AEC Virus Eye

Obsah:

www.aec.cz

Pro PC WORLD připravuje Tomáš Přibyl - tomas.pribyl@aec.cz

VAROVÁNÍ PŘED VIREM, KTERÝ NEEXISTUJE

Čas od času snad každému uživateli elektronické pošty objeví v jeho mailboxu zpráva varující před mimořádně nebezpečným a právě objeveným virem, proti kterému není „lék" a který je nesmírně agresivní. Zároveň příjemce vybízí, aby vykonal dobrý skutek a pomohl šíření viru zastavit tím, že právu o něm předá dál.

Takovýmto zprávám se říká „hoaxy" (což česky znamená „žertík" či „smyšlenka").

Jedním z takovýchto „hoaxů" je e-mail následujícího znění, který se poprvé objevil ve Spojených státech někdy ve druhé polovině roku 1998 (samozřejmě v angličtině), o několik měsíců později pak nějaký neznámý dobrodinec prokázal uživatelům českého internetu doslova „medvědí službu" a přeložil jej do jazyka českého. Zřejmě neexistuje lidská síla, která by jeho šíření dokázala zarazit, takže je velmi pravděpodobné, že se s ním (nebo s nějakým velmi podobným e-mailem) dříve či později setkáte.

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 obrazovky "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 virus 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.

A samozřejmě, že „Důležitost" u této zprávy byla nastavena jako „Velká!"

Většina „běžných uživatelů" se k smrti vyděsí, ani na okamžik je nenapadne pochybovat a uposlechne žádosti o rozeslání e-mailu na co největší množství adres. A to je právě ta největší chyba. Žádný vir Buddylst.zip totiž neexistuje, nikdo jej nikdy neviděl. Podobné zprávy mají jediný cíl: lavinovité šíření a způsobování paniky.

Přitom z e-mailové hlavičky zprávy, která „přinesla" varování před všezničujícím „virem" Buddylst.zip je zřejmé, že tento blud prošel počítači již několika desítek uživatelů.

Podívejme se nyní na tuto konkrétní zprávy kapku podrobněji. Psychologicky i technicky je totiž připravena více než dobře, byť po podrobnější prohlídce má několik „zádrhelů".

Úvod je nádherný – jste ubezpečeni, že vás mají všichni moc rádi a že jim osud vašich dat (a potažmo i nervové soustavy) není lhostejný. A teď přichází onen hlavní „strašák" – po internetu koluje tajuplný destruktivní soubor. Uživatel bystří pozornost. Protože zpráva přišla elektronickou poštou, znamená to, že je napojený na internet a že se jej bytostně týká. To by mohlo být nebezpečné, navíc zpráva přichází od osoby známé nebo blízké (a tudíž brané jako důvěryhodné). Na tom něco bude.

Ovšem je tu několik logických chybiček. Autor zprávy evidentně nezná rozdíly mezi „virem" (část programového kódu, která se šíří bez vědomí uživatele a jeho zásahu) a „trojským koněm" (program, který vykonává mimo svého hlavního úkolu ještě další činnosti, o kterých uživatel nemá ani potuchy). Podle popisu je tedy Buddylst.zip trojským koněm (mimo spořiče obrazovky provádí i „neplechu" v počítači) a nikoliv virem, jak jej chybně označuje autor zprávy.

Ale budiž, drobná terminologická chybička není katastrofou, za kterou by se muselo popravovat.

„Harddisk bude úplně zničen a osoba, která Vám poslala zprávu, bude mít přístup k Vašemu jménu a heslu přes internet." Hrůza hrůzoucí. Ale zkuste si položit otázku: K čemu bude neznámému hackerovi seznam mých hesel, když všechny informace jím chráněné budou ve věčných lovištích všech informací?

Další logická chyba: Přestože o dotyčném „viru" nikdo nic neví, jsou známy jeho destruktivní aktivity! A punc důvěryhodnosti zprávě dodává jméno Microsoft. Proč ale o viru „informuje" právě tento gigant a nikoliv antivirové firmy, které mají podobnou činnost v náplni práce? Myslíte si, že informační politika společnosti Microsoft (nebo kterékoliv jiné firmy) spočívá v posílání e-mailových zpráv s výzvou „rozeslat co nejvíce lidem"? Chybí i jakýkoliv časový údaj kromě poněkud volné formulace „včera ráno". Tato je použitelná dnes, zítra, za týden, za měsíc, prostě kdykoliv. To je případ i výše uvedeného hoaxu – ač starý již několik let, po čase se znovu a znovu vynořuje ze zákoutí internetu.

