Scéna zločinu: Internet

Špionáž, vydírání, teror – to jsou metody organizovaného zločinu, stále běžnější dokonce i na webu. Chip vám ukáže, jak **INTERNETOVÁ MAFIE** řádí v milionech počítačů. Zároveň vám poradíme, jak můžete své PC ochránit, aby se z něj nestala zombie...

VALENTIN PLETZER

Stejná scéna jako ta z 26. února 2008 se už asi neuvidí: autor posledního viru legendární „skupiny 29A" se vzdal. Je to dostatečný důvod ke štěstí? Zcela určitě ne! Lidé od 29A si získali slávu a čest, což „odpláceli" i početnými vzorovými viry. Většina autorů malwaru dnes už ale nevěnuje moc pozornosti „Proof-of-Concepts"; ve skutečnosti je většina zákeřného kódu programována pouze s cílem zisku.

Internet je polem organizovaného zločinu už delší dobu, což potvrzují i čísla, která nedávno zveřejnila laboratoř AV na testování virů: zatímco v roce 1999 registrovala pouhých 100 000 nových škůdců, v roce 2007 už jich bylo 5,5 milionu! Navíc, před deseti lety se jednalo téměř výhradně o viry, dnes tu máme trojské koně, boty i spyware, což činí internet mnohem nebezpečnějším.

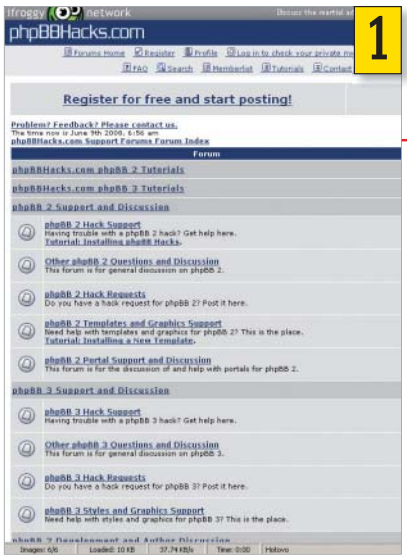
Pohledem na další studii zjistíme, proč je internetová mafie stále silnější: podle nejnovějších prognóz od firmy E-commerce a Distance Selling Trade Asosociation se obrat v on-line obchodu letos zvýšil o dalších devět procent, na 11,9 miliardy eur, a to jen v Německu! I v České republice obrat domácích internetových obchodů přesáhl 18 miliard korun! Organizovaný zločin získává peníze i z této obrovské ochoty utrácet peníze na internetu. Není tak žádným překvapením, že si mezitím některé internetové mafie zařídily vlastní providery: například Russian Business Network. Navíc stále častěji posílají své hackery na univerzity a zároveň nabízejí odměnu za neznámé bezpečnostní mezery.

Zdá se, že není žádná naděje tento vývoj zastavit, a to i proto, že mafie používá velmi dobré maskovací prostředky a odhalit ji na „rozlehlých internetových pláních" je téměř nemožné. Navíc jsou častokrát policie či jiné veřejné autority zcela bezmocné – organizovaný zločin operuje celosvětově a přitom neexistuje protiváha v podobě „internetového Interpolu".

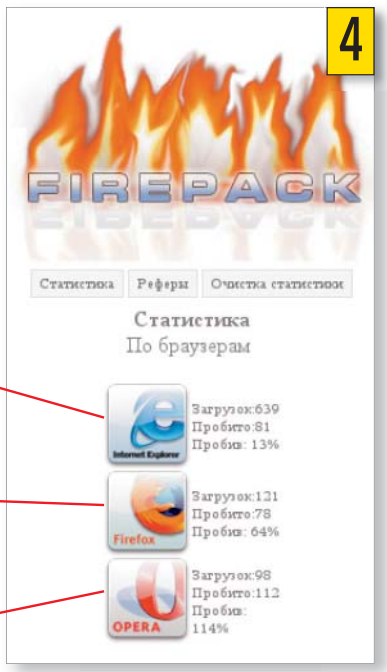
Dokonce i bezpečnostní experti výrobců bezpečnostních programů občas selžou ve svých pokusech o zastavení internetového útoku. V zemích, jako je Rusko či Čína, neexistují vůbec žádné kontaktní osoby, které by pomohly odhalit pachatele. Také oběti zůstávají skryté v obavě o svou pověst. Která společnost by přece připustila, že se stala obětí zločinu?

