CSI: Internet

7. část

Vandalismus na internetu

Dorostenecký hacker znetvořil webovou stránku internetového fóra a vymazal uživatelská data. Snaživý „script kiddy" však po sobě zanechal stopy, které neušly našemu vyšetřovatelskému týmu.

Valentin Pletzer, autor@chip.cz

Martina Najberková to stále ještě nemůže pochopit. „Hacked By DjEmrah," opakuje nevěřícně. „Když jsem to uviděla na naší domovské stránce, málem se mi zastavilo srdce." Martina Najberková je šéfredaktorkou velkého fóra věnovaného herním konzolím. Osudného dne však z této webové stránky nezbylo zhola nic. Kdo na ni zavítal, spatřil jen hackerovu jízlivou zprávu.

Tento druh útoků se anglicky jmenuje defacement (znetvoření). Pachateli bývají zpravidla „script kiddies", tedy jacísi „rádobyhackeři", jejichž schopnosti postačují jen na vyhledávání volně dostupných škodlivých kódů na internetu a kteří mají jediný cíl – škodit. Těmto zpravidla pubertálním narušitelům jde hlavně o vzbuzení pozornosti. Chtějí, podobně jako jiná sorta stejně postižených mladistvých – sprejeři, prostě zviditelnit své jméno, případně jméno příslušného gangu. Na svých webech se pak holedbají dlouhými seznamy zdevastovaných stránek. Avšak to, co junioršti hackeři sami považují za zábavu, má pro jejich oběti často velmi hořkou příchuť. Především tehdy, závisí-li na poničené webové stránce živobytí jejího provozovatele – například v případě internetových obchodů. Kromě finančního výpadku způsobeného nedostupností stránky je totiž důsledkem i odrazení zákazníků.

Abychom zjistili, k jak velké škodě došlo, chceme změněnou webovou stránku nechat odborně posoudit. Avšak naši znalci mají smůlu: aby fórum nezůstalo dlouho off-line, byla nahrána záloha z minulého dne. „Škoda naštěstí není tak velká," říká šéfredaktorka. „Hacker sice pokazil naši domovskou stránku a smazal seznam všech uživatelů, ale zbytek stránek zůstal nedotčen."

Místo činu

SYMBOL VÍTĚZSTVÍ: Signaturou internetového vandala je turecký půlměsíc. Naštěstí nezanechal žádný škodlivý kód, který by mohl infikovat počítače návštěvníků stránky.

Objevujeme místo průniku

Při práci se nejprve soustřeďujeme na nejvyšší prioritu Martiny Najberkové: aby se podobná událost neopakovala, je třeba především uzavřít bezpečnostní mezeru, kterou útočník využil. Jinak nebude dlouho trvat, a dočkáme se dalšího napadení. Na postiženém serveru tvoří základní kostru softwaru systém pro správu fór Burning Board a portálové nástroje JGS. Ty ještě doplňuje řada plug-inů a dalších rozšíření, speciálně vyvinutých pro potřeby fóra. To celou věc silně komplikuje, neboť pro úplnou analýzu by zde byl zapotřebí rozsáhlý audit, při němž by bylo nutné zkontrolovat řádek po řádku i vlastnoručně psané programy.

Poněvadž ale vše nasvědčuje tomu, že za vloupáním stojí nějaký „script kiddy", který si vypomohl dostupnými hackerskými stavebnicemi, analýzu začínáme u základního softwaru. Máme tak velkou šanci, že pro toto vybavení je v nějaké bezpečnostní diskusní skupině inkriminovaná mezera zdokumentována. Tyto „mailing listy" jsou ovšem poněkud sporná záležitost, neboť na jedné straně se v nich správci systémů informují o rizicích, ale na druhé straně mohou v nich publikované příklady programových kódů posloužit jako perfektní podklady pro hackerské útoky.

Je tomu tak i v tomto případě. V diskusní skupině Bugtraq nacházíme 21 bezpečnostních mezer pro Burning Board a tři

Nový seriál Chipu

V americkém kriminálním seriálu o CSI objasňují vyšetřovatelé zločiny pomocí vědeckých metod. Chip si vzal „Kriminálku Las Vegas" za vzor pro novou řadu článků, která ukáže, jak profesionální vyšetřovatelé a specialisté bojují proti strmě narůstající počítačové kriminalitě.

