Bezpečnost

Staronové nebezpečí

Rhybaření

Dnes se budeme zabývat jednou zvláštní kategorií škodlivých programů, která v poslední době zažívá nebývalý rozmach. Jde o takzvaný phishing, česky občas překládaný jako rhybaření. Ano, autoři těchto programů vypadají trochu jako rybáři, kteří rozhazují své sítě a pak čekají, jaký úlovek se jim podaří vytáhnout.

Text: Pavel Baudiš, Alwil Software

Phishing využívá metody sociálního inženýrství a další technické prostředky k tomu, aby získal od uživatelů citlivé informace, nejčastěji hesla či detaily o kreditních kartách. Využívá k tomu maskování za důvěryhodné zdroje. Často k tomuto účelu zneužívá elektronickou poštu či programy pro instantní výměnu zpráv, ovšem není výjimkou, že pro phishing je využíván i klasický trojský kůň.

První rhybáři

První pokusy o phishing i samotný termín vznikly v polovině devadesátých let v souvislosti s krádežemi údajů k účtům a službám u AOL (America On Line). Tehdy někteří uživatelé vystupovali jako členové týmu AOL a přes instantní zprávy požadovali po jiných heslo k ověření účtu či ke kontrole zaplacení. Takto „ukradené“ účty pak byly využívány k distribuci warezu – kradených programů. V posledních několika letech se však phishing rozšířil daleko více a dnes patří k nejrozšířenějším a nejnebezpečnějším formám útoku na nic netušící uživatele. Velmi jednoduchou a účinnou metodou je zneužití elektronické pošty – uživatel obdrží zprávu, že jeho banka, ISP provider, Paypal, eBay či podobně potřebuje ověřit nějaké údaje a že má přejít na připojený webový link a tam údaje doplnit. Tato adresa však nemá se skutečnou bankou nic společného, jen její design je velmi věrohodný a vypadá podobně jako stránky skutečné banky. Když důvěřivý a nic zlého netušící uživatel vyplní citlivé údaje, získá k nim přístup útočník, který pak může dané konto bez problémů vybrat či zneužít. Kromě „falešné“ adresy mohou takové zprávy obsahovat i javaskript, který modifikuje adresu přímo v prohlížeči. Často je zneužíván i Cross Site Scripting, který pomocí chyby na originálních stránkách umožní útočníkovi získat citlivá data. Škodlivé programy na počítači mohou přímo monitorovat data zadaná uživatelem a obejít tak zabezpečené stránky, mohou jednoduše modifikovat speciální soubor hosts, který pak správnou webovou adresu převede na zcela jiné místo, a podobně.

Smrtící následky

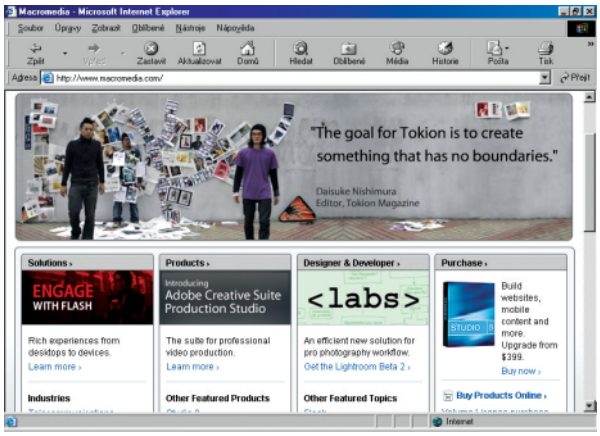
Phishing může mít velmi vážné a nepříjemné důsledky: odcizení identity může vést ke zneužití účtu, k jeho vykradení a k také tomu, že nad ním nakonec uživatel nemá žádnou kontrolu. U kreditních karet a bankovních účtů je pak důsledkem přímá finanční ztráta. Jen v prosinci 2005 bylo zaznamenáno skoro dvacet tisíc nových unikátních pokusů o phishing, přičemž vzniklo více než sedm tisíc webových stránek, které se o phishing pokoušely. Tyto stránky často vznikají na serverech bez vědomí jejich vlastníků či správců – o jednom takovém případu psala před nedávnem i Lupa.cz. Takřka 90 % pokusů o phishing se týkalo bankovních a finančních služeb, o služby ISP (Internet Service Provider) šlo v pěti procentech případů. Takřka polovina webových stránek se nacházela v USA, následovala Jižní Korea a Čína. V prosinci bylo zaznamenáno 180 nových trojských koní přímo souvisejících s phishingem.