Každým dnem se stává nebezpečnější dokonce i pouhá běžná návštěva internetu, a to proto, že zdánlivě neškodné stránky „přejdou" k organizovanému zločinu. Příklad vám vysvětlí princip tohoto ohrožení: skupina čínských hackerů dokázala skrz mezeru v serverovém softwaru propašovat zákeřný kód asi na 20 000 webových stránek. Výsledek: uživatelé napadených stránek (například i fóra Federal Biological Research Centre) byli nasměrováni na nebezpečnou pornostránku. Hrozba samozřejmě nespočívala jen v nemravných obrázcích zobrazovaných na samotné webové stránce; problémem byl JavaScript, který (zatímco si zvědavý surfař prohlížel hanbaté obrázky) spustil na pozadí vyhledávání typických bezpečnostních mezer v aktuálních prohlížečích. Když byla například na počítač nainstalována zastaralá verze RealPlayeru, pak s pomocí zneužití její zranitelnosti byl do systému nic netušící oběti automaticky nainstalován downloader.

Downloadery (neboli stahovače) jsou malé nástroje, často využívané internetovou mafií. Jsou rychle staženy i nainstalovány,



Velice nebezpečné Přes bezpečnostní mezeru v softwaru diskusního 1 fóra může internetová mafie pašovat nebezpečné skripty 2 na zdánlivě neškodné webové stránky. Software analyzuje konfiguraci počítače oběti a aktivuje odpovídající zákeřný kód, který dodá trojan, v závislosti na prohlížeči 3. Hacker kontroluje skript pomocí softwaru Firepack 4. Úspěchy i selhání jsou nahrávány...



NAJDETE NA DVD

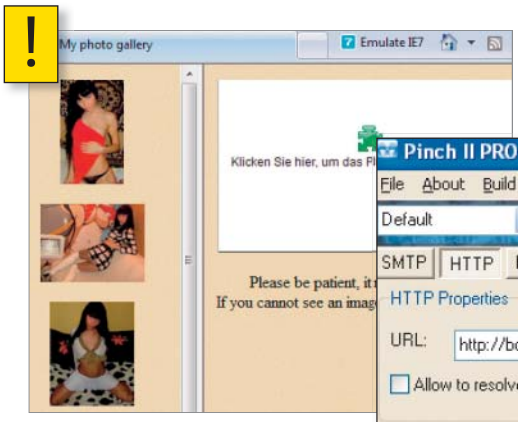
Pro bezpečný počítač

AntiVir PersonalEdition Classic ► antivirový nástroj
Spybot - Search & Destroy ► známý antimalware program
Spamihilator ► obrana před spamem
McAfee SiteAdvisor ► pro bezpečné surfování
Ad-Aware 2007 ► oblíbený antimalware nástroj
Firefox ► alternativní bezpečný browser
NoScript ► rozšíření pro blokování skriptů
Mozilla Thunderbird ► alternativní poštovní klient
Recuva ► obnova smazaných dat

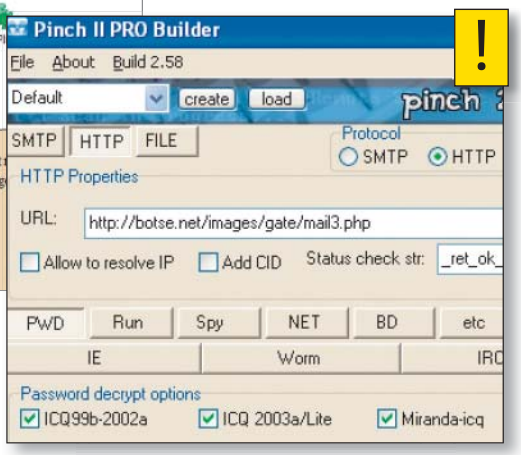
► **NA DVD:** Programy pro tento článek najdete pod DVD indexem: **ODBLOKOVÁNÍ VIRŮ**

a jakmile se stanou aktivními, jsou zárukou toho, že je počítač trvale infikován nejnovější verzí malwaru. Aby bylo zaručeno, že stahovač není identifikovatelný virovým scannerem, je soubor obvykle komprimovaný a skrytý pomocí nestandardního EXE packeru. Prostřednictvím stahovače může být infiltrované PC kontrolováno třetí osobou, a navíc existuje velká pravděpodobnost, že bude zneužito pro nekalé účely.

