2009: Rok supervirů

Conficker patří minulosti – pro útoky na váš počítač nyní hackeři připravují nové, mnohem nebezpečnější zbraně. Prozradíme vám, co mají v záloze, a poradíme, **JAK SE PROTI TOMU BRÁNIT**.

CLAUDIO MILLER, PETR KRATOCHVÍL

Nový malware funguje jako víceúčelové zbraně.

Na počátku tohoto roku vystrašil celou řadu uživatelů vir Conficker. Tato hrozba, šířící se prostřednictvím staré mezery ve Windows (Microsoft nabízí záplatu už téměř rok) jako lesní požár, napadla miliony uživatelů po celém světě. Již během řádění Confickeru se po internetu začal nenápadně šířit nový vir – Gumblar. Ten je podle bezpečnostních expertů mnohem nebezpečnější než Conflicker: od března do června dokázal napadnout více než sto tisíc britských webů, včetně známých „lifestyle" portálů (například **www.variety.com**).

Gumblar je extrémně nebezpečnou ukázkou nové zbraně počítačových zločinců. Trend je zřejmý: malware útočí tak, aby nepoškodil nebo nesmazal data uživatelů, a zároveň pátrá po citlivých a zpeněžitelných informacích. V hledáčku má čísla kreditních karet, přístupové údaje na weby a osobní informace. Zároveň hackeři neustále vylepšují techniky šíření virů a jejich ukrývání v počítači. Nový malware (jako například Gumblar) a jeho metody útoku naznačují ještě jeden trend: ještě nikdy nebylo surfování po internetu tak nebezpečné jako letos. My jsme pro vás na DVD připravili nástroje, které toto riziko sníží a které vám v případě napadení pomohou s obranou.

Gumblar: Dynamický kód viru

Tím, co dělá vir jménem Gumblar tak nebezpečným, je rafinovaný způsob budování svého „hnízda" na napadených stránkách: nikdy nepoužívá stejný kód znovu a mění „scénář" u každého napadeného webu. Tento dynamicky generovaný kód ztěžuje internetovým firmám detekci jednotlivých útoků.

Když uživatel navštíví napadený web, Gumblar zaútočí na prohlížeč a pomocí mezery ve flash/pdf plug-inu se pokusí proniknout do počítače. V případě úspěchu zaznamená historii surfování uživatele a na disku pátrá po přihlašovacích údajích a heslech. V Internet Exploreru navíc manipuluje s výsledky vyhledávání pomocí Googlu. Pokud uživatel klikne na některý z těchto „vyhledaných" odkazů, je přesměrován na jeden z dalších napadených webů s další dávkou malwaru. Jako „bonus" pak Gumblar vytváří zadní vrátka, prostřednictvím kterých mohou hackeři počítač připojit do sítě botů a zneužívat například k rozesílání spamu.

Obrana před Gumblarem není prozatím nijak extrémně obtížná – jeho útoku dokáže zabránit většina kvalitních bezpečnostních balíků. Podstatně nepříjemnější je jeho odstranění z infikovaného počítače. V době vzniku tohoto článku byla známa pouze jediná, radikální metoda – naformátování disku a reinstalace Windows.

Plug-iny v browserech: Brány do počítače

Rozšíření a plug-iny se dnes využívají na většině webů – přehrávají filmy a hudbu, nabízejí animace, zobrazují dokumenty, a dokonce i spouští aplikace. Jejich deaktivace je tak pro většinu uživatelů téměř nemožná. Zdá se tedy, že jedinou cestou je mít všechny tyto „doplňky" v nejnovějších verzích...

K podobné situaci již v minulosti došlo – před několika lety byly nejčastějším cílem hackerů ActiveX komponenty, které podporoval tehdy jednoznačně dominantní Internet Explorer. V operačních systémech před Windows Vista nabízí ActiveX rozsáhlá přístupová práva k systému, a tak hackerům usnadňuje čtení dat, nebo dokonce samotné ovládnutí systému. Kvůli vylepšenému řízení uživatelských práv ve Vistě a rostoucí popularitě alternativních prohlížečů (například Firefoxu a Google Chrome) si hackeři začali všímat i těchto aplikací. Po určité době však kyberzločinci zjistili, že nejsnáze zneužitelnou slabinou budou doplňky rozšiřující schopnosti prohlížečů. Právě proto dnes malware do počítačů proniká pomocí komponent pro Javu, QuickTime, PDF rozšíření a Flash plug-inů.