Více než věrohodné

Během posledního roku se mění i metody, které autoři phishingu používají – zajímavý případ z poslední doby se objevil i ve Washington Post. Útok byl namířen proti uživatelům malé banky Mountain America ze Salt Lake City. Útočníci požádali a obdrželi (!) SSL certifikát pro fiktivní firmu, která se jmenovala stejně a sídlila na stejném místě jako výše uvedená banka. Na fiktivních stránkách, které ale včetně certifikátu vypadaly naprosto věrohodně, pak byla informace o skutečném bezpečnostním programu Verified by Visa a požadavek na zadání čísla kreditní karty. Vše vypadalo naprosto věrohodně a trvalo mnoho hodin, než byl certifikát zrušen a stránky odstraněny.

Snadná obrana

Jak se dá proti phishingu bránit? I když existuje řada technických prostředků, nejdůležitější zbraní je určitě vlastní mozek. Stejně jako kdysi u AOL, ani dnes neposílají banky žádosti o hesla elektronickou poštou, a pokud vám nějaká důvěryhodná zpráva přijde, nikdy nevyužívejte přímý link uvnitř takové zprávy, ale obraťte se na banku standardním způsobem, případně si vše i jinak (třeba telefonicky) ověřte. Nakupujte přes internet jen u ověřených obchodníků a vždy si dvakrát rozmyslete, než někam své citlivé údaje (včetně e-mailové adresy!) napíšete. Přeji vám, aby vás žádné phishingové trable nepotkaly a abyste těmto „rhybářům“ na jejich háčky neskočili!



Macromedia Flash Player

Oprava chyby

Adobe (Macromedia) vydalo opravu nespecifikované chyby, kterou mohl útočník pomocí zákeřně upraveného .swf souboru zneužít ke spuštění cizího kódu. Tato chyba byla identifikována a následně opravena v řadě produktů (např. Shockwave Player, Flash MX 2004...). Podrobnější informace najdete na *www.macromedia.com/devnet/security/security_zone/apsb06-03.html*.
Info: *zpravy.actinet.cz*

Zafi.D

Návrat poštovního červa

Přední účastník virového top ten za prosinec není zrovna nový: Zafi.D páše své nekalé rejdy už půldruhého roku. V prosinci 2005 na něj však připadlo celých 30 % ze všech škodlivých programů. Důvodem jeho návratu na první místo je nevyjasněné zmizení rodiny červů Doombot. Ještě v listopadu figuroval Zafi až na 18. místě.
Info: *www.kaspersky.com*

Mezera ve WMF

Bezbranná Windows

Katastrofální bezpečnostní díra v obrazovém formátu WMF názorně demonstruje, jak bezbranný je operační systém Microsoftu. Stačí si v Internet Exploreru prohlížet speciální WMF obrázek a už se instalují nežádoucí cizí programy, aniž by tomu uživatel mohl zabránit. A ohroženy jsou všechny počítače s Windows XP nebo 2000 – to je opravdová noční můra!

V čem je problém? WMF (Windows Metafile) není obyčejný pixelový formát, který jen zaznamenává barvu obrazových bodů. Namísto toho obsahuje znakové příkazy pro vektorovou grafiku – a vyvolává tedy funkce. V jedné z nich je však chyba, která dovoluje spouštění cizích programů.

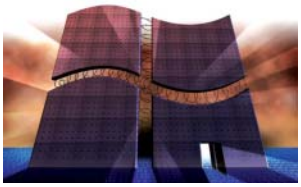
Ale ještě horší než chyba v programu je skutečnost, že v kauze WMF selhal krizový management Microsoftu. Už krátce po Vánocích totiž bezpečnostní firma Websense na jedné spywarové stránce odhalila trojského koně, který tuto mezeru využívá. O den později narostl počet takových webových stránek na více než tisíc; spyware a trojské koně se mezi surfaři šířily přímo masově.

A Microsoft? Obr se právě oddával zimnímu spánku, a tak si IT obec musela pomoci sama. Ilfak Guilfanov, vývojář na volné noze, napsal potřebnou záplatu – a jako soukromá osoba byl rychlejší než mezinárodní koncern. Poněvadž se však jeho patch nedostal k uživatelům prostřednictvím Windows Update, většina se jich o nebezpečí nedozvěděla a škůdce se nerušeně dál šířil po webu, e-mailem i komunikačními programy.