Stahovače „nabízejí“ malwaru ještě jednu výhodu – díky nim je signatura škůdce změněna dříve, než výrobci antivirového nástroje mohou reagovat updatem. Proaktivní ochranný mechanismus tak získává na větší důležitosti. Stahovač se používal i v námi dříve zmíněném hromadném hackingu, který proběhl v březnu tohoto roku. V tomto případě byl původcem nainstalovaný Zlob Trojan – klient celosvětově největšího botnetu (dálkově ovládaných počítačů). Internetová mafie také



Nebezpečí přes porno: Návštěva takovýchto stránek je pro malware pozvánkou do počítače...



Trojan na přání: S pomocí takovéhoto nástroje lze vytvořit záškodníka podle vašich přání...

Falešné bezpečí: Ačkoliv se to na první pohled nezdá, na tomto webu nekoupíte nástroje od firmy McAfee.

uvažovala nad problémem, co dělat v případě, že by stahovač nemohl nepozorovaně projít přes bezpečnostní mezeru. Řešení je „zajímavé": zmiňované webové pornostránky uživatelům nabízely také video, k jehož přehrání byl potřeba videokodek. Samozřejmě že údajný kodek byl jen jinou verzí stahovače...

Botnety: efektivní nástroj mafie pro špinavou práci

Mnoho lidí se domnívá, že botnety jsou jen obyčejné spamové nástroje. Ve skutečnosti jsou botnety nástrojem, který internetová mafie používá k páchání nejrůznějších „skandálních skutků". Jejich pomocí lze vydírat, šířit viry či útočit na vybrané servery. Najít všechny zombie počítače je téměř nemožné, bojovníci proti nim se zaměřují na nejzranitelnější prvek sítě botů – infrastrukturu. Zatímco dříve byl bot kontrolován z centrálního jádra, dnes je obvykle komunikace decentralizována a zašifrována. Dříve stačilo analyzovat botnet, najít master server a deaktivovat ho. Armáda zombie počítačů tak byla bez hlavy a rozprášená. V současnosti se pro botnety budují sítě typu P2P komunit. To znamená, že každý bot plní funkci serveru a klienta. Pokud se server porouchá, pak jeho funkci převezme další bot.

Aby bylo zajištěno, že nikdo nemůže botnet jednoduše převzít a nakrmit ho vlastními příkazy, je komunikace také zakódována. Příkazy akceptované botem závisí na jeho struktuře – a ta je velice flexibilní. Software moderního botu je uspořádán modulárně. Každý jednotlivý „bot klient" je vybaven určitou základní strukturou podobně jako u Firefoxu. Pokud je ke speciálnímu útoku vyžadována další funkce, pak ji botnet manažer dokáže přidat podobně jako plug-in do browseru. V jiném případě se bot může chovat jako stahovač a instaluje další škůdce: například velice známý trojan zvaný Pinch je dokonalý slídivý nástroj, který se postupně přeměnil v jakýsi standard organizovaného zločinu. Jakmile je tento trojan spuštěn, začne vytvářet seznam všech hesel a dat prohlížeče, kterých se zmocní. Tato data jsou ukládána jako zašifrovaný textový soubor a zaslána zpět k hackerovi. Hacker, obvykle subdodavatel či jen malá ryba internetové mafie, filtruje data, která by dodavatele mohla zajímat.

Zbývající informace jsou nabízeny v balících po stovkách či tisících ve fórech. Pokud projeví zájem nějaký jiný hacker, může si

Jak odrazit webové útoky: Jak ochráníte sami sebe?

Pokud vám na routeru neustále bliká dioda „znázorňující" internetové spojení a disk bezdůvodně drnčí, pak zcela jistě potřebujete zkontrolovat systém. Nebo ještě lépe: ochraňte svůj počítač dřív, než se z něj stane zombie.

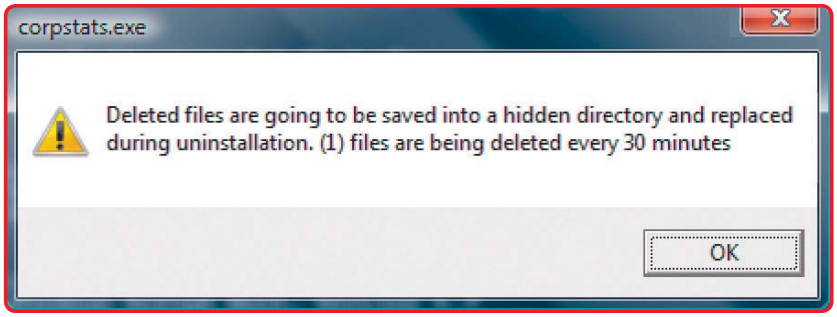
Zůstaňte na tom bezpečnějším břehu a předejděte krádeži dat. Pokud myslíte na bezpečnost až poté, co je váš počítač infikován botem či něčím podobným, mohou být vaše hesla a důležitá data pryč, dokonce aniž byste o tom věděli...

