiřadit ke konkrétní IP adrese (kterou je reprezentován příslušný síťový adaptér) či určitému rozsahu adres.**

**Nastavení programu se provádí pomocí modulu TrustPort® Personal Firewall Configurator, který umožňuje editaci stávajících a vytváření nových pravidel. Funkce jejich importu a exportu umožňuje jednoduché sdílení a výměnu konfigurací mezi jednotlivými uživateli, což významně ulehčuje správu většího počtu instalací např. v lokální síti. Firewall je vždy po instalaci implicitně nastaven tak, že veškerá průchozí spojení blokuje. Teprve jeho konfigurací vytváříme pravidla povolující průchod určených datových toků. Také v případě TrustPort® Personal Firewallu je už v současné době k dispozici jeho anglická i česká verze.**


AEC
DATA SECURITY COMPANY