Teprve 5. ledna, déle než týden po první vlně útoků, dokázal Microsoft zveřejnit vlastní záplatu. Konkrétně to znamená, že po dlouhých deset dnů měli internetoví mafiáni na každém domácím počítači otevřeny dveře dokořán.

Avšak noční můra neskončila, neboť ve WMF byly objeveny další chyby. Naštěstí – alespoň do redakční uzávěrky – se zatím žádní škůdci neobjevili. Zbývá doufat, že Microsoft tentokrát zareaguje rychleji...

Info: *http://isc.sans.org*



WMF: Čekání na záplatu

Deset dní ponechal Microsoft uživatele Windows bez opravy nebezpečné mezery. Samozřejmě se přivalily vlny útoků.

27. 12. 2005
Bezpečnostní firma hlásí první webové stránky zneužívající chybu ve WMF.

28. 12. 2005
Počet infikovaných stránek přesahuje 1000.

31. 12. 2005
Přicházejí i útoky po e-mailu a prostřednictvím messengerů.

2. 1. 2006
Ilfak Guilfanov zveřejňuje vlastní opravu chyby.

4. 1. 2006
Microsoft bagatelizuje nebezpečí a ohlašuje patch na 10. leden.

5. 1. 2006
Na nátlak veřejnosti rozesílá Microsoft záplatu dříve.

9. 1. 2006
Ve WMF objeveny další bezpečnostní mezery.

On-line podvod

Google zneužit k phishingu

Internetoví podvodníci mají novou fintu – odkazy na své stránky implantují do URL Googlu, neboť takovým adresám uživatel více důvěřuje. Na vině je funkce vyhledávacího stroje, která jednoduše přesměrovává na jinou adresu. Tak by se surfař například přes odkaz *http://www.google.com/url?sa=t&url=http://www.podvodnik.cz* mohl ocitnout přímo na phishingové stránce. Konec odkazu *www.podvodnik.cz* se samozřejmě dá volbou znaků bez konkrétního významu zamaskovat.

Info: *www.google.com*

Chatovací nástroje

Messengery jako brána pro viry

Ti, kdo chatují, mají nebezpečný život: rozšíření červů a rootkitů drasticky narostlo – od roku 2004 na více než dvacetinásobek. Jen v posledním čtvrtletí 2005 bylo evidováno 778 případů, v prvním kvartálu jich bylo jen 59. Nejoblíbenějším cílem útoků byl MSN s 57 %, ale ani AOL s 37 % příliš nezaostal. Pouhých 6 % tak zbylo na síť Yahoo. Běžné virové skenery však už naštěstí chrání i před těmito nebezpečími.

Info: *www.facetime.com*

Datoví špioni

Co je vlastně spyware?

Dobrá zpráva: Antispywarová koalice teď ví, co to je spyware. Konsorcium firem Microsoft, Symantec, AOL a dalších vydalo dokument, který definuje jeho hranice a vyjmenovává stupně rizika. Nejvyšší riziko se například přisuzuje spywaru šířícímu se pomocí červů. Dokument má sloužit jako směrnice pro programátory.

Info: *www.antispywarecoalition.org*

ZoneAlarm

Lokální eskalace práv

Byla objevena zranitelnost v produktu ZoneAlarm ve verzi 6.x a pravděpodobně i starší, která umožní lokálnímu útočníkovi zvýšit systémová oprávnění. Proces „VSMON.exe“ (The TrueVector service) nahrává při svém spuštění několik dynamických knihoven. Pokud nějakou z nich nenajde, pokusí se prohledat předem definovaný adresní prostor. Toho může útočník zneužít a nahrát vlastní knihovnu, která pak poběží s lokálními systémovými právy. Na záplatě se pracuje.

Info: *zpravy.actinet.cz*

Internetové útoky v roce 2005

Další ohlédnutí za rokem 2005, tentokráte v podání antivirové společnosti Kaspersky Lab, najdete na *www.viruslist.com/en/analysis?pubid=180265451*. Jsou zde zpracovány statistiky nejpoužívanějších útoků, nejpoužívanějších portů a geografické rozdělení počtu útoků. Do budoucna se očekává další nárůst spamu a dále červů a botů, které budou zneužívat několik různých zranitelností.

Info: *zpravy.actinet.cz*

NOVÉ BEZPEČNOSTNÍ MEZERY

Windows

Outlook 2000, XP, 2003, Exchange Server

Stačí jedna modifikovaná zpráva a poštovní server i s jeho klienty máte ve své moci. Může za to chyba v TNEF (Transport Neutral Encapsulation Format), který se používá u mailů ve formátu RTF (Rich Text Format).

