Setkání elitních hackerů

Rootkit pro Windows 7, prolomené SSL šifrování, manipulovatelný automatický aktualizační program – na konferencích Black Hat a Defcon prezentují světově proslulí hackeři to nejlepší z hackingu...

ULI RIES

V předvečer konference Black Hat se někteří prominentní hackeři sami stali oběťmi hackerů: undergroundové skupině „Anti-Sec“ se podařilo hacknout servery Dana Kaminského a Kevina Mitnicka. Úlovek: důvěrné e-mailové a chatové rozhovory, jakož i seznam hesel Kaminského, která moc pečlivě uložena nebyla. Není to nic moc senzačního, ale v médiích to vypadá přinejmenším efektně...

Dřívější premiéry: První rootkit pro Windows 7

Hned první den konference Black Hat vyvolala pozornost prezentace 18letého Rakušana Petera Kleissnera. Předvedl bootkit „Stoned“ – což je rootkit nahraný dříve, než je spuštěn operační systém. Zvláštností je navíc to, že Stoned dokáže vpašovat malware do všech verzí Windows včetně Windows 7. Navíc dokáže „hacknout“ TrueCrypt, což je oblíbený opensourcový software pro kódování disku.

Útoky zcela odlišné povahy nabízí jiný z nástrojů, poprvé představený na Defconu: software „Ippon“ obelstí automatický aktualizační mechanismus známých aplikací, jako je Adobe Acrobat či Skype. Ippon přinutí programy, aby se domnívaly, že dochází k aktualizaci, ve skutečnosti do nich však natlačí trojského koně. Funguje to následujícím způsobem: Útok začíná útokem MitM (Man-in-the-Middle). Nejjednodušším způsobem je využití Wi-Fi: nástroj simuluje free Wi-Fi hotspot na PC útočníka a takto vstoupí do datového provozu uživatelů, kteří hledají volný přístup na internet. V ohrožení však nejsou jen bezdrátové sítě: spoofingový nástroj ARP lze využít i pro útoky MitM v kabelových sítích. Tento nástroj v dalším kroku zfalšuje síťové adresy, a pokud někdo v takto sledovaném datovém provozu spustí aktualizaci aplikace a připojí se k některé ze známých aktualizačních adres, Ippon přeruší spojení a do aplikace doručí malware.

Jeff Moss je zakladatel konference Defcon a také vlastník bezpečnostní firmy Black Hat.

Peter Kleissner na konferenci představil bootkit, který dokáže infikovat i nová Windows 7.

Moxie Marlinspike nalezl slabé místo v bezpečnostním protokolu SSL - tedy dokonalou příležitost pro phishingové stránky.

Dan Kaminsky se sám stal obětí hackingu – na konferenci koloval seznam jeho hesel...

SSL plné mezer: Stavební manuál pro perfektní phishing

Takovému útoku lze předcházet pomocí SSL kódování přenosu dat nebo záplatami, které jsou digitálně podepsané a distribuované Microsoftem (Ippon tedy nemusí dělat starosti aktualizačnímu programu Windows). Doporučit však lze i obecné bezpečnostní opatření: pokud musíte stáhnout aktualizace ve veřejných sítích, musíte tak učinit přímo z webových stránek výrobce. Nezávisle na sobě představili Dan Kaminsky a Moxie Marlinspike nebezpečné slabé místo implementace kódovacího protokolu SSL (Secure Socket Layer). Tito hackeři předvedli, jak by dokázali „vydat“ platný SSL certifikát pro jakoukoliv internetovou doménu. Kdyby kyberzločinci dokázali tento trik používat, vytvářeli by perfektní kopie webových stránek zabezpečených SSL a stali se tak experty na vytváření nerozeznatelných phishingových stránek. Podle hackerů nepodléhá v současnosti tomuto certifikačnímu triku pouze Firefox 3.5.

INFO: www.blackhat.com
www.defcon.com

FOTO: ULI RIES