FTP server: Nové metody šíření

Aby hackeři zajistili co nejlepší šíření malwaru mezi uživatele, obvykle používají jako „základny" známé a často navštěvované weby. Tyto weby ale mívají poměrně kvalitní ochranu, která rychle zasáhne a ukončí šíření malwaru. Tvůrci Gumblaru našli jinou cestu, jak škůdce rychle rozšířit mezi maximální počet uživatelů. Pokud je vir umístěn na počítači obsahujícím přístupová data na FTP server, infikuje škůdce všechny webové stránky připojující se k serveru. V hledáčku škůdců jsou především stránky nabízející velké objemy dat – například stránky výzkumných ústavů nebo „stahovacích" portálů, které často na FTP serverech ukládají data.

Triky s FTP však používají i jiní hackeři. V červnu tohoto roku hackeři infikovali pomocí ukradených přístupových údajů k FTP serverům více než 40 tisíc stránek. Pokud uživatel otevře jednu z těchto stránek a spustí se škodlivý „javascript", je uživatel automaticky přesměrován na falešné stránky Google Analytics. Tam už proběhne známý proces: prostřednictví mezer v prohlížeči a jeho doplňcích je do počítače nahrán příslušný malware...

NA DVD

AVG 8.5 CHIP EDITION

Plná verze
Na Chip DVD najdete i plnou verze bezpečnostního balíku od AVG, která nabízí komplexní zabezpečení počítače před škodlivým softwarem a útoky z internetu. Více informací o programu a zabezpečení počítače najdete na Chip DVD.

INFO

Pět nejaktivnějších virových hrozeb

1. STUH
Trojský kůň z rodiny Stuh nahrává stisky klávesnice a pátrá po heslech. Zároveň vypíná systém automatického nahrávání oprav (Windows Update), čímž připravuje cestu pro pozdější útoky.

2. FRAUDLOAD
Tento typ virů je také označován jako falešné antiviry (Rogue AV). Pomocí bezpečnostních mezer proniknou tyto viry do počítače, začnou uživatele zahlcovat hlášeními o nalezených virech a snaží se ho donutit ke koupi „bezpečnostního produktu", během které zneužijí informace o použité kreditní kartě.

3. MONDER
Také Monder patří do rodiny „falešných antivirů". Navíc ale „upravuje" bezpečnostní nastavení operačního systému a do počítače nahrává další malware.

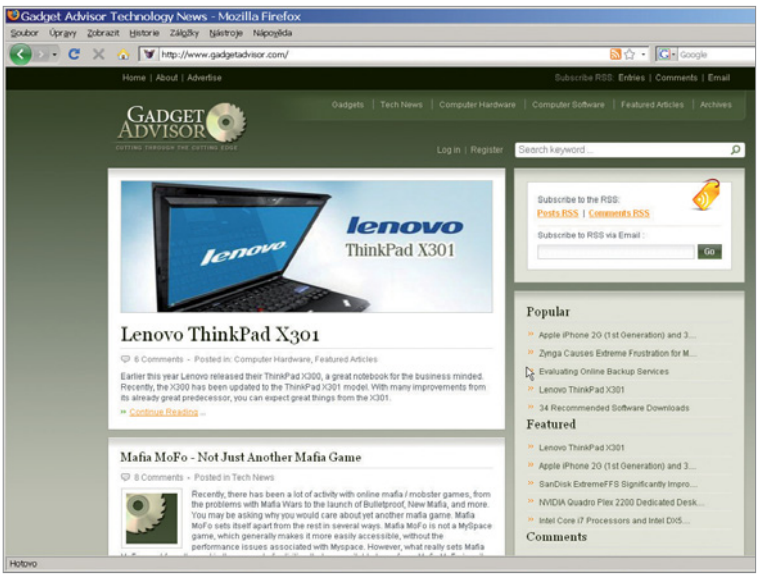
4. AUTORUN
Tato virová hrozba se vždy šíří stejným způsobem: škůdce při vložení/připojení externích datových nosičů zneužije funkci autostart a spustí exe soubor s malwarem.

5. BUZUS
Škůdce jménem Buzus patří mezi klasický spyware. Prohledává napadený počítač a pátrá po číslech kreditních karet a přístupových datech k bankovním účtům. Nepohrdne ani přístupovými údaji k e-mailovým kontům a FTP serverům.