➜ Příslušné updaty už Microsoft představil při příležitosti své měsíční distribuce aktualizací.

Info: *www.microsoft.com/technet/security/bulletin/MS06-003.mspx*

Norton System Works

Chyba v designu umožňuje útočníkům ukrýt vlastní programy, tj. spouštět je skoro jako rootkit. Vězí za tím funkce pro sledování odpadkového koše. Ta využívá skrytý adresář jménem NProtect, který antivirové programy při normálním skenování nezkoumají.

➜ Symantec prostřednictvím Live-Update nahrává záplatu, která kritickou funkci vypíná.

Info: *http://securityresponse.symantec.com/avcenter/security/Content/2006.01.10.html*

Linux

SuSE 9.x, 10

Mezery v programech xpdf, kpdf, gpdf a kword umožňují hackerům útoky typu DoS.

➜ Opravené pakety si můžete stáhnout přes FTP ze serveru SuSE.

Info: *ftp://ftp.suse.com/pub/suse/i386/*

Ubuntu 5.10

Problém v tzv. bogofiltru dává útočníkům možnost napadení typu Denial of Service. „Bogofilter“ má normálně za úkol vytřídit z e-mailů spam.

➜ Ubuntu nabízí ke stažení aktualizační paket operačního systému.

Info: *http://archive.ubuntu.com/ubuntu/pool/main/b/bogofilter*

Apple

Quicktime 7.0.4

Update Quicktime na verzi 7.0.4 měl původně odstranit bezpečnostní mezeru při zacházení s obrázky. Prostřednictvím speciálního obrazového souboru ve formátu GIF, TIFF, TGA nebo QTIF mohli útočníci spouštět vlastní kód na cizích počítačích. Nyní se i záplata zdá chybná…

➜ Apple stahuje Quicktime 7.0.4, a nabízí dokonce nástroj pro jeho odstranění.

Info: *www.apple.com/support/*

Apple Mac OS X

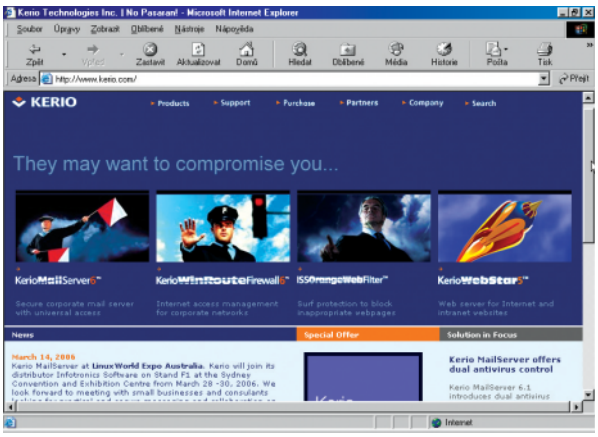
Společnost Apple vydala záplaty pro Mac OS X ve verzích 10.3.9 a 10.4.5. Celkem jsou opraveny tři bezpečnostní chyby, jde o CoreTypes, Mail a Safari.

Info: *http://docs.info.apple.com/article.html?artnum=303453*

Kancelářské aplikace

Březnové opravy pro Microsoft Office

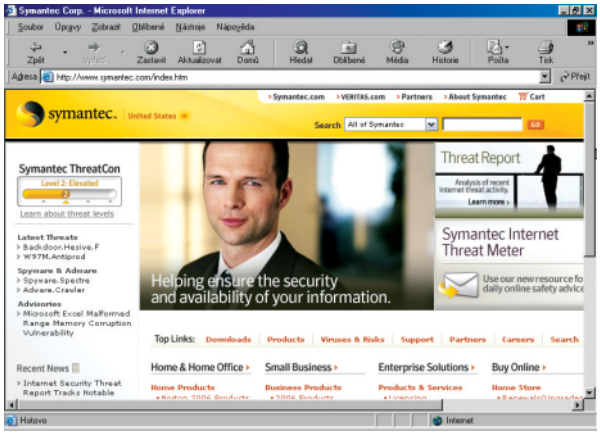
Microsoft uvolnil opravy pro Microsoft Office 2000 SP3, Office XP SP3, Office 2003 SP1 a SP2, Microsoft Works Suites 2000 až 2006 včetně, Microsoft Office X a Office 2004 pro Mac OS X. Mimo jiné jsou opraveny kritické chyby v Microsoft Excelu, které umožňovaly vzdálené spuštění cizího kódu. Další informace včetně odkazů pro jednotlivé záplaty naleznete na *www.microsoft.com/technet/security/Bulletin/MS06-012.mspx*.
Info: *zpravy.actinet.cz*



