



Navíc chyby typu XSS se podle autorů výzkumu nejnázneji dohledávají, nicméně časem se nejspíš objeví celá řada dalších metod využívajících jiných principů. Google tak, tvrdí Johansen a Osborn, sice může odstranit konkrétně zjištěné chyby, ale samotný problém zůstává.

...ani MS Office

Společnost Google ovšem může uklidnit, že na konferenci došlo i na její konkurenty – Apple (viz výše) a Microsoft. Výzkumníci se soustředili na MS Office. V minulosti byly dokumenty MS Office častým vektorem útoku. Microsoft ale udělal v novějších formátech souborů celou řadu opatření včetně otevírání starších formátů nebo podezřelých dokumentů ve speciálně chráněných režimech. Kdo dnes naráží třeba na makroviry? Útočníci mají nyní jiné oblíbenější cesty do systémů, PDF, flash nebo Javu.

Přesto na Black Hatu výzkumníci ukázali, že formát MS Office nabízí podvodníkům stále řadu možností. Demonstrovali to Sung-Ting Tsai a Ming-Chieh Pan z Tchajvanu. Dokumenty MS Office se podle nich často používají v těch nepokročilejších útocích (APT, Advanced Persistent Threats), které bývají přizpůsobeny na míru konkrétnímu příjemci.

Výzkumníci tvrdí, že otevřít dokument ve Wordu nebo Excelu není bezpečné ani v případě, že uživatel má MS Office aktualizován a aktuálně nejsou známy ani žádné hrozby typu zero day. Potíž je v tom, že útočníci mohou zkoušet různá hybridní zneužití, kdy do dokumentu MS Office vloží jiný obsah, typicky video ve formátu flash.

Zde už nad zero day zranitelnostmi nemá

Microsoft kontrolu (alespoň přímou). Kód v souboru flash pak může vypnout i ochrany v novějších verzích Windows DEP (Prevence spuštění dat, Data Execution Prevention) a ASLR (znáhodnění adresního prostoru, Address Space Layout Randomization). Adobe se sice snaží pro objekty flash vytvořit ochranu na způsob sandboxu, všechny tyto technologie jsou však zatím překonatelné.

Každopádně proti těmto typům útoku dává jen malou ochranu antivírus založený na signaturách, i když systémy pro prevenci vniknutí (IPS) rizika zneužití snižují.

Ještě k hrozbám APT a relativní bezpečnosti jednotlivých platforem: Alex Stamos a jeho kolegové z organizace ISEC se pokusili analyzovat problém těchto hrozeb na MacOS X. Google byl v Číně před dvěma roky kompromitován, když jeho zaměstnanci používali Windows a už tehdy notně zastaralý MS Internet Explorer 6. Pomohlo by mít místo toho počítače Apple?

Stamosův závěr je, že nikoliv, protože jádro útoků APT se nevztahuje ke konkrétnímu softwaru ani zranitelnostem. Každopádně sítě se systémy MacOS jsou možná odolnější v první fázi útoku, nicméně jakmile podvodníci již jednou najdou cestu do sítě, je tato platforma oproti Windows údajně ještě mnohem snáze ovládnutelná.

Odpojit od internetu nestačí

Tim Roxey z agentury North American Electric Reliability Corporation (NERC), která má za cíl prosazování průmyslových standardů, tvrdil na Black Hatu, že energetické systémy i průmyslové podniky jsou stále citlivé na kybernetické útoky, dokonce

i takové, které lze spustit prostým odesláním textové zprávy. Stále roste podíl komunikace mezi zařízeními bez lidské účasti (MLM) a útočník vstoupí do tohoto procesu.

Některé systémy ve vzdálených lokalitách využívají karty pro mobilní připojení k internetu. Útočníkovi v těchto případech stačí jediné – znát telefonní čísla přiřazená kartám a už zkoušet posílat SMS s útočným kódem. I systémy, které jsou chráněny odpojením od internetu, mohou být stále zranitelné přes GSM nebo pomocí senzorů monitorujících jejich stav (které už mnohdy k internetu připojeny jsou).

Jednotky PLC (programovatelné automaty, Programmable Logic Controller) řídící průmyslové procesy budou podle Roxeyho stále častějším cílem útoků. Dillon Beresford z NSS Labs tvrdí, že průnik na úrovni čerpa Stuxnet lze vytvořit řádově během týdnů práce v pokoji, tj. bez dalších důvěrných informací. Podobné prostředky nemají tedy zdaleka k dispozici jen vlády, armády nebo tajné služby, ale tyto útoky může provádět celá řada skupin i jednotlivců.

Platit, nebo ne?

Má se platit výzkumníkům za objevené bezpečnostní zranitelnosti? Přístupy se liší, Google a Mozilla tak činí, Microsoft či Oracle ne. Microsoft ovšem nabízí odměny jednorázové (za odhalení autora viru apod.).

