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:

- **Ohlédnutí za počítačovými viry roku 2003**
- **TrustPort® Mobile Encryption jde do světa**
- **Kaspersky uvádí Anti-Virus pro ISA server**
- **Kdo píše počítačové viry?**

Stejně jako v letech minulých, i letos se bude pod odbornou záštitou společnosti AEC a ze mediálního partnerství vydavatelství Vogel Publishing konat konference Security. Její první ročníky se uskutečnily již počátkem devadesátých let (tehdy ještě pod názvem Virus), od té doby se konference stala stálicí na českém bezpečnostním nebi s pravidelnou účastí předních domácích i zahraničních specialistů a vysokou návštěvností. Letošní ročník akce se bude konat v úterý 6. dubna v prostorách hotelu Andel´s. Bližší informace naleznete na konference.aec.cz

AEC DATA SECURITY COMPANY

Ohlédnutí za počítačovými viry roku 2004

Minulý rok 2003 byl z pohledu problematiky počítačových škodlivých kódů rokem velice rušným. Nebudeme daleko od pravdy, když ho označíme za jeden z nejrušnějších v jejich dosavadní dvacetileté historii. Evidovaný počet známých virů, červů a dalších druhů škodlivého software se během minulého roku těsně přiblížil hranici devadesáti tisícům exemplářů.

Rok 2003 byl především rokem červů. Nejprve to byli červi síťoví, kteří překvapili rychlostí a objemem svého šíření. Když už se zdálo, že nemají konkurenci a jejich e-mailoví „příbuzní“ jsou mimo hru, objevil se Sobig.F, který tuto teorii razantně vyvrátil. Ve stínu červů však během celého roku nenápadně zvedali hlavu trojští koně, dialery a další škodlivé programy určené pro špehovaní. Všeobecně se dá říci, že v minulém roce se počítačové viry posunuly od „dětských hrátek“ pubertálních programátorů dokazujících si svoje schopnosti do světa „těžkého byznysu“. Řada moderních škodlivých kódů a jejich výstupy jsou nyní zneužívány např. spammery, pro které jsou nejen zdrojem e-mailových adres, ale i počítačů zneužitelných při skrytém rozesílání nevyžádané pošty.

Pojďme se tedy podívat na virové události tak, jak je přinášely jednotlivé měsíce minulého roku.

Leden

- Útok síťového červa Slammer. I když Slammer infikoval pouze Microsoft SQL servery, přesto v době, kdy jeho epidemie vrcholila, způsobil svým šířením značné škody. Za méně než 15 minut dokázal obsáhnout všechny dostupné IP adresy v celém internetu a masivní provoz, který vygeneroval, dokázal zablokovat řadu sítových prvků a služeb.
- První člen rodiny Sobig (verze „A“) je na světě. Zatím se jedná o nepříliš výrazného „řadového“ e-mailového červa.

Únor

- Červ Lovgate se šíří přes síťová sdílení. Zajímavý je hlavně svou schopností proniknout i přes síťová sdílení chráněná heslem, k čemuž využívá slovníkový útok. Nespoléhá však výhradně na tuto cestu a čile se šíří i pomocí starého dobrého e-mailu.

Březen

- Další červi inspirovaní Lovgatem snažící se o lámání hesel síťových sdílení (Deloader a další verze Lovgate).
- E-mailový červ Ganda využívá téma války v Iráku.

Květen

- Komplexní e-mailový/P2P/IRC červ Fizzer ve službách spammerů. Objevuje se v prvních květnových dnech. Kromě e-mailu se dokáže šířit také pomocí výměnné sítě KaZaa. Obsahuje zadní vrátka na bázi IRC, nástroj pro DoS útoky, trojského koně kradoucího hesla a HTTP server s některými dalšími komponentami.
- Druhá a třetí varianta červů Sobig („B“ a „C“). Obě se záhy objevují „In the Wild“, zneužívají metod sociálního inženýrství a mají časově omezenou funkčnost. Že by jejich programátor stále něco vylepšoval?

Červen

- Druhá verze červa Bugbear.B se specializuje na banky. Podobně jako původní verze v sobě kombinuje schopnosti e-mailového a síťového červa s keyloggerem, trojským koněm. Navíc dokáže být do jisté míry polymorfní. Na mušku si bere hlavně bankovní instituce z celého světa. Seznam jejich domén si nese s sebou - v ČR si ale vybral špatně: union.cz.
- Čtvrtá a pátá varianta z rodiny Sobig („D“ a „E“). Verze „D“ obsahuje chybičky a nešíří se, ale verze „E“ se více než povedla a má se čile k světu.