Kerio MailServer

Zranitelná pošta

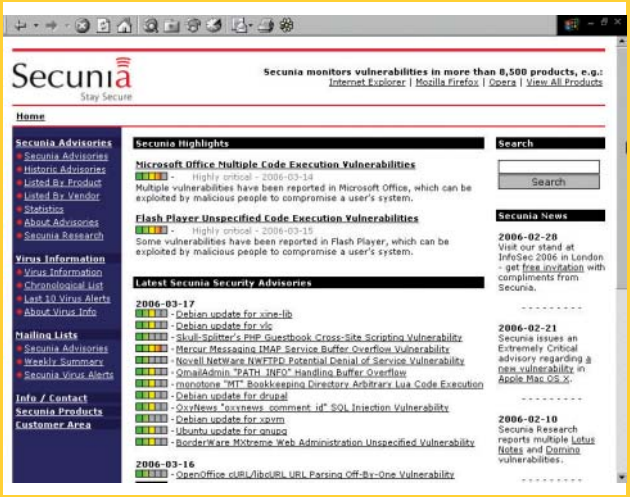
Kerio MailServer verze nižší než 6.1.3 Patch 1 obsahuje zranitelnost (viz *www.frsirt.com/english/advisories/2006/0898*), která dovolí vzdálenému útočníkovi shodit server. Chyba nastane při zpracování speciálně upraveného argumentu příkazu IMAP „LOGIN“. Opravená verze 6.1.3 Patch 1 je již k dispozici na stránkách *www.kerio.com/kms_download.html*.



Symantec Ghost

Několik zranitelností

Aplikace Symantec Ghost 8.0 a 8.2 obsahuje zranitelnosti, které umožňují lokálním uživatelům přístup k utajeným datům nebo i získat vyšší přístupová práva k aplikaci. Podrobný popis chyb naleznete v původním oznámení výrobce. Doporučuje se aktualizovat na verzi 8.3.
Info: *zpravy.actinet.cz*



WinACE

Nesprávná manipulace s ARJ archivy

Secunia Research objevila chybu ve WinACE verze 2.60 při manipulaci s příliš velkými hlavičkami v ARJ archivu, které se nevejdou do fixně velikého bufferu (viz *http://secunia.com/secunia_research/2005-67/advisory/*). Otevřením zákeřně upraveného ARJ archivu dojde k přetečení zásobníku, což umožňuje spustit libovolný kód na uživatelově počítači. Dle vyjádření Secunie bude chyba opravena v příští verzi programu. Záplata prozatím není dostupná.
Info: *zpravy.actinet.cz*

KRÁTCE

➜ Antivirus McAfee má potíže s ActiveX

U Security Center od McAfee může být na počítači spuštěn cizí kód, jestliže v záškodnické webové stránce je obsažen ActiveX. Firma už ale zveřejnila záplatu.
Info: *www.mcafee.com*

➜ RAR archivy obcházejí Norton Antivirus

Pomocí speciálních RAR archivů mohou hackeři vyvolat přetečení bufferu v programu Norton Antivirus a získat tak přístup do počítače. Až do redakční uzávěrky nebyla definitivní záplata na tuto mezeru k dispozici.
Info: *www.symantec.com*

Bezpečnostní zpráva

Windows bezpečnější než Linux?

„Cyber Security Bulletin“ amerického ministerstva národní obrany přisuzuje Linuxu téměř třikrát tolik bezpečnostních mezer než systému Windows. Konkrétně 2328 chyb v Linuxu proti 812 prohřeškům v operačním systému Microsoftu. To ovšem nic nevypovídá o tom, jak jsou nalezené chyby závažné. Podrobnou zprávu najdete na uvedené adrese.
Info: *www.us-cert.gov/cas/bulletins/SB2005.html*

2005 – rok graywaru

Výroční zpráva Trend Micro 2005 Roundup označila rok 2005 za rok graywaru – 65 % nejnebezpečnějších útoků v sobě skrývalo spyware, adware, backdoor (tzv. zadní vrátka), rootkit nebo bot.