Na Black Hatu tato společnost navíc oznámila cenu BlueHat v hodnotě 250 000 dolarů. Je určena za nejlepší novou technologii, která bude útočníkovi bránit zneužívání zranitelností v paměti. Mělo by jít o obecnější postup, který omezí možnosti zneužití funkcí připomínajících ASLR.

Krádeže duševního vlastnictví zasáhly celý svět

Studie Operation Shady RAT (Operace Krysa ve stínu), kterou zveřejnila společnost McAfee, mapuje několik let akcí profesionálního gangu kybernetických zločinců. Útočníkům se podařilo zmocnit obchodních tajemství a duševního vlastnictví největších světových firem i vlád států. Jde podle všeho o nejmasivnější sérii kybernetických útoků posledních několika let.

ALEŠ PIKORA

Počítačovní podvodníci se dnes nezajímají v první řadě o informace o bankovních účtech nebo platebních kartách. Trh s těmito

údaji je již nasycený a ceny, za které lze tyto údaje prodávat, nízké.

Pro útočníky je mnohem výnosnější soustředít se na duševní vlastnictví firem a dalších institucí, např. vlád a státních agentur.

Na současném černém trhu se výborně prodávají státní tajemství, zdrojové kódy softwaru, databáze softwarových chyb, archivy firemních důvěrných e-mailů, znění právních smluv, technická dokumentace k výrobkům nebo údaje o konfiguraci systémů SCADA (aplikace pro řízení průmyslových procesů).

Útoky proti všem

Ukazuje se, že zločinci jsou ve snaze získat cenná data schopni vyvinout systematické úsilí, které v případě některých cílů trvá i několik roků. Operation Shady RAT mapuje posledních pět let útoků proti více než 70 velkým nadnárodním firmám, vládám i neziskovým organizacím.

Postiženy byly instituce v celkem 14 zemích, což se zdá skoro neuvěřitelné.

Anatomie útoku

- **Příprava:** Zmapování struktury organizace, volba kontaktů (e-mailových adres), snaha o „sociální zmapování“ cílů (zaměstnanců), pokus získat insidera.
- **Průnik:** Personalizovaný phishingový e-mail obsahující podvodný dokument PDF nebo DOC nebo linky na web pokoušející se o útok typu drive-by download. Další varianty: rozesílání médií DVD nebo USB flash s malwarem. Využívání různých zranitelností typu zero day v běžně používaném softwaru.
- **Vznik zadních vrátek:** Pokus kompromitovat účet s co největšími oprávněními, snaha o zvýšení oprávnění. Potřeba kompromitovat další počítače pro případ, že útočníci přijdou o přístup k původnímu. Instalace dodatečného malwaru ve firemní síti.
- **Zapojení do infrastruktury:** Instalace trojských koní a keyloggerů, které útočníci budou moci vzdáleně spravovat. Zřízení šifrovaného tunelu mezi kompromitovanými počítači a řídicím (command and control) serverem.
- **Prohledávání sítě a krádeže dat**
- **Dodatečné škody:** Instalace trojských koní do objevených zdrojových kódů, narušení kritických systémů SCADA apod.
- **Monitoring:** Snaha vyhnout se detekci, aktualizace malwaru, odinstalování kódů, u nichž je nejvyšší riziko odhalení. Další sledování provozu sítě a dat. V této fázi útočníci také analyzují ukradená data a zřejmě se je pokoušejí zpeněžit.

Kompromitována byla data subjektů velmi různého typu: od americké vládní agentury po vietnamskou, státem vlastněnou firmu, od dodavatelů armády po firmu

podnikající na poli satelitní komunikace.

Mezi ukradenými daty jsou pak i takové speciální informace jako databáze odposlechů nebo mapy ropných polí.

Slovo RAT v názvu studie současně znamená zkratku nástroje pro vzdálený přístup (Remote Access Tools); právě tyto nástroje útočníci často používali k další práci s kompromitovanými sítěmi. Mnohdy se jim dařilo fungovat zcela nepozorovaně.

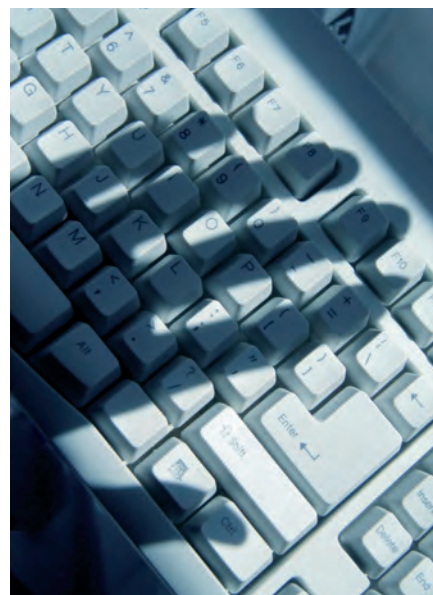
„Velké firmy se dnes dělí de facto na dvě kategorie: na ty, které vědí, že byly napadeny, a na ty, které sice napadeny byly rovněž, ale nevědí o tom,“ uvádí Dmitri Alperovitch, výzkumník hrozeb ve společnosti McAfee a hlavní autor studie.

