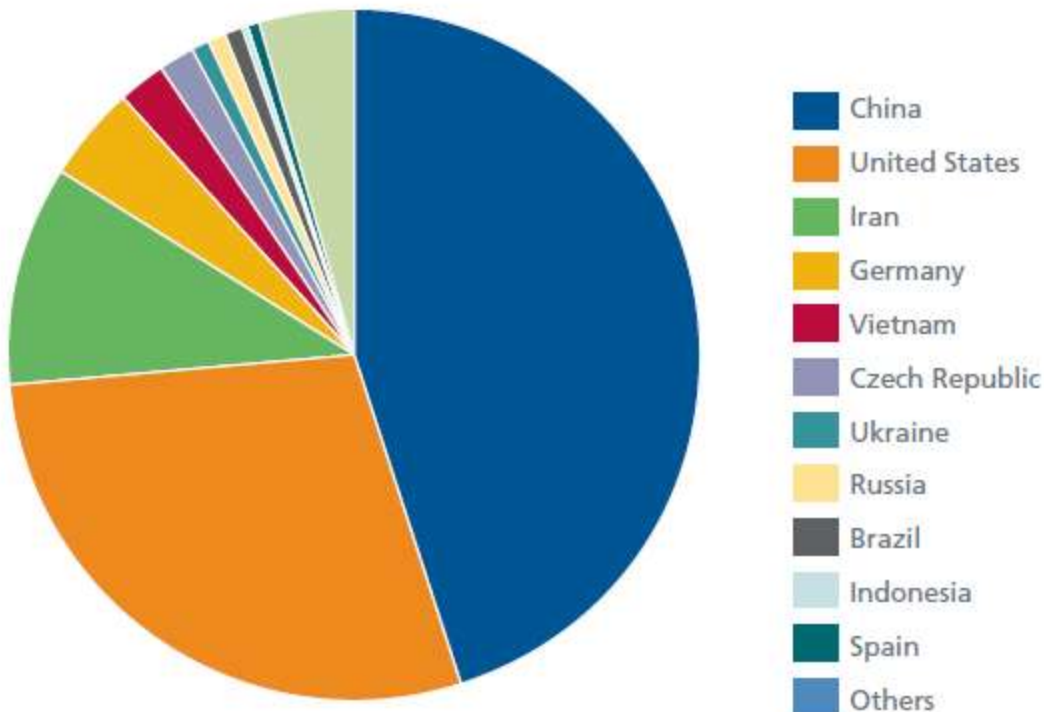


Komentář: Zpráva o hrozbách McAfee za 4. čtvrtletí 2010

Brno 8.3. 2011

Sources of SQL-Injection Attacks



Útoky na webové aplikace

V hodnocení hrozeb za poslední čtvrtletí roku 2010, které sepsala společnost McAfee na základě údajů ze své monitorovací sítě, se objevila i Česká republika, která "obsadila" šesté místo v žebříčku zdrojů útoku SQL-Injection. Zpráva McAfee neuvádí cíle těchto útoků, ale bylo by hazardem spoléhat se na to, že pod svícnem zůstane tma.