OPERAČNÍ SYSTÉM: Použijte službu automatických aktualizací. Váš operační systém by měl být vždy s nejnovějšími záplatami. Jinak vám nepomůže žádný firewall či virový scanner, protože některé útoky na systém se velmi jednoduše dokáží vypořádat s ochrannými opatřeními.

APLIKACE: Pravidelně aktualizujte i všechny své programy – společně s webovým prohlížečem a bezpečnostním softwarem –, a to především proto, že většina úspěšných útoků je založena na zranitelnosti aplikací pracujících s formáty PDF, DOC a AVI. Dobrý virový scanner a alternativa prohlížeče IE7 (Firefox, či lépe Opera) jsou bezpochyby dobrým začátkem...

ANTISPYWARE: Mnoho nástrojů zdarma nedokáže najít žádný malware, nebo (pokud ho najdou) ho nedokáže odstranit – tuto funkci obsahují jen placené verze. Proto doporučujeme jen některé z nich – například Spybot – Search & Destroy či The Avenger. Pomocí nich pravidelně svůj počítač kontrolujte.

ANTISPAM: Nežádoucí e-maily nejsou jen nepříjemností, ale mohou být také nebezpečné. Proto kompletní ochranný balík nezahrnuje jen bezpečného e-mailového klienta, ale také dobrý spamový filtr. Doporučujeme program Mozilla Thunderbird v kombinaci se Spamihilatorem. Ten druhý lze také používat s jinými klienty, protože se chová jako transparentní proxy



Vyděračský přístup: Nejprve jsou zašifrovány všechny dokumenty ve složkách na disku C, pak se objeví žádost o výkupné. A každých 30 minut bude smazán 1 soubor...

tento balík informací (nazývaný dump) koupit, zužitkovat i tento „zbytek dat". Tímto způsobem se například shromažďují sériová čísla softwaru a pak na webových stránkách prodávána společně s pirátskými kopiemi.

Obchod se strachem: Špatný software s povinností koupě

I koupi virového zabijáka lze přirovnat k ruské ruletě na internetu. To proto, že na webových stránkách lze stále častěji narazit na software, který je vytvořen internetovou mafií. Ve většině případů jde o tzv. wrong killers a spyware blockery (označované obecně jako rogue antispyware). Wrong znamená, že imituje vzhled známých produktů, ale nedrží se „jejich funkce". Zatímco většina padělatelů svým produktům dává jiná jména, v rámci našeho pátrání jsme zjistili, že existují i imitátoři značek McAfee, Panda nebo Avira. Jejich produkty jsou okopírovány do nejmenšího detailu; dokonce i doména obsahuje „část řetězce" originálu.

Kupující při instalaci rogue antispyware produktu tratí hned třikrát: zbytečně ztrácí čas s produktem, který mu nenabídne ochranu před viry, a naopak ztratí soukromí a bezpečnost svých dat. Program obvykle proslídí nejen systém, ale často také „najde zákeřný software" a pro jeho odstranění požaduje upgrade, za který je opět nutné zaplatit. Navíc je pochopitelné, že odstranění takovéhoto programu ze systému je velmi obtížné...

Soukromí uživatelé však nejsou jediným, kdo jsou takovouto ilegální činnosti postiženi. Stále častěji se cílem internetové mafie stávají i firmy. Faktem ale je, že dobře cílené útoky na firemní sítě nejsou až tak časté. Ve skutečnosti se to hackerům častokrát povede jen šťastnou náhodou. Boty a trojské koně nejprve shromažďují vše, co by mohlo být nějak zajímavé, a pak tyto dokumenty a záznamy posílají na tzv. dump site. Útočník zde tento materiál prohledá a vyjme vše, co považuje za užitečné. V případě, že získá jakákoliv citlivá data, která nemůže využít pro sebe, pak tato data prodá dál tomu, kdo nabídne nejvíce. Takto se citlivé dokumenty neustále drží ve „špatných rukou". Internetová mafie si však našla řešení i pro případ, že by pro data neexistoval žádný vhodný kupec: existuje velmi speciální trojan, který dokáže získat peníze i ze zcela neprodejných dat.