Značnou mediální pozornost si letos získaly bezpečnostní incidenty RSA, Lockheed Martin nebo Sony, ovšem tyto firmy pravděpodobně nepředstavují žádnou výjimku. Většina postižených organizací, sledovaných v rámci studie, únik dat pravděpodobně vůbec nezaznamenala – až do chvíle, kdy jim tuto informaci poskytla společnost McAfee.

Není jasné, jak útočníci s ukradenými daty naložili. Možná část z nich prodali konkurenci napadených firem, která je teď použije ve vlastních produktech. Vyčíslit celkové ztráty je obtížné, v některých případech však útoky mohou poškodit nejen dotčené organizace, ale i celé země, tvrdí D. Alperovitch ve zprávě. Uvádí rovněž, že tato operace znamená největší „přesun“ duševního vlastnictví, k němuž kdy došlo v dosavadních lidských dějinách.

Podle údajů byly informace o probíhajících útocích získány, když ve spolupráci s bezpečnostní komunitou byl objeven jeden z řídicích (command and control) serverů podvodníků.

Pouze na tomto jediném serveru se nacházela ukradená data v objemu petabajtů. Všechny tyto akce provedla, zdá se, jediná skupina útočnicků, která používala příslušný



řídicí server. Vše se pravděpodobně uskutečňovalo s podporou nějaké vlády nebo obdobné instituce disponující dostatečnými zdroji pro činnost podobného rozsahu. V souvislosti s kybernetickou špionáží bývá nejčastěji zmiňovanou zemí Čína (nebo Rusko), závěry studie Operation Shady RAT ale nikoho konkrétního nejmenejí.

Akce profesionálů

Jak se ukazuje, operace Aurora – útok proti Googlu – i Night Dragon – útok proti energetickým firmám – představují jen špičku ledovce. Postupy typu APT (Advanced Persistent Threats, pokročilé přetrvávající hrozby) jsou dnes mnohem častější, než si řada potenciálních obětí připouští.

Útočníci provádějící akce každopádně disponovali mnohem většími znalostmi i zdroji než aktivistické amatérské skupiny hackerů, jsou jsou Anonymous nebo LulzSec. Operace postupovala promyšleně, zaměřovala se nikoliv na destrukci, ale na cenné duševní vlastnictví.

Útok byl velmi komplexní, neomezoval se na jediný typ malwaru nebo zneužití konkrétní zranitelnosti. Prováděné postupy byly přesně cílené (spear phishing). Na počátku stál obvykle e-mail odeslaný tak, aby v případě kompromitování počítače byl ovládnut účet s co nejvyššími oprávněními; následovala snaha ovládnout i další počítače, aby tak v případě vyčištění jednoho stroje útočníci neztratili přístup do sítě.

Celá kauza rozhodně není u konce a útočníci jsou podle všeho stále aktivní. Likvidace jednoho řídicího serveru neznamená, že si vzápětí nezřídí nový. Vyřadit z činnosti celou infrastrukturu podvodníků je přitom obtížné, protože to závisí na vymahatelnosti práva po celém světě.

Autor pracuje jako ředitel divize DataGuard ve společnosti PCS

Tipy pro ochranu

- **Zabezpečení e-mailu a webové štíty:** tyto nástroje by měly snížit riziko doručení e-mailu obsahujícího škodlivou přílohu. Webový štít by měl uživateli zabránit po kliknutí na link zobrazit podvodný web.
- **Komplexní ochrana koncových bodů:** měla by bránit stahování a instalaci malwaru do počítačů.
- **Firewall a systém IPS (prevence vniknutí):** měly by odhalit komunikaci mezi kompromitovaným počítačem a řídicím serverem podvodníků.
- **Whitelist aplikací:** Měl by v podnikové síti povolit pouze provoz schválených aplikací.
- **Monitoring databází:** Měl by zabránit nebo alespoň odhalit neoprávněný přístup ke kritickým databázím.
- **Implementace šifrování:** Kritická data pak budou i v případě krádeže pro útočníky bezcenná.
- **Systémy DLP (Data Loss Prevention):** Monitoring pohybu kritických dat.
- **Ostatní:** analýza fungování sítě (může odhalit podezřelé chování), systém pro centrální správu zranitelností (umožňuje včasnou a efektivní instalaci bezpečnostních záplat), školení uživatelů...