Mírný ústup počítačových virů ve prospěch různých „graywarových hrozeb“ zaznamenalo v roce 2005 centrum WTC (World Tracking Center) společnosti Trend Micro, Inc., které monitoruje celosvětový výskyt škodlivého softwaru (malwaru), spamu a dalších ilegálních aktivit zneužívajících internet. Vyplývá to z výroční zprávy Trend Micro 2005 Roundup, zveřejněné před koncem roku 2005. Nejrozšířenějším virem za rok 2005 se stal červ WORM_NETSKY.P s více než 1 600 000 nakaženými počítači a javový applet JAVA_BYTEVER.A s více než 660 000 průniky. Šestadvacet procent všech vyhlášených poplachů se týkalo některé z variant červa WORM_MYTOB, červ WORM_SOBER měl na svědomí 16 procent poplachů.

Metody

Nejúspěšnější metodou šíření malwaru bylo minulý rok jeho umisťování na sdílené síťové disky (37 procent), následovalo zneužití slabých míst v operačních a dalších systémech (19 procent). Rozesílání kódu mailem, zneužití IRC messagingu a přímé sdílení se na šíření malwaru podílelo shodně deseti procenty. Kvůli ztíženému odhalení svých výtvorů využívali autoři malwaru v hojné míře binární packery, umožňující průběžnou změnu souborů s červy a boty a tím pádem jejich snazší šíření. S objevem botu ZOTOB je také zřejmé, že tvůrci malwaru již mají k dispozici jak technologie, tak snahu zneužívat slabá místa v operačních systémech okamžitě poté, co jsou tato slabá místa zveřejněna.

Mobily a roootkity

Spammeři začali své oběti stále častěji oslovovat i v jiných jazycích než v angličtině. Nejčastějšími tématy spamu byly nabídky hazardních her, erotických služeb a vzdělávání. Ani phishingové aktivity (zahrnované do kategorie spamu) v loňském roce nepolevovaly, i když explicitní zobrazení phishingové adresy se objevilo pouze ve 13 procentech spamů (oproti 76 % v roce 2004). V minulém roce došlo také k dalšímu rozmachu malwaru pro mobilní telefony. Objevil se první červ pro různé mobilní platformy a také první malware určený pro sbírání kontaktů uložených v mobilu a jejich zasílání na jiný mobil nacházející se ve stejné oblasti. Rok 2005 znamenal i větší rozšíření rootkitů, přičemž v jeho závěru se objevily i rootkity spojené s jinými druhy hrozeb.

Cíl: peníze

I v roce 2005 byla většina hrozeb motivována finančním prospěchem, nikoli snahou o zviditelnění nebo vychloubačstvím. Útočníkům jde stále více o krádež informací, proto se snaží útočit spíše na konkrétní organizaci nebo menší skupinu uživatelů počítačů. Speciálně vytvořené trojské koně se pomalu šíří, často zůstávají dlouhou dobu neidentifikovány a během svého působení sbírají důvěrné informace. V roce 2005 se objevil i nový druh útoku, označovaný jako spy-phishing, při němž se trojský kůň využívá pro zjištění přístupového jména a hesla na určitou webovou stránku. Stále častěji také dochází ke kombinovaným útokům, kdy spam je nositelem jak trojského koně, tak spywaru nebo adwaru, mnohdy od jiných původců. Útočník tak nejen získává potenciálně zpeněžitelné informace z infikovaného počítače, ale zároveň dostává provizi od zadavatelů adwarových reklamních kampaní. Jeden program zavedený do počítače oběti může postupně stahovat další malware a nakonec je počítač zamořen mnoha různými škodlivými kódy a využíván k různým nekalým účelům.

Zdroj: Trend Micro

Deset hlavních předpovědí pro zabezpečení v roce 2006

Gary Middleton, ředitel bezpečnostních řešení ve společnosti Dimension Data, shrnuje, co mohou v tomto roce společnosti očekávat v oblasti zabezpečení informací.

1. Očekávejte větší škody, ale méně epidemií.
Množství infekcí v roce 2006 pravděpodobně vzroste a organizace se už nemohou spoléhat na to, že se o problémech a masových útocích dozvědí z médií. Předpoklad, že žádné zprávy znamenají dobré zprávy, povede k falešnému pocitu bezpečnosti.

2. Útoky už se nebudou zaměřovat pouze na operační systém Microsoftu.
Terčem útoků se stane více aplikací a dalších prvků infrastruktury, což povede k větším nárokům na opravování chyb zabezpečení.

3. Spyware bude nadále představovat velký problém.
Organizace mohou očekávat více spywarových infekcí, což jim bude vyčerpávat přenosové pásmo, povede k nárůstu volání na technickou podporu a ve výsledku nepříznivě ovlivní produktivitu zaměstnanců. Z toho důvodu bude třeba více investovat do dalších technologií na boj proti spywaru.

