

Komentář

Brno 4.8. 2011

McAfee odhaluje největší sérii cyber útoků posledních pěti let

Útok pojmenovaný společností McAfee jako Operation Shady RAT odcizil data ze 72 společností ve 14 státech světa včetně vládních organizací a agentur nebo národních olympijských výborů.

Dmitri Alperovitch, Vice President Threat Research společnosti McAfee, komentuje report týkající se těchto útoků následovně.

„To, čeho jsem byli svědky v posledních pěti až šesti letech, nebylo nic menšího než historicky bezprecedentní přesun bohatství - přísně střeženého státního tajemství (včetně dat z tajných vládních sítí), zdrojového kódu, databází odposlechů, e-mailových archivů, detailů průzkumů pro nové aukce ropných a naftových polí, elektronických archivů, atd. První útoky začaly již v roce 2006. Nejkratší útoky trvali méně než jeden měsíc a nejdelší známý útok na Olympijský výbor v Asii běžel 28 měsíců a končil v lednu 2010.

Po usilovné analýze logů jsme byli překvapeni obrovskou rozmanitostí obětí organizací a drzostí pachatelů. Napadené organizace jsme rozdělili do následujících kategorií a světových regionů.“



Byl použit následující standardní postup pro tyto typy cílených útoků. Cílený phishing e-mail obsahující exploit je odeslán na správně zvolenou úroveň přístupu v konkrétní společnosti a exploit při otevření v neaktualizovaných systémech spustí stahování malwaru. Malware naváže spojení s řídicím serverem (Command & Control Server) a může být skrze něj ovládán pomocí komentářů ukrytých v kódu webové stránky (odborníci McAfee získali do tohoto řídicího serveru přístup, mají proto k dispozici obrovské množství údajů o všech útocích, které z něj probíhaly). Následně útočníci přistupují na infikované počítače a pokouší se získat přístupové údaje s co nejvyšším stupněm oprávnění. Zároveň infikují další stroje, aby v případě ztráty jednoho z nich nepřišli o přístup do sítě organizace. Hlavním cíle operace je ale identifikovat klíčová data a vynést je ze společnosti.

Zájem o informace uložené na serverech národních Olympijských výborů, jakož i o informace z Mezinárodního olympijského výboru (IOC) a Světové antidopingové agentury v době přípravy

Olympiády 2008 a bezprostřední návaznosti na samotnou Olympiádu v roce 2008, byl obzvláště zajímavý a potenciálně ukázal prstem na stát, stojící za útoky. Mezi oběťmi útoku je i mnoho euroamerických politických a neziskových organizací nebo expertní skupiny národní bezpečnosti USA, což zužuje množinu možných útočníků. Útok na Organizaci spojených národů nebo na sekretariát ASEAN (Sdružení Národů Jihovýchodní Asie) naznačuje i jiný motivační zájem skupiny než ekonomický přínos.

Z nalezených stop společností McAfee, která nejmenuje samotný zdroj útoku, vyplývá logický závěr, který zveřejnily zpravodajské servery na celém světě, že útočníkem může být i samotný stát Čína.

Operation Shady RAT je další z řady populárních APT útoků, které mají téměř identický průběh, ale přesto jsou stále úspěšné. Společnost McAfee nabízí ve svém portfoliu ochranu proti všem fázím útoku. Nejspíš právě proto je natolik úspěšná i při jejich odhalování (v minulosti např. Operation Aurora, Night Dragon) a poznatky, které během šetření bezpečnostní odborníci získají, mohou zpět využít při vývoji všech částí portfolia bezpečnostních nástrojů.

Pro ochranu proti první fázi útoku je nutná pokročilá kontrola emailového a webového provozu na perimetru, aby se útočníkům nepodařilo infiltrovat vnitřní stroj. Pokud by již k infiltraci koncového bodu mělo dojít, je možné využít nástrojů implementujících hostovské IPS, případně úplně eliminovat neznámý software pomocí aplikačního whitelistingu (o antivirové ochraně, která je úplnou samozřejmostí, nemluvě). Identifikaci a případně blokaci podezřelé aktivity na vnitřní síti a perimetru zajistí kvalitní síťová IPS sonda. Cílem útočníků není infiltrace systémů, ale především zcizení citlivých dat, proto může být další vrstvou ochrany před útokem silné šifrování souborů nebo DLP systém.

PDF verzi Operation Shady RAT reportu včetně kompletního seznamu všech 72 cílů, včetně země původu, data zahájení prvního útoku a doby trvání narušení najdete [ZDE](#).

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

-

Společnost COMGUARD a.s. je nadnárodní společností zaměřenou na value-added distribuci produktů bezpečnosti IT. K jejím hlavním partnerům patří společnosti McAfee (vč. akvizované Secure Computing), Cyberoam, ActivIdentity, Infoblox, LogRhythm, Trustwave, SonicWALL, SecurEnvoy, Procera Networks, Zeus Technology a další. Společnost působí na trzích střední a východní Evropy, zejména v České republice a na Slovensku. Poskytuje řešení a služby pro segment SMB, velké komerční společnosti a státní organizace. Společnost je vlastněna jejím managementem.

Další informace: <http://www.comguard.cz/>, Lenka Wallezská, Marketing Manager, e-mail: lenka.wallezka@comguard.cz, tel.: +420 544 509 066.