AEC
DATA SECURITY COMPANY

Srpen (jeden z nejhorších měsíců virové historie)

- První „drobeček“ z rodiny červů Mimail. Pod rouškou důležité zprávy od lokálního systémového administrátora úspěšně klame některé uživatele.
- Síťový červ Blaster (alias Lovsan) se šíří po celém světě. Zneužívá v té době několik týdnů známou chybu v RPC komponentě operačních systémů Windows a vynucenými restarty způsobuje nemalé problémy uživatelům nezáplatovaných počítačů. Jeho 6 kB kód obsahuje mimo jiné velice efektivní rutinu generování IP adres. Mediální publicitu si vysloužil hlavně plánovaným útokem všech svých kopií na server windowsupdate.com.
- Další síťový červ Welchi (alias Nachi) se ho snaží likvidovat. Ale svým šířením, které je podobně úspěšné, způsobuje řadu dalších incidentů. Červ bohužel zůstává červem, i když jeho úmysly jsou dobré.

- Sobig.F překonává všechny dosavadní rekordy. Sobig ve své zatím poslední verzi naplno využívá svůj potenciál, který mimo jiné nashromáždily i jeho verze předchozí. Jednotliví uživatelé hlásí stovky až tisíce, větší organizace a poskytovatelé internetového připojení i stovky tisíc exemplářů zachycených infikovaných e-mailů. Tomuto náporu podléhají některé servery. Sobig.F však navíc obsahuje skrytou funkci, která umožňuje jednotlivým kopiím červa se synchronizovat a ve stanovený čas stáhnout z dvaceti předem definovaných počítačů v internetu další škodlivý kód. Díky úsilí antivirových firem , ISP a bezpečnostních organizací se tomu podařilo včas zabránit. Na druhé straně se ale už nikdy nedovíme, co tento kód obsahoval. Objevují se spekulace, že jednotlivé verze Sobig jsou výtvorem neznámé organizace, která červa využila k získání prostředků pro instalaci skrytých proxy serverů zneužívaných spammery k rozesílání nevyžádané pošty.

Září

- Objevuje se červ Swen maskovaný za bezpečnostní záplatu. Dokonalá ukázka sociálního inženýrství. Swen zneužívá více metod šíření a pokud se v systému usadí, dá práci ho odtud dostat. Snaží se totiž aktivně „bojovat“ proti antivirovým programům i zásahům uživatele, které by ho mohli poškodit.

Říjen

- Červ Mimail.C podniká DoS útoky. Pokud jste v této době dostali e-mail od „kolegy“ Jamese, bylo třeba se mít na pozoru. Červ totiž zneužíval místní doménové jméno.
- Červ Sober se skrývá pod rouškou antivirové utility.

Listopad

- Deset nových variant červa Mimail během jediného měsíce. Nemá rád anti-spamové organizace a hlavně jejich servery, proti kterým podniká z infikovaných stanic DoS útoky. Kromě toho krade čísla kreditních karet a uživatelské údaje pro přihlášení do on-line platebních systémů, za které se za tímto účelem „převléká“.

Prosinec

- Sober se vrací ve verzi „C“. Poklidnou předvánoční atmosféru ale příliš nenarušuje.

AEC
DATA SECURITY COMPANY

TrustPort® Mobile Encryption jde do světa

Šifrovací program TrustPort Mobile Encryption z dílny společnosti AEC, který je určen pro instalaci na mobilní komunikátory Nokia 9210, je nyní k dispozici prostřednictvím Nokia Software Market.

Programy TrustPort Mobile Encryption, které jsou plně kompatibilní s aplikací TrustPort Archive Encryption pro počítače PC, jsou dostupné pro platformy EPOC a Pocket PC. Verzi pro platformu EPOC 6.x používanou na komunikátorech Nokia 9210 zařadil do své nabídky i jejich výrobce ve svém webovém Nokia Software Market, což lze považovat za potvrzení jeho kvalit.

TrustPort Mobile Encryption pro EPOC slouží pro šifrování a dešifrování dat. Používá formát CPH. Původní soubory, které jsou šifrovány, mohou být v případě potřeby bezpečně smazány. Se soubory CPH lze jednoduše pracovat i na klasických počítačích PC pomocí aplikace TrustPort Archive Encryption.

Pomocí TrustPort Mobile Encryption mohou šifrovat i uživatelé mobilních zařízení se systémy Microsoft Pocket PC. V této verzi dokáže program kromě souborů CPH pracovat i s plnohodnotnými šifrovanými archívy ve formátu CAR, který používá program TrustPort Archive Encryption pro PC.

Kaspersky uvádí Anti-Virus pro ISA server

Společnost Kaspersky Labs oznámila, že uvádí na trh nový antivirový program Kaspersky Anti-Virus 5.0 for Microsoft ISA Server, čímž dále rozšiřuje portfolio svých produktů pro komplexní ochranu podnikových sítí.