4. Rychlé posílání zpráv a sítě peer-to-peer budou způsobovat ještě větší potíže.
Rychlé prosazování a používání posílání zpráv prostřednictvím messengerů a využívání aplikací P2P může vystavit organizace novým hrozbám.

5. Zabezpečení zpráv se začne brát vážně.
Před dvěma lety organizace poprvé masivně investovaly do produktů pro filtrování nevyžádaných e-mailů. Dnes se ohnisko zájmu pomalu přesouvá směrem k řešením, která kromě ochrany před viry a spamem zajišťují také šifrování.

6. Představenstva firem budou bezpečnosti věnovat větší pozornost.
V souladu s globálním trendem správných řídicích postupů budou představenstva firem věnovat větší pozornost ochraně informačního majetku organizací před rostoucím množstvím interních a externích hrozeb.

7. Zabezpečení bezdrátové komunikace získá větší pozornost.
Vzhledem k rostoucí poptávce koncových uživatelů po mobilitě potřebují organizace zajistit, aby jejich bezdrátové přístupové body byly chráněny před neoprávněným přístupem.

8. Instalace oprav začne být selektivní.
Počet oprav vydávaných pro operační systémy, aplikace a další prvky infrastruktury IT roste alarmujícím tempem. Začíná být příliš pracné a nákladné implementovat všechny opravy, a proto organizace začnou selektivně instalovat opravy na základě hodnoty příslušných prvků IT a na základě konkrétních hrozeb, jimž čelí.

9. Trend směrem k bezpečné infrastruktuře bude pokračovat.
Zabezpečení je čím dál tím častěji zabudováno přímo na vrstvě infrastruktury, takže jsme svědky konvergence správy sítě, systémů a zabezpečení. V důsledku toho budou zákazníci čím dál tím častěji hledat jediného poskytovatele, který jim dodá, bude podporovat, spravovat a zabezpečovat celou infrastrukturu.

10. Bude se klást větší důraz na zabezpečení koncových bodů.
Mnohem větší pozornost se bude věnovat tomu, jak se k síti připojují nezabezpečené koncové body, například notebooky, stolní počítače a další zařízení.

Zdroj: Dimension Data

McAfee AVERT Labs

Co vás nemine

Společnost McAfee oslavila 19. prosince 2005 desáté výročí založení McAfee AVERT Labs a dekádu sledování a ochrany před internetovými hrozbami. V souvislosti s výročím McAfee AVERT Labs také zveřejňují své předpovědi týkající se bezpečnostních rizik v roce 2006.

Během posledních deseti let zaznamenaly McAfee AVERT Labs dramatickou změnu v typech a rychlosti útoků; od disket, pomocí nichž se útoky šířily manuálním kontaktem s počítači, přes sofistikovanější techniky včetně masových e-mailů, které se dnes stále hojně vyskytují, až po útoky, které se samostatně šíří po jednotlivých sítích i na celém světě prostřednictvím internetu. Podle McAfee AVERT Labs existuje nyní na internetu přes 160 000 různých typů bezpečnostních hrozeb, spolu s dalšími tisícovkami těch, které ještě nebyly identifikovány. Během deseti let od svého založení se McAfee AVERT Labs rozrostly z malého týmu, který pracoval v sídle společnosti v kalifornské Santa Claře, v Amsterdamu, Paříži a Sydney, na celosvětový tým vědců a inženýrů ve dvaceti městech na pěti kontinentech a ve čtrnácti zemích, který funguje 24 hodin denně, sedm dní v týdnu a 365 dní v roce.

„Melissa“ a Jimmy Kuo

McAfee AVERT Labs identifikovaly dva ze světově nejznámějších útoků: útoky viru Melissa v roce 1999 a viru MyDoom v roce 2004. Jimmy Kuo, spolupracovník McAfee, nejenže virus Melissa pojmenoval, ale také se aktivně účastnil identifikace a zatčení jeho autora. Jimmy Kuo obdržel za svou účast na potlačení tohoto viru cenu Fed 100. Jimmy se spojil s exekutivou, úspěšně informoval všechny její složky o hrozbě viru a umožnil tak redukovat následné škody. Podle časopisu Computer Economics se finanční dopad viru Melissa v roce 1999 odhaduje na 1,5 miliardy amerických dolarů.