ZDROJ: G DATA

V minulosti platilo pravidlo, že pokud nesurfujete po pornografických a nebezpečných stránkách, útoků virů se bát nemusíte. Dnes ale moderní malware nestaví svá „hnízda" jen na pochybných stránkách. Odhaduje se, že v současnosti se 85 procent malwaru šíří přes populární a na první pohled bezpečné weby. Typickou ukázkou je napadení známého amerického „tech-

nologického“ webu „Gadget Advisor“, který se ve spárech internetové mafie ocitl letos v květnu. Tato taktika přináší hackerům celou řadu výhod: těmto populárním webům uživatelé obvykle důvěřují a stahují z nich cokoliv bez větších obav. U webu Gadget Advisor byla použita zranitelnost při zpracování PDF **(www.f-secure.com/vulnerabilities/SA29773)** a pomocí škodlivého kódu v „iframe“ se do počítače dostal malware (Trojan-Downloader.Win32.Agent.brxr), který nakazil obrovské množství počítačů...



V utajení: Malware na vás může zaútočit i ze zdánlivě bezpečného webu. Útokům hackerů neodolal ani populární portál Gadget Advisor.

BlackHat-SEO: Zneužití Googlu

K přilákání co největšího počtu uživatelů však počítačoví zločinci používají i další triky. Pomocí analytických nástrojů Googlu najdou nejvíce vyhledávané pojmy a vytvoří weby, které budou přesně odpovídat těmto pojmům. Ty také dokáží prosadit do čela vyhledaných výsledků. Tato forma optimalizace pro vyhledávače (Search optimization – SEO) je také označována jako Blackhat SEO a funguje následujícím způsobem: hackeři zvolí nejpopulárnější pojmy, jako například „YouTube“ nebo „TV on-line“, případně aktuální témata (zřícení letadla AirFrance, herní veletrh E3). Na takové téma pak vytvoří speciálně upravené stránky, které umístí na servery freewebhostingových firem. Tyto stránky ale nejsou zavirované – pouze obsahují skript, který vás přesměruje na jiné weby, které se pokusí na počítač oběti nainstalovat malware. Pokud nemáte kvalitní softwarovou ochranu, během chvíle se váš počítač hemží malwarem...

Sociální sítě: Cíl hackerů

Kromě odkazů „vyhledaných“ Googlem existuje celá řada jiných metod využívaných hackery k lákání uživatelů na nakažené weby. Oblíbeným trikem je šíření odkazů ve velkých sociálních sítích – například ve Facebooku, který má přibližně 200 milionů registrovaných uživatelů. Hackeři používají specializované nástroje, kterými automaticky zakládají uživatelské profily. Tyto nástroje také dokáží detekovat a překonat ochrany typu „captcha“. Falešné profily jsou poté použity k odesílání zpráv ostatním uživatelům. Tyto zprávy obsahují odkazy na weby, ze kterých uživatelé mohou „získat“ malware, aniž by na cokoliv klikli. Stejný trik používají hackeři pro microblogovací službu Twitter.

I zde jsou pro šíření odkazů na infikované stránky vytvářeny falešné profily. S cílem odlišit se od běžných zpráv (Tweets) zde ale hackeři využívají aktuální nejpopulárnější výrazy (Hashtags).

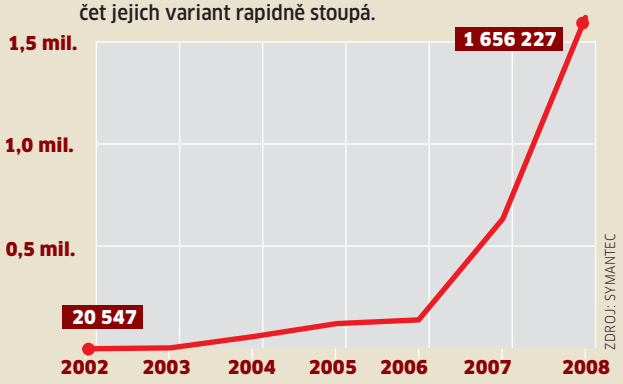
Vzhledem k limitu 140 znaků na jednu zprávu musí hackeři často zkracovat a „šifrovat“ dlouhé odkazy pomocí služeb, jako je například TinyURL – tak skrývají odkazy na zavirované weby. Ukázkou této zákeřné metody v praxi byla série útoků z konce května letošního roku, kdy Twitter zavalila lavina zpráv s odkazy na weby s videem. Po jejich navštívení byli uživatelé vyzváni k nainstalování „videokodeku“ pro korektní zobrazení filmů. Místo kodeku se ale na disk uživatele stáhl PrivacyCenter, známý falešný antivirový nástroj (označovaný jako Rouge AV). Po nainstalování začal program předstírat kontrolu systému a varovat před „nalezenými“ viry.

