

# Nové hrozby malwaru!

Karim Ibrah



Červi se šíří skrz aplikace Web 2.0., rok SQL injection útoků na legitimní webové stránky, napadení RSS kanálů, multimedia malware, trojani útočí na routery, MacOS X v zorném úhlu... To jsou jen některá z hesel provázejících aktuální varování. Internet dnes poskytuje nekonečné množství informací, zábavy a vzdělávání, ale také nové způsoby, které hackeři snadno využívají díky zastaralým bezpečnostním technologiím.

## V jednoduchosti je síla

K širšímu zneužití aplikací Web 2.0 pro šíření malwaru došlo počátkem srpna. Zajímavý a zároveň nebezpečný je způsob, jakým byly aplikace Web 2.0 zneužity k šíření malwaru. Útočníci pro šíření svého červa využili servery MySpace a Facebook, jejichž koncepce je založena na fenoménu Web 2.0. Pro lepší pochopení útoku uvádíme konkrétní příklady. Napadený počítač v případě, že je jeho majitel aktivním uživatelem 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 ji infikovat počítač. Když se oběť nechá nalákat (přece jen zpráva přišla od známé osoby, která pravděpodobně v minulosti již zaslala zprávu s obdobným obsahem), je přesměrována

na falešné stránky tentokrát populárního 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 codecsetup.exe je červ, který 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 náказa se šíří dál.

Nebezpečnost a zároveň genialita tohoto červa spočívala v jeho ochraně proti odhalení. Průběžně se spojuje se serverem v České republice a pomocí HTTP POST requestů může dojít ke změně rozepisovaných zpráv, komentářů či linků. Pro úplnost uvádím označení, který uvedený červ obdržel od společnosti Secure Computing (Trojan.Downloader.Gen) a od společnosti McAfee (W32/Koobface.worm).

## SQL injection – náказa přes jakoukoliv stránku!

Další hrozbou, snad ještě masovějšího charakteru, která má co do činění s Web 2.0, je určitě SQL injection. Počínaje dubnem došlo k dramatickému nárůstu útoků využívajících právě tuto metodu, během pár týdnů dosáhl počet napadených webů více než osm set tisíc a každý z nás se může pouhým zadáním do vyhledávače Google přesvědčit, jak aktuální číslo vypadá (vepište najít „allintitle: script src=http“ a užasnete, kam jsou v naprosté většině případů přesměrovávány 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 špatně chráněných, ale renomovaných webových serverů po celém světě a schopnosti následně prostřednictvím těchto serverů infikovat počítače obyčejných návštěvníků. Například téměř 240 tisíc webových stránek pak takto distribuuje exploity pro zneužití zranitelností ve Flash Playeru, které zcela otevírají vrátka k vašemu počítači nebo do vaší sítě.



## Multimedia malware

Teprve v červenci tohoto roku se začal šířit nový trojan napadající multimediální soubory uložené na pevných discích obětí. Malware vloží nežádoucí příkaz do multimediálních souborů, ty se pak často stávají předmětem sdílení v peer-to-peer sítích a sami uživatelé se postarají o šíření zákeřného kódu. Soubory lze snadno přehrát ve Windows Media Playeru, ale zároveň WMP otevírá browser uživatele a zobrazuje zákeřný obsah stránek hackerů například s informací, že uživateli chybí potřebný kodek pro přehrávání a může být ze stránek snadno získán. Místo něj se natáhne trojan pro krádež hesel.

## Ani routery nejsou chráněny

Nová varianta trojanu DNSChanger se začala šířit v červnu. Provede „bruteforce attack“ na většinou základní autentizaci do webového rozhraní

(GUI) routeru. Následný cíl trojanu je získat přístup k nastavení routerů a změnit nastavení DNS k nasměrování na adresy podvržené útočníky. Devastující efekt takto snadného útoku je v tom, že následně jsou veškeré DNS dotazy z podnikové sítě jdoucí přes napadený router pod kontrolou hackerů, a tak i uživatelé, jejichž počítač není napaden, mohou obdržet injektovaný nežádoucí obsah, zatímco navštěvují své oblíbené stránky.