A na závěr to nejdůležitější: „Prosím podnikněte veškerá opatření a předejte tuto informaci Vašim přátelům, známým a kolegům v práci." Autor zprávy vyzývá k podniknutí opatření a zároveň

nabádá, o jaká opatření má jít: Rozeslat tento e-mail co nejvíce lidem. A právě v tomto je největší nebezpečí tzv. hoaxů. Jejich masové šíření, kterému mnozí uživatelé houfně napomáhají. Jedná se o jakousi obdobu proslulého viru Melissa, který se od každého uživatele rozesílal na padesát dalších e-mailových adres (ten se ale nespouštěl pouhým otevřením e-mailu, ale až připojeného wordovského souboru, který obsahoval makrovirus).

Shrňme si nyní výše uvedené poznatky z jednoho konkrétního případu do několika víceméně obecných postulátů:

- Hoax typicky obsahuje varování před novým virem.
- Virus je vždy destruktivní.
- Virus je vždy neznámý a není proti němu ochrany.
- Důvěryhodnost má zprávě dodat jméno některé z renomovaných firem v daném případě Microsoft a AOL.
- Zpráva neobsahuje odkaz na antivirovou firmu. Pokud nějaký odkaz obsahuje, pak zpravidla telefonní číslo nějakého administrátora kdesi daleko za hranicemi – tedy telefon, kam normálního smrtelníka ani nenapadne zavolat.
- Dle zprávy je většinou nebezpečná již jen samotná manipulace s e-mailem,
- Zpráva vždy obsahuje výzvu k tomu, aby byla rozeslána dále

Jak se bránit? Obrana neexistuje – snad jen zakázat v poštovním klientovi přijímání zpráv od určitých osob, které ve jménu dobrodiní celého lidstva rozesílají hoaxy každé dvě hodiny. 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: Ve většině případů stačí třeba pouhý pohled na webovskou stránku, protože o události podobného typu zcela určitě informují. Zajímavým zdrojem informací je také stránka **www.hoax.cz**

Mimo výše uvedené zprávy „Buddylst.zip" (přičemž „na lep" jí sedl i jeden významný český deník, který hoax redakčně upravit a bezostyšně vydal jako velkou senzaci) světem koluje několik tisíc podobných „varování". Za zmínku stojí například zpráva označována jako „Good Times", která se v několika mutacích znovu a znovu vynořuje z hlubin internetu, objevuje se např. jako „Irina", „Penpal Greetings", „PKZIP300" nebo „Deeyenda Maddick". Úsměvně působí příběh programku SHEEP, který spouštěl poměrně vyvedenou grafiku skotačícího beránka. Program byl mnoha e-maily označován za krvelačného trojského koně ničícího data na pevném disku až do té doby, kdy se z Japonska přihlásil jeho udivený tvůrce. Mimochodem byl překvapen i nekontrolovaným šířením svého programu, který byl určen výhradně pro komerční účely. Spousta těchto zpráv se nesnaží ani nijak maskovat, že se jedná o žert, například tzv. „Naughty Robot", který o sobě tvrdil, že je „internetovým pavoukem" sbírajícím důvěrná data.

Hoax přitom nemusí mít vždy všechny výše popsané příznaky – dokonce nemusí jít ani o varování před počítačovým virem. Velice často totiž využívá metod sociálního inženýrství – prostě jakýkoliv „podvůdek", na který lidé zareagují a zprávu rozešlou dál. Jakákoliv anonymní zpráva, byť se navenek tvářící jako sebelepší úmysl (výzva k záchraně jihoamerických deštných pralesů či snaha o získání vzácné krevní skupiny pro kamaráda), anonymem také zůstává. A uvedený odkaz v těle zprávy na třetí stranu (web nějaké nadace nebo telefonní číslo nemocnice) není podpisem, ale pouze odkazem.

Pravděpodobnost, že se setkáte s nějakým hoaxem je dost velká. Je tedy vhodné být připraveni a naučit se rozlišovat mezi informacemi a „informacemi".

NETSKY, NETSKY, NETSKY…

Další z nesčetných variant e-mailového červa NetSky se objevila 13. října 2004.

Charakteristické vlastnosti:

- Rozesílání infikovaných e-mailů pomocí vlastního SMTP motoru.
- Získávání e-mailových adres z různých souborů nacházejících se na disku infikovaného počítače.
- Falšování adresy odesílatele infikovaného e-mailu.

Pokud je červ z infikovaného e-mailu uživatelem spuštěn, zobrazuje maskovací dialogové okno s textem: „File corrupted replace this!". Červ se do systému infikuje jako MsnMsgrs.exe do systémového adresáře Windows. Do systémového registru dále přidává klíč, který zajišťuje jeho spuštění. Do adresáře Windows červ kopíruje další soubory s příponou ZIP.

E-mailové adresy červ čerpá z různých typů souborů nalezených na disku infikovaného počítač. Dokáže zpracovat soubory s těmito příponami: .adb, .asp, .dbx, .doc, .eml, .htm, .html, .php, .pl, .php, .rtf, .uin, .vbs, .wab, .oft,.sht, .tbb, .txt.

Infikovaná zpráva je seskládána z mnoha předem daných komponent (různý předmět, text a název přiloženého souboru). Přípona souboru s červem může být .pif, .com, .scr, .bat nebo .zip.