Po neúspěšném „pokusu“ o odstranění virů přesměroval nástroj PrivacyCenter vyděšeného uživatele na WWW stránku, kde si mohl zakoupit „plnou verzi“ bezpečnostního nástroje, která si s viry určitě poradí. Co se dělo s účtem, ke kterému neznalý uživatel při nákupu fiktivního bezpečnostního nástroje prozradil informace o kreditní kartě, si jistě dokáže čtenář Chipu představit...

Uživatelé Facebooku se také mohli setkat s několika nepříjemnými viry v neuvěřitelném počtu variací. Například červ Boface, který se objevil na počátku roku 2008, zaútočil na uživatele hned v 56 různých variantách. Zajímavé je, že tento škůdce je nebezpečný pouze pro uživatele Facebooku – na počítači se stává aktivním teprve poté, co se

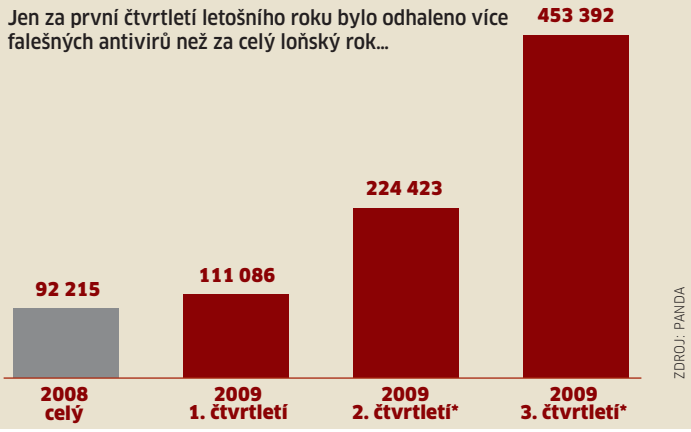
POČET NOVĚ DETEKOVANÉHO MALWARU

Od té doby, co se viry dokáží samy modifikovat, počet jejich variant rapidně stoupá.



TREND: FALEŠNÉ ANTIVIRY

Jen za první čtvrtletí letošního roku bylo odhaleno více falešných antivirů než za celý loňský rok...



*odhad

Hnízdo virů: Hackeři stále častěji využívají pro distribuci svých „nástrojů“ také služby pro úschovu souborů.

přihlásíte ke svému účtu na této komunitní síti. Pak začne všem kontaktům uživatele rozesílat krátké e-maily obsahující odkaz na „zajímavé videostránky“. Tyto stránky také obsahují vir Boface a jako bonus přidávají „falešný antivir“. Ten je na napadený počítač nainstalován a okamžitě začne bombardovat uživatele falešnými virovými varováními. Opět je cílem získat údaje o kreditní kartě, a to poté, co se uživatel rozhodne zakoupit „plnou verzi“ bezpečnostního nástroje. Odhaduje se, že škůdce s označením Boface napadl již téměř dva miliony uživatelů, a jejich počet se neustále zvyšuje.

PDF: Vnímavý Office formát

Za největší hrozbu současnosti považují experti falešné antivirové programy, které mají za cíl zjistit informace o vašem kontu a číslech kreditních karet, případně „zkontrolovat“ váš počítač na přítomnost citlivých dat. Odhaduje se, že počet „falešných AV programů“ za čtvrtletí se ještě v tomto roce zdvojnásobí (viz graf dole). Dalším nepříjemným trendem je nárůst útoků za použití zmanipulovaných PDF souborů. Až doposud byly považovány za nejoblíbenější cíl hackerů formáty kancelářských programů od Microsoftu. V současnosti je však překvapivě polovina všech napadených dokumentů ve formátu PDF.

V tomto trendu hrají roli tři důležité faktory. Především hackeři často identifikovali bezpečnostní mezery v programech Adobe (například Acrobat a Reader), které jim umožňovaly převzít kontrolu nad systémem a infiltrovat do počítače další malware. Pro ilustraci stačí uvést odkaz na statistiku serveru Secunia pro produkty Adobe Acrobat 8.x a 9.x – se 40 a 22 zranitelnostmi **(http://secunia.com/advisories/product/12256/)**.

Druhým faktorem je skutečnost, že dokumenty ve formátu PDF mohou být zmanipulovány relativně snadno, např. implementací zákeřného JavaScriptu.