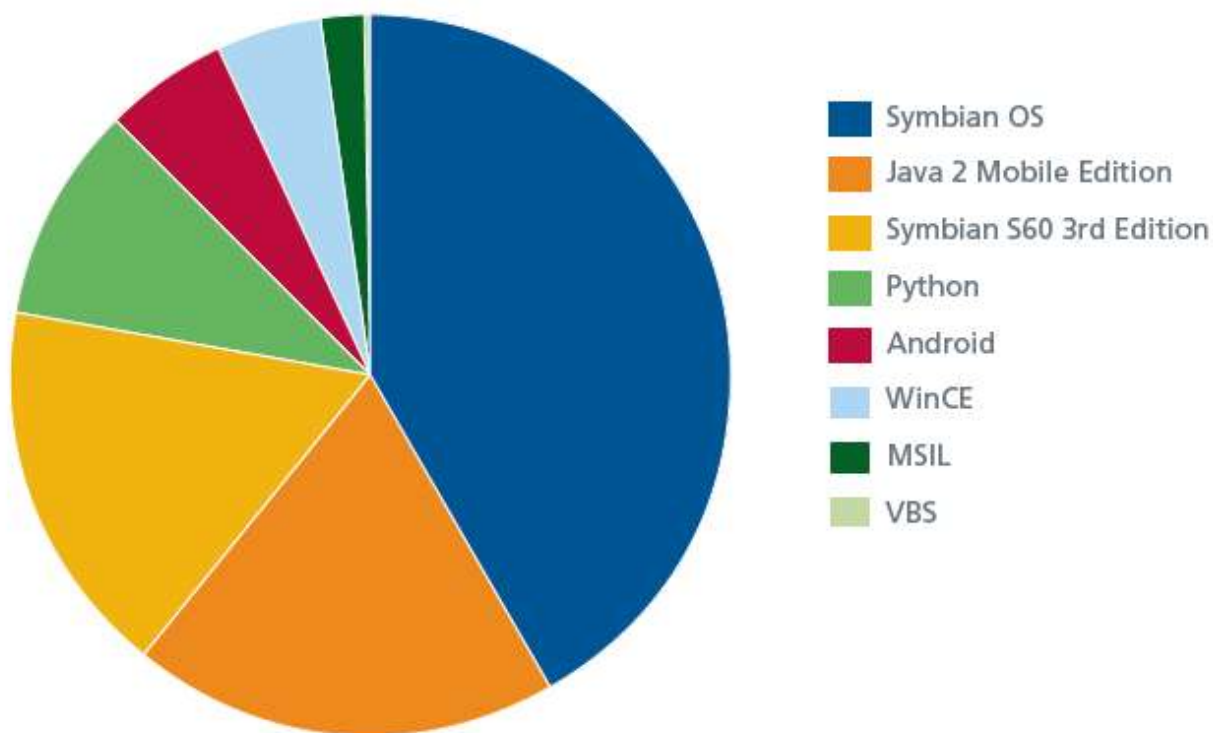
Útoky SQL-Injection jsou nejčastěji vedeny za účelem získání dat a mohou ohrozit i přístupové údaje uživatelů. Většinou jsou mířeny na veřejné webové prezentace a právě míra jejich zabezpečení určí možnost úspěchu. Chybám ve webových aplikacích se nelze nikdy úplně vyhnout, proto je zapotřebí provádět pravidelné testy a zranitelnosti urychleně opravovat.

Společnost McAfee přesně pro tyto účely dodává Web Vulnerability Assessment Module do produktu Vulnerability Manager. Stačí pouze nastavit frekvenci a cíle testů a jsme schopni získat report zranitelnosti z pohledu útočníka a následně chyby opravit dříve, než budou

zneužity. Další možností ochrany proti SQL-Injection útokům je použití web application firewallu WebDefend společnosti Trustwave. Ten funguje jako reverzní proxy a kontroluje každý požadavek, který je na webovou aplikaci vyslán. Zranitelnost nalezenou pomocí McAfee Vulnerability Manageru můžeme ihned eliminovat pravidlem na WebDefend web application firewallu.

Známým příkladem SQL-Injection je série útoků prováděná osobou (nebo skupinou osob) pod pseudonymem „Igigi“. Byla zveřejněna data z mnoha českých a slovenských webů, útočník nebyl nalezen. Data nebyla zneužita, protože to pravděpodobně nebylo cílem útočníka, i přesto ale jména společností utrpěla. Nelze odhadnout, kolik se odehrává útoků, které nejsou zveřejněny a jejichž následkem získávají útočníci přístup do cizích systémů, aniž by o tom oběti útoků věděly.

Mobile Threats by Platform, 2009–2010



Mobilní zařízení plnohodnotným cílem počítačového podsvětí

Nárůst hrozeb pro mobilní platformy je enormní a je dán několika faktory:

- 1) Rapidně narůstá počet chytrých telefonů. Často navíc obsahují zastaralý operační systém a software, takže jsou jednoduše napadnutelné.

- 2) Mobilní internet se stává masovou záležitostí, což umožňuje tvorbu mobilních botnetů, krádeží dat a přístupových údajů.
- 3) Bezpečnostní software na mobilních telefonech používá jen minimum uživatelů. Takové prostředí je rájem pro škodlivý software, který může na pozadí pracovat, aniž by o něm měl uživatel ponětí.
- 4) Ztráta a krádež mobilního telefonu je ještě snadnější, než tomu je v případě notebooku. Přitom vzhledem k výkonnosti a kapacitě začínají obsahovat telefony prakticky stejné množství citlivých dat jako notebooky (emaily, dokumenty, atd.)

Centrální správa mobilních zařízení je stejně důležitá jako správa klasických počítačů (resp. notebooků). Vzhledem k velkému množství platform a verzí operačních systémů může být nalezení jednotné správy obtížné. Společnost McAfee nabízí širokou podporu platform a velkou výhodu v minimalizaci systémových nároků, což je zatím u mobilních platform velmi důležitá podmínka. McAfee Enterprise Mobility Management nefunguje jako další software, který využívá zdroje mobilního zařízení, ale místo toho vynucuje a monitoruje použití funkcí samotného operačního systému. Elegančně tak umožní např. vynucení šifrování a definici bezpečnostní politiky.

Robert Šefr, IT Security Consultant, COMGUARD, a.s.