Škůdci ze série „Trojan.Ransom" dokáží zašifrovat libovolná data a znemožnit tak oběti v přístupu k nim. Ne, cílem není zničení souborů – naopak oběti musí platit za to, aby svá data získaly zpět. Cenová struktura takovéhoto vydírání se liší případ od případu: jsou známy případy, kdy útočníkům stačilo pouze 11 dolarů, ale objevily se i případy, kdy bylo požadováno 300 dolarů. V některých případech zvláštní postup zajistí, že oběť platí ihned: z balíku dat je každých 30 minut neodvolatelně smazán jeden soubor.

Verdikt: Internetovou mafii lze zastavit, ale pouze tehdy, budeme-li všichni spolupracovat

Ačkoliv se v záležitosti angažují bezpečnostní experti a bezpečnostní firmy chrlí jeden produkt za druhým, ve finále vždy padá odpovědnost na samotného uživatele. Každý z nás by měl pravidelně updatovat svůj operační systém, včas aktualizovat virové signatury a používat kvalitní firewall. Globální řešení – jakýsi „internetový Interpol" – k dispozici v dohledné budoucnosti nebude. Navíc, i kdyby došlo k vytvoření mezinárodních autorit pro trestní stíhání, byla by situace při řešení takovýchto případů poněkud problematická. Dokud nebudou problematické počítače ve všech domácnostech vyměněny za bezpečné, budou ty staré a zanedbané vždy představovat hrozbu pro ostatní uživatele – nezávisle na tom, jak pečlivě jste chráněni.

AUTOR.@CHIP.CZ

mezi vaším počítačem a e-mailovým serverem.

SÍŤOVÁ BEZPEČNOST: Experti se neustále dohadují, zda vůbec má desktopový firewall smysl či nikoliv. Všichni se nicméně shodují v jednom: z internetu by neměly být dostupné žádné služby Windows. Uživatelům XP, kteří svá PC propojili přímo s DSL linkami, tedy doporučujeme, aby odpojili Windows Services: tím deaktivujete všechny nežádoucí síťové služby. Uživatelé Windows Vista se tohoto problému vůbec bát nemusí: zde nejsou žádné služby implicitně dostupné přes internet. To samé obvykle platí pro domácí sítě, které jsou s internetem propojeny pomocí routeru...

Ve Windows Vista lze navíc zvýšit bezpečnost použitím šifrování, nebo „protected módu".

INFO

Internetový Interpol

Nutnost vytvoření instituce bojující s internetovými zločiny si začíná uvědomovat stále více lidí. Bohužel, ne dostatečně se tak děje na vládní úrovni.

Jak vyřešíte útok zahraniční sítě botů na váš portál? Jakým způsobem zabráníte masivní phishingové kampani se stopami vedoucími do zahraničí? Na tyto otázky se začíná rýsovat nadějná odpověď: na počátku dubna letošního roku byla zahájena činnost projektu CSIRT.CZ, který má prostřednictvím tzv. CSIRT týmů zvýšit schopnost efektivně řešit vzniklé bezpečnostní incidenty. Předností pracoviště CSIRT.CZ je přímá spolupráce s ostatními světovými CSIRT týmy. To umožňuje ve velmi krátké době účinně řešit nejen útoky z různých částí světa, ale i prevenci samu. CSIRT.CZ má také sloužit jako místo „poslední záchrany" v případě útoku, kdy napadená síť nedokáže kontaktovat správce sítě, jež je zdrojem útoku, nebo kdy správa dané sítě na hlášení nereaguje. Pokud je detekován útok z jiného státu, CSIRT.CZ zahájí v rámci internetové sítě okamžitou mezinárodní spolupráci, která povede k vyřešení problému. Celý program profesionálně zajišťuje sdružení CESNET, které je zodpovědné za metodiku programu, a společnost NESS Czech, která se stará o provozní stránku.

Zdá se vám to vše báječné? Možná se ptáte, kde to má háček. Hák je skrytý v pravomocích CSIRT týmů – ty jsou totiž téměř nulové (a nejinak je tomu i ve většině ostatních zemích). Optimisté mohou očekávat, že se situace zlepší po roce 2011, kdy podle zveřejněného plánu končí „pilotní provoz" a může dojít ke změně zákona...