

Nové směry v odhalování malwaru

DAVID KUTÁLEK

Rozvoj aplikací pracujících na principech Webu 2.0 (Facebook apod.) vytváří prostředí pro rychlé šíření škodlivých kódů na počítače nic netušících uživatelů. Malware využívá pestré palety zranitelností a neustále mění svoji podobu. Stále častěji jsou přitom prvním zdrojem nákazy legitimní webové servery. Web tak uživatelům poskytuje nekonečné množství informací, zábavy, vzdělávání, ale ještě více nových útoků.

Epidemie v sociálních sítích

K širšímu zneužití aplikací Web 2.0 pro šíření malwaru došlo počátkem srpna roku 2008. Zajímavým a zároveň nebezpečným je způsob, jakým byly aplikace Web 2.0 zneužity k šíření malwaru. Útočníci pro šíření svého červa využili servery MySpace a Facebook. Pro lepší pochopení útoku lze uvést konkrétní příklady.

Napadený počítač v případě, že jeho majitel je aktivním uživatelem řešení MySpace či Facebook, rozešle zprávy typu „To musíte vidět!!! Super video klipy.“ všem „přátelům“ v kontaktním listu uživatele. Cílem zpráv je nalákat oběť ke zhlédnutí videa a při této příležitosti jí infikovat počítač.

Když se oběť nechá nalákat (přeci jen zpráva přišla od známé osoby a pravděpodobně sama v minulosti již zaslala zprávu s obdobným obsahem), je přeměrována na falešné stránky vydávající se za YouTube, kde je informována, že používá zastaralou verzi Flash Playeru a je jí nabídnuta ke stažení aktualizace. Ve skutečnosti tato aktualizace respektive soubor nesoucí název „codcsetup.exe“ je červem, kterého si uživatel nevědomky nainstaluje do svého počítače.

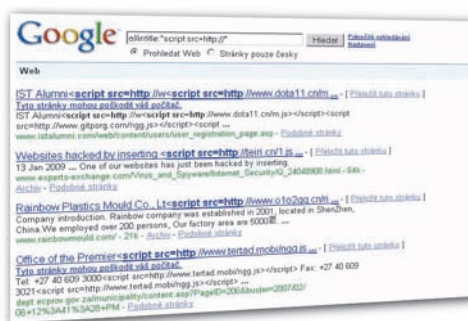
Ten okamžitě po nainstalování rozešle obdobné zprávy všem „přátelům“ v kontaktním listu uživatele a vše se opakuje a nákaza se šíří dál. Uvedený červ je znám třeba pod označením Trojan.Downloader.Gen nebo W32/Koobface.worm.

Nákaza přes jakoukoliv stránku

Další aktuální hrozbou ještě masovějšího charakteru je SQL Injection. Počínaje dubnem 2008 došlo k dramatickému nárůstu útoků využívajících právě tuto metodu, během pár týdnů dosáhl počet napadených webů více než 800 000 – každý se může pouhým zadáním do vyhledávače Google pře-

vědět, jak aktuální číslo vypadá (zadejte heslo „allintitle: script src=http“ a přesvědčte se, kam jsou v naprosté většině případů přeměrovávány renomované webové stránky).

Převážná část těchto útoků směřovala proti platformám ASP (Active Server Pages) nebo ASP.Net (nástupce ASP), které nedostatečně ověřují přístup uživatelů. Zákeřnost útoku SQL Injection spočívá v napadení nechráněných či nedostatečně chráněných, ale renomovaných web serverů po celém světě a ve schopnosti následně prostřednic-



Příklad hledání stránek odkazujících na malware.

tivím těchto serverů infikovat počítače obyčejných návštěvníků. Například téměř 240 tisíc webových stránek takto distribuuje exploity pro zneužití zranitelnosti ve Flash Playeru, která úplně otevírá vrátka k počítači nebo do sítě uživatele.

Přitažlivost útoků stoupá

Útok na koncové počítače přes mnohdy důvěryhodné webové servery je pro útočníky v současné době velmi atraktivní. Možnosti přímého útoku jsou totiž omezené využíváním překladu adres (NAT) a nasazováním firewallů. Ty jsou zpravidla nastaveny velmi restriktivně směrem dovnitř, ale mnohem benevolentněji směrem ven. Pro útočníky je tudíž snazší nechat iniciativu na uživateli a způsobit, aby si nákazu donesl domů sám: z oblíbeného blogu, diskusního fóra nebo z webu místní jídelny. Balíčky nástrojů pro zneužití zranitelností si útočník může už i koupit na černém trhu.

Proaktivní kontrola

Závažnost ohrožení malwarem vychází hlavně z faktu, že se jedná o cílené a dynamické útoky, které nebudou odhaleny pomocí klasických aktualizací signatur antivirových programů. Vývoj nových metod de-

tekce malwaru tak jde nyní především dvěma směry: cestou proaktivního skenování a globálních reputačních systémů.

Chce-li uživatel proaktivně eliminovat zákeřné aktivní kódy již na vstupu do své sítě, musí je analyzovat v reálném čase a stanovit jejich předpokládané chování. Na webové bráně není prostor ani čas kódy spouštět a sledovat jejich projevy, proto se využívá heuristická analýza kódu. Zkoumají se jednotlivé instrukce a jejich kontext (tzv. rule-based heuristika) a posuzuje se i rizikovitost takto zjištěného chování (weight-based heuristika). Pomocí těchto metod je možné odhalit a blokovat i nový malware bez existujících signatur.

Globální reputační systém je potom logickým doplňkem a přináší prvek kolektivního povědomí o důvěryhodnosti jednotlivých webových serverů. Jakmile se ze serveru začne šířit nákaza a člen systému (typicky webová bezpečnostní brána) ji odhalí, zhorší serveru reputaci a upozorní tak na problém ostatní brány. Jakmile je server od nákazy vyčištěn, reputace se postupně sama zlepšuje. Tím se reputační systém liší od blacklistů, které je zpravidla nutné ručně promazávat.

Šifrovaný provoz

Stále častěji bývají napadení šířena i v šifrovaném https (SSL) provozu, který tradiční ochranné mechanismy neumějí zkontrolovat. Zde vzniká skutečné slepé místo organizace, kudy můžou bezstarostně do sítě pronikat škodlivé kódy. Jelikož si většinou nelze dovolit https zcela zakázat, je potřeba jej na bráně dočasně dešifrovat a podrobit kontrole.

Dostupná řešení

Na trhu našťastí dnes existují nástroje připravené předcházet těmto napadením sítě. Vybrat si zájemce může komplexní webovou bránu s integrovanou bezpečností nebo třeba dodatečnou bezpečnostní gateway pro doplnění stávajícího řešení. Oba typy bran zpravidla obsahují srovnatelné funkcionality, liší se ale především způsobem nasazení a kvalitou detekce. Zástupcem prvně jmenované je například Secure Web od McAfee, zatímco u druhé může být představitelem ProxyAV od společnosti Blue Coat.

Autor je konzultantem společnosti Comguard.