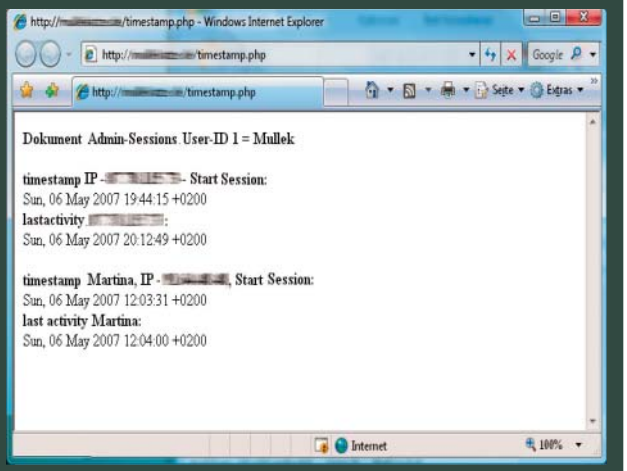
pro portál JGS. Díky znalosti verzí softwaru používaného na našem serveru se nám seznam dosud neuzavřených mezer daří dále omezit. A pak už to máme: v jednom z mailů je popsáno, jak lze nově nastavit heslo správce fóra – což je samozřejmě také skvělý návod pro „script kiddies".

Dá se v něm zjistit, jak lze prostřednictvím vyhledávacího formuláře v softwaru fóra pomocí tzv. „SQL Injection" propašovat záškodnický kód, který je pak přenesen přímo do databanky. Pomocí něho může útočník nejen načítat data, ale také je zapisovat – například uživatelská jména nebo hesla. Když normální uživatel zadá své vyhledávací kritérium, systém z něj vytvoří SQL dotaz, který pak databanka interpretuje. Hacker ovšem vloží nejen vyhledávací pojem, ale také svůj vlastní SQL příkaz, který se pak rovněž provede. Chceme-li tomu zabránit, je nutno každý vstup kontrolovat a škodlivý kód vyloučit.

Pátráme po stopách

Abychom se přesvědčili, že vstupní bránou pro hackera skutečně bylo nedostatečně zabezpečené vyhledávání ve fóru, prozkoumáváme log soubor webového serveru. Tam jsou zaprotokolována všechna volání stránek, včetně příslušné IP adresy a času. Byla by zde tedy uvedena i případná SQL Injection, stejně jako vyvolání každé jiné stránky. Není ovšem vyloučeno, že útočník tyto položky vymazal, aby po sobě zahladil stopy.

Důkazní materiál



ANALÝZA: **Protokol webového serveru prozradil datum a čas napadení i s IP adresou útočníka.**

Položky protokolovacího souboru redukujeme jen na vyhledávací požadavky – a pak už v nich objevujeme stopu, která napadení prozrazuje: náš záškodník pouhými třemi SQL příkazy vymazal z databanky všechny uživatele, nově založil účet správce a nastavil vlastní heslo. Nyní už tedy známe vetřelcovu IP adresu. Jejím cíleným hledáním v protokolu pak detekujeme všechny aktivity hackerského dorostence. Abychom mu zabránili v dalších neplechách, aktualizujeme softwarový systém fóra, čímž bezpečnostní díru zacelujeme.

BUGTRAQ: **Mezer ke zneužití opravdu není málo...**

Protiakce

Teď už by pro vetřelce mohlo jít do tuhého: díky protokolu webového serveru nyní známe přesný čas a také IP adresu, z níž útok přišel. Nevíme ovšem, zda se za touto adresou, kterou dokážeme přiřadit jednomu z poskytovatelů, skutečně skrývá přímo „náš člověk". Byl-li totiž chytrý, pak zneužil další oběť jako prostředníka a tak ho vtáhl do celého případu.

Ve hře je tedy především následující důležitý faktor: pouze v případě, že se za zjištěnou IP adresou skrývá skutečný pachatel, existuje reálná šance, jak jej pohnat k zodpovědnosti. Martina Najberková se proto rozhoduje nechat raději celou záležitost v klidu. „Ten stres mi za to nestojí," říká. „Hlavně jsem ráda, že se nestalo nic horšího." A tak je výsledkem nerozvážné klukoviny alespoň jedno pozitivum: v tomto internetovém fóru budou už napříště aktualizace odstraňující bezpečnostní mezery v seznamu priorit zcela nahoře.

Hackeři však ovládají ještě mnoho jiných triků, které už se nedají překazit jen prostou aktualizací softwaru – a už v příštím pokračování našeho seriálu některé z nich odhalíme.

Valentin Pletzer

VÍCE INFORMACÍ

www.securityfocus.com: Vedle diskusní skupiny Bugtraq je zde udržována také databanka bezpečnostních mezer.