Kaspersky Anti-Virus 5.0 for Microsoft ISA Server monitoruje všechny soubory, které prostřednictvím protokolů HTTP a FTP procházejí přes firewall Microsoft Internet Security and Acceleration serveru. Program funguje jako filtr, který skenuje a analyzuje příchozí datový provoz a hledá v něm přítomné škodlivé kódy. Pokud nalezne infikovaný objekt, zablokuje jej přímo na vstupní bráně a nedopustí jeho proniknutí do lokální sítě.

Řešení svému uživateli nabízí široké spektrum užitečných funkcí, které jsou přístupny prostřednictvím uživatelského rozhranní plně integrovaného do ISA Microsoft Management Console. Administrátor může např. plánovat automatickou aktualizaci antivirových databází nebo je stáhnout a aplikovat manuálně. Dále může nastavovat řadu parametrů antivirového skenování a např. vytvářet skupiny uživatelů s různými požadavky na stupeň antivirové ochrany. Užitečnou funkcí zvyšující efektivnost komunikace v síti jsou seznamy „bezpečných serverů“ a uživatelských skupin, pro něž nejsou určité typy souborů antivirovým programem na ISA serveru kontrolovány.

Licencování programu Kaspersky Anti-Virus 5.0 for Microsoft ISA servery je odvislé od počtu pracovních stanic a souborových serverů, které se nacházejí v chráněné síti.

AEC
DATA SECURITY COMPANY

Kdo píše počítačové viry?

„Počítačové viry píší antivirové firmy, protože jinak by jejich programy nikdo nekupoval.“ Tvrzení, se kterým se lze setkat relativně často. Je pravdivé či nikoliv?

Především si musíme uvědomit, že nikdy nedokážeme přinést negativní důkaz. Nikdy nepřineseme důkaz, že antivirové firmy nepíší počítačové viry. V dané chvíli můžeme přinést pouze pozitivní důkaz (kdyby existoval): počítačové viry píší antivirové firmy. Dosud se jej ale nikomu nikdy předložit nepodařilo. A není pochyb o tom, že kdyby existoval, už dávno by k jeho zveřejnění došlo. Vždyť ztráty způsobené škodlivými kódy jdou celosvětově do miliard dolarů – právníci celého světa by si v takovém případě na antivirovém průmyslu smlsli s velkým gustem. Přikloňme se tedy k prvnímu tvrzení: žádný důkaz, že by antivirové firmy psaly viry dosud nebyl předložen. Dle presumpce neviny tedy musíme předpokládat, že viry nepíší.

A kdo je tedy vytváří? Programátoři, studenti, prostě obyčejní lidé z masa a kostí. Pisatele virů najdete mezi středoškolskými studenty, mezi stárnoucími pány, rekrutují ze z nejrůznějších sociálních i společenských vrstev. Není ani tak důležité, kdo je píše, ale jaké důvody jej k tomu vedou.

V drtivé většině případů jsou to důvody osobní. Může to být snaha dokázat sobě nebo světu, že „na to mám“. Může to být snaha „pomstít“ se za příkoří. Může to být snaha zakomplexovaného programátora, který chce ukázat, že „mám na víc“. Pisatelem může být zhrzený mladíček snažící se tímto způsobem dokázat své milé, že je „někdo“. Ostatně jedno staré pravidlo říká, že je mnohem snadnější bořit než stavět, ničit než budovat.

Argument, kterým se někteří pisatelé virů ohánějí a kterým se někdy pokoušejí svou činnost „zoficiálnit“ či „omlouvat“, je: Snažíme se hledat díry v systémech, snažíme se na ně upozorňovat. Proti tomuto argumentu samozřejmě nelze nic namítat, horší je to se způsobem jeho provádění. Upozorňovat na bezpečnostní chyby vytvořením počítačového viru, který poškodí data na statisících počítačů asi není tím nejvhodnějším způsobem. Je to stejné, jako kdybychom přistihli zloděje a on se bránil tím, že pouze chtěl upozornit na nedostatky zabezpečovacího systému. Ostatně: tito „hrdinové“ zpravidla ani nevystupují pod svými skutečnými jmény, ale mají zapotřebí se skrývat pod nejrůznějšími zkratkami či přezdívkami.

Ať tak či onak, počítačové viry jsou faktorem, který výrazně snižuje efektivitu práce v oblasti informačních technologií, nutí firmy investovat prostředky do zvyšování bezpečnostní úrovně apod. Jako takové jsou tedy veskrze negativní záležitostí – ať si jejich pisatelé tvrdí, co chtějí.

AEC
DATA SECURITY COMPANY