„MyDoom“ a Craig Schmugar

Tento výzkumný pracovník McAfee AVERT Labs byl odpovědný za identifikaci viru MyDoom. Červ MyDoom proslul tím, že byl nejrychleji se šířícím útokem malwaru a podle Computer Economics zasáhl na vrcholu své aktivity 12 000 systémů za hodinu. Finanční dopad viru MyDoom v roce 2004 byl odhadnut na 5,25 miliardy amerických dolarů.

Předpověď největších bezpečnostních rizik pro rok 2006

Více útoků na mobilní zařízení

Malware napadající mobilní zařízení byl poprvé zaznamenán v červnu 2004, kdy skupina profesionálních autorů virů vytvořila první pokusný virus určený k napadení smartphone telefonů – a dokázala, že lze vytvořit škodlivý kód napadající operační systémy Symbian. Během krátké doby po tomto viru byl vypuštěn „Duts“ – první virus pro kapesní PC, napadající i soubory smartphone telefonů. Od té doby se objevila řada trojských koňů určených pro mobilní zařízení, což způsobilo alarmující nárůst mobilního malwaru. McAfee AVERT Labs očekávají, že v roce 2006 dojde k podstatnému nárůstu celosvětových útoků na mobilní zařízení. Používání technologie smartphone hraje klíčovou roli v přesunu útoků z multifunkčních přenosných počítačů na kapesní zařízení. V souvislosti se stále se rozvíjející konektivitou smart telefonů očekávají McAfee AVERT Labs, že se tyto útoky rychle přesunou i na konvergovaná zařízení.

McAfee AVERT Labs očekávají, že škody napáchané těmito novými útoky na mobilní zařízení budou větší než ty způsobené dnešními útoky na PC, a to v důsledku většího množství smartphone telefonů a faktu, že jen velice málo z nich je chráněno bezpečnostními řešeními. Například v roce 2004 pronikl virus 'I Love You' desítky milionů PC v několika hodinách, a to i přesto, že na polovině z nich byl nainstalován bezpečnostní software. V porovnání s touto situací by mobilní útok zaměřený na několik operačních systémů mohl infikovat až 200 milionů smartphone telefonů ve stejný okamžik, protože většina těchto zařízení v současnosti nemá nainstalovány žádné bezpečnostní programy.

Podle McAfee AVERT Labs roste šíření mobilního malwaru při ročním porovnání desetkrát rychleji než PC malware. Zákazníci přitom instalují bezpečnostní programy do svých mobilních zařízení mnohem méně než do svých PC, protože vnímají riziko mobilních útoků jako menší. Autoři mobilního malwaru se však poučili od počítačových hackerů a autorů virů a vytvářejí sofistikované útoky, pro zákazníky téměř neodhalitelné, které jim přinášejí obrovské finanční zisky. To povede k tomu, že mobilní útoky budou mnohem vyspělejší a schopné devastovat sítě a data zákazníků bez jakéhokoli varování.

Phishing a krádež identity – vývoj nového odvětví

Phishing byl poprvé rozpoznán jako vážná hrozba v roce 2004. Původně bylo slovo phishing používáno hackery jako popis procesu krádeže uživatelských jmen a hesel k účtům America Online® (AOL). Od té doby se schopnosti kriminálních živlů využít moderních technologií značně rozvinuly. Phishing bude vážným problémem i v roce 2006, protože útoky budou stále více cílené díky použití spywarových programů a „password stealerů“. Vady v e-mailových protokolech, bezpečnostní nedostatky v internetových prohlížečích a nedostatek základního povědomí o bezpečnosti počítačů povedou k nárůstu phishingu, protože pachatelé počítačové kriminality je budou jistě využívat. McAfee AVERT Labs předpovídají nárůst výskytu distribuovaných phishing trojských koňů – ty udělají z infikovaného počítače phishing webový server a spamují ostatní uživatele s cílem přivést je na takové internetové stránky.

V roce 2006 McAfee AVERT Labs také očekávají větší množství případů krádeže hesel pomocí zjišťování přístupového jména a hesla na falešných přihlašovacích stránkách a rostoucí počet útoků na populární služby, jako například eBay. V souvislosti s phishingovými incidenty, které následovaly po hurikánu Katrina, McAfee AVERT Labs dále očekávají útoky využívající vůli lidí pomáhat druhým v nouzi. Naproti tomu počet útoků na poskytovatele internetového připojení by měl klesat, zatímco útoky proti finančním institucím se budou objevovat v nezmenšené míře.

Zdroj: McAfee Inc., *www.mcafee.com*