Posledním faktorem je podceňování tohoto problému uživateli – mnoho uživatelů nemá o těchto hrozbách ani tušení, a tudíž si ani bezpečnostní aktualizace těchto programů nestahují.

Základním krokem k bezpečnějšímu surfování tedy může být i pravidelná aktualizace produktů pro zobrazení souborů PDF a zakázání JavaScriptu. Například v Adobe Readeru/Acrobatu toho dosáhnete pomocí odstranění zatržítka v nabídce »Úpravy | Předvolby | Všeobecné | JavaScript«.

Sdílení souborů: Obvyklý zdroj virů

Infikované PDF soubory se šíří dvěma cestami: přes webové stránky, které přímo nahrají PDF do okna prohlížeče, případně přes přílohy e-mailů. Protože PDF je jedním z obvyklých formátů pro dokumenty na webu a má (stále ještě) dobrou pověst, nevěří těmto souborům pouze zlomek uživatelů, a jen málokdo tedy očekává v přílohách ve formátu PDF zákeřný malware.

Jiné formáty souborů, které slouží jako nositelé virů, preferují cestu šíření pomocí služeb sdílení souborů a služeb pro „úschovu“ souborů (typickým příkladem je služba Rapidshare). Podle Symantecu byly v roce 2008 rozšířeny pomocí „sdílení souborů“ přibližně dvě třetiny virem infikovaných EXE souborů. Již zmiňované „úschovny“ jako RapidShare nebo MediaFire jsou také stále častěji cílem útoků kyberzločinců. Stále oblíbenější taktikou je rozšíření odkazů na stažení souborů pomocí diskusních fór a sociálních sítí. Do karet hackerům hraje i fakt, že většina podobných serverů není na „černém seznamu“ nebezpečných stránek, a nezanedbatelnou výhodou je i naprostá anonymita...

Všechny tyto nové metody mají jedno společné – jsou mnohem efektivnější než šíření nebezpečných linků přes spamové e-maily. Ve chvíli, kdy tempo růstu spamu a phishingových mailů v elektronických schránkách klesá, měli by se uživatelé připravit na nové taktiky kyberzločinců. Jejich útoky totiž budou stále efektivnější a nebezpečnější... AUTOR@CHIP.CZ

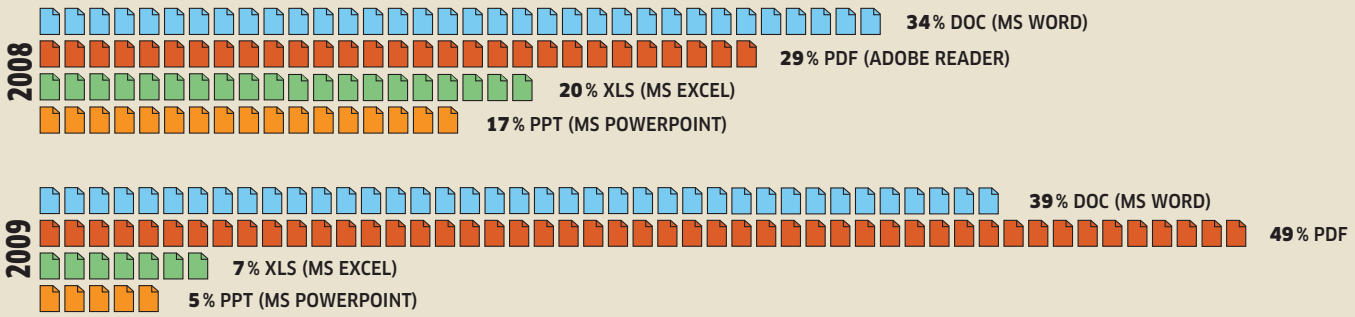
INFO

Útoky pomocí USB disků

Zpátky ke kořenům – to je nejnovější heslo hackerů při šíření malwaru. V dobách před masovým rozvojem internetu byly hlavním médiem pro šíření virů diskety. V současnosti se tato taktika znovu začíná využívat, a to na základě obrovského nárůstu popularity přenosných datových médií – USB flash disků nebo datových karet (např. SD). Tímto způsobem se vir šíří od počítače k počítači. Ochrana je však relativně snadná: kvalitní antivirový nástroj, nebo alespoň deaktivace funkce autostart...

ÚTOKY NA KANCELÁŘSKÉ DOKUMENTY

V roce 2008 se hackeři zaměřili na formáty Microsoftu a šířili viry pomocí typů souborů z kancelářského balíku MS Office. Letos trend ukazuje větší počet upravených PDF souborů...



ZDROJ: F-SECURE