NEBEZPEČÍ TAKÉ PRO OBRÁZKY?

Čtrnáctého září 2004 společnost Microsoft zveřejnila v rámci Microsoft Security Bulletinu (MS04-028) také chybu, která umožňuje zneužití obrázku ve formátu JPEG ke spuštění škodlivého kódu na počítači, kde je zobrazen. Chyba spočívá v přetečení paměti (buffer overrun) při zpracování grafického souboru.

Díky této chybě může být počítač infikován škodlivým kódem při prohlížení webové stránky, která obsahuje příslušným způsobem upravený JPEG soubor, pomocí MS Internet Exploreru nebo čtení e-mailové zprávy v HTML formátu, která škodlivý JPEG soubor obsahuje, v některé ze zasažených verzí Outlooku. Ke spuštění nežádoucího kódu může dojít i v případě, že je obrázek vložen v dokumentu MS Office a dokonce i tehdy, když si uživatel uloží zákeřný JPEG soubor do adresáře na disk svého počítače a obsah tohoto adresáře si posléze prohlíží pomocí Windows Exploreru (běžné prohlížení obsahu disků).

První pokusný kód zneužívající tuto chybu (exploit), který dokáže spustit kód vložený v JPG souboru v okamžiku, kdy je tento otevřen byl zveřejněn na webu již 17. září. Tento exploit pouze „shazuje" Internet Explorer.

Už 24. září se ale objevil nástroj, který umožňuje vytvářet JPG soubory obsahující MS04-028 exploit. V tomto případě dokáže stáhnout z internetu a spustit v podstatě jakýkoliv soubor. Funguje ale pouze v případě, že je obrázek prohlížen lokálně (tzn. je stažen přímo do počítače). Pokud je obrázek prohlížen vzdáleně (např. na webové stránce), škodlivý kód se neaktivuje.

Zcela jistě se ale dá očekávat, že postupem času budou vytvořeny další nástroje zneužívající uvedenou bezpečnostní chybu, které mohou být daleko propracovanější a nebezpečnější. Kdokoliv může časem vytvořit univerzální exploit, který bude fungovat i při „vzdáleném" prohlížení infikovaného obrázku.

Doporučujeme tedy nainstalovat všechny potřebné bezpečnostní záplaty dané k dispozici společností Microsoft. Můžete je najít např. na
http://www.microsoft.com/security/bulletins/200409_jpeg.mspx

Otestovat, zda je váš počítač náchylný na uvedenou chybu, můžete pomocí utility, kterou najdete zde:
http://www.microsoft.com/downloads/details.aspx?familyid=71CD9E74-7142-4780-83E5-CE54401DA1D1&displaylang=en

F-SECURE INTERNET SECURITY 2005

Pomyslné brány společnosti F-Secure opouští nové verze programů F-Secure Internet Security 2005 a F-Secure Client Security. Kromě mnoha vylepšení, která obsahují, je důležité i to, že jsou v češtině.

F-Secure uvolnil nové verze svých programů určených k ochraně domácích uživatelů a malých firem, které nemají vlastní IT oddělení. F-Secure Internet Security 2005 a F-Secure Anti-Virus 2005 nově obsahují nástroje na likvidaci spyware a záchranné CD. F-Secure Internet Security 2005 navíc přináší ochranu před hrozbami přicházejícími z internetu. Kromě anti-spyware obsahuje také funkce pro kontrolu přístupu, likvidaci spamu, přesměrování vytáčeného internetového připojení a ochranu proti dalším zranitelnostem.

F-Secure Internet Security 2005 obsahuje oproti předchozí verzi množství nových funkcí a vylepšení. Anti-spyware chrání uživatele před nežádoucími aplikacemi, které mohou být instalovány s některým software (např. klienty P2P sítí). Další nové funkce zabraňují úniku citlivých informací, které mohou být odeslány z chráněného počítače do internetu některými škodlivými kódy. Nejmladší uživatelé jsou chráněni před nežádoucím obsahem přicházejícím z internetu pomocí modulu „Parental Control". Program dokáže blokovat internetové stránky obsahující odkaz na nežádoucí materiály. Anti-Spam filtruje nevyžádané e-mailové zprávy a redukuje útoky typu „phishing". Anti dialer zabraňuje nežádoucímu podvodnému přesměrování vytáčeného připojení k internetu na drahé linky bez vědomí uživatele. Nový systém automatické aktualizace udržuje denně všechny součásti programu (virové definiční databáze, parental control a anti-spam) v maximální pohotovosti tak, aby dokázaly reagovat na každou novou hrozbu. Uživatel má taktéž k dispozici bezpečnostní zpravodajství informující ho o nových hrozbách. F-Secure Internet Security 2005 je kompatibilní s Windows XP SP 2 a podporuje také Microsoft Security Center, do kterého je integrován.

[KONEC magazínu AEC VIRUS EYE]