### Klíčové komponenty webové bezpečnostní brány:

- Podpora hloubkové inspekce webového provozu, aktivních kódů a skriptů v rámci HTTP i HTTPS.
- Web cache provázaná s bezpečností. Stále žádaná funkcionality webové cache musí být připravena pro prostředí dynamicky generovaného obsahu webu a doplněna o metody kontroly uloženého obsahu při aktualizaci signatur malwaru a virů, aniž by byl přitom snížen výkon či znovu načítána celá cache.
- Anti-malware modul pro detekci škodlivých aktivních kódů na základě chování, doplněný o tradiční aktualizace signatur virů a spywaru.
- SSL scanner, který umožňuje kontrolování šifrované komunikace uživatelů se zdroji na internetu. Jen tak lze zabránit průniku hackerů, virů a dalšího škodlivého obsahu skrytého v SSL (HTTPS) provozu a ve spojení s DLP modulem zabraňuje i úniku citlivých informací přes tento šifrovaný provoz.
- URL filtrace. Automatizovaná URL filtrace umožňuje řízení přístupu zaměstnanců ke zdrojům internetu a zajišťuje tak vyšší produktivitu i menší čerpání internetového pásma.
- Systém globálních reputací.

### Řešením je kontrola aktivních kódů webového obsahu

Nebezpečnost ohrožení malwarem vychází hlavně z faktu, že se jedná o cílené útoky, které nebudou odhaleny pomocí klasických aktualizací signatur antivirových programů. Navíc stále častěji bývají napadení šířena v šifrovaném HTTPS (SSL) provozu, který tradiční ochranné mechanismy neumějí zkontrolovat. Zde vzniká skutečně slepé místo organizace před tradičními hrozbami virů a spywaru, novými hrozbami malwaru a skrytý šifrovaný provoz rovněž nahrává úniku citlivých informací z organizace, jak chtěnému, tak i nechtěnému.

Na trhu existují nástroje připravené předcházet těmto napadením našich sítí. Dovolil bych si pro ilustraci možnosti zmínit jedno z nejucelnějších řešení, a to Webwasher od společnosti Secure Computing. Toto zařízení využívá již dnes mnoho bankovních domů, úřadů i podniků právě proto, že přináší komplexní řešení proti hrozbám přicházejícím jak z internetu, tak z vnitřní sítě společnosti. Kombinuje webovou proxy, URL filtraci a cache s bezpečnostními mechanismy, především HTTPS proxy, která umožní SSL provoz dešifrovat, zkontrolovat a opět zašifrovat, a anti-malwarové ochrany založené na využívání proaktivní ochrany s klasifikací potenciální činnosti aktivních kódů na cílové aplikaci. Důležitý je i systém globální inteligence TrustedSource.org přidávající reputace.

karim.ifrah@comguard.cz

Autor je konzultantem společnosti COMGUARD a. s. Bylo využito zdrojů publikovaných laboratořemi Secure Computing.

inzerce

# Chcete si připadat SKUTEČNĚ ZABEZPEČENI?

## Poříd'te si...

# secure

computing®

## Webwasher®

Web Gateway Security

» Již od 35 000 Kč

### » Secure Web 2.0

Ochrání Vás před hrozbami webového provozu v prostředí Web 2.0 a zneužívání Internetu zaměstnanci.

» Komplexní řešení: SecureWeb Cache, URL Filtrace SmartFilter, AntiMalware, kontrola SSL a Antispam.

Unikátní sada ochrany s napojením na TrustedSource.org

» Gartner Magic kvadrant leader.

## SecureCache™

Webwasher Gateway

» Zdarma

» Revoluční technologie šetří až 50 % konektivity i v dnešním dynamickém prostředí WEB 2.0 a podrobuje „skladované“ objekty proaktivní kontrole a testům reputace.

» Nativní provázanost s ostatními moduly Webwasher.

## IronMail®

Messaging Gateway Security

» Promo

» Přesná a efektivní detekce spamu a virů.

» Nejkomplexnější řešení s ochranou proti úniku dat, IPS pro mail servery a web mail, šifrování, uživatelské účty, LDAP.

» Gartner Magic kvadrant leader.

## SmartFilter®

Web Gateway Security

- » Řízení přístupu k internetu.
- » Zvýšení produktivity práce.



## Sidewinder®

Network Gateway Security

- » Aplikační proxy firewall.
- » IPS, Antivirus, Antispam, URL filtrace.

Distributor pro ČR a SR

www.comguard.cz; info@comguard.cz

**COMGUARD**  
communication security