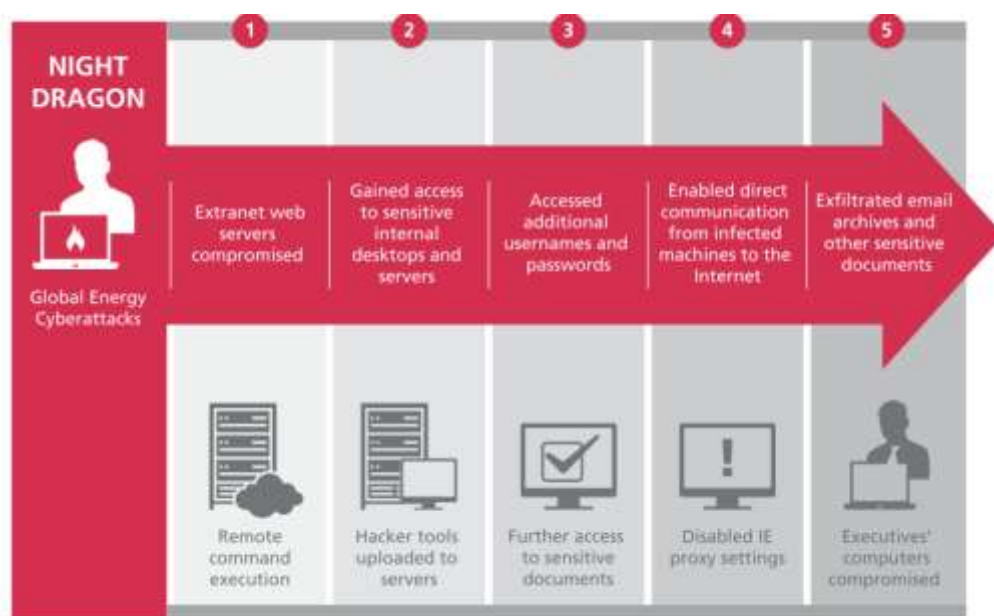


Komentář: Night Dragon, Operation Aurora a další útoky aneb Mladý a perspektivní tým s úkolem odcizit vaše data

Brno 8.4. 2011

Útoky typu „Advanced Persistent Threat“ ukazují, že i společnosti s pokročilým zabezpečením IT infrastruktury, mohou být nabourány. Cílem průniku jsou většinou citlivá data, v některých případech i průmyslová sabotáž. Na citlivá data byly zaměřeny útoky jako Operation Aurora, Night Dragon nebo úplně aktuální útok na společnost RSA, při kterém byla odcizena data týkající se zařízení SecurID. Ukázkovým příkladem sabotáže byl i útok vedený červem Stuxnet.

Na následujícím obrázku je pět fází popisující celý útok Night Dragon, který byl zveřejněn společností McAfee.



První fáze – jen dva prstíčky...

Útočníci se nejprve snaží zjistit co nejvíce informací o svém cíli. Jakákoliv informace je cenná, ať už se jedná o infrastrukturu nebo zaměstnance. Jakmile je mozaika dat dostatečná, mohou se útočníci pokoušet o otevírání prvních dveří do systému. Pokusy mohou být čistě technické – jako např. ovládnutí jednoho z webových serverů pomocí SQL-injection nebo jiné zranitelnosti; nebo mohou zahrnovat prvky sociálního inženýrství – vytipovaným osobám je zasílán škodlivý kód, který je uveden věrohodným příběhem (věrohodným např. proto, že o dané osobě lze zjistit dostatek informací ze sociálních sítí). Jeden z vektorů útoku nakonec uspěje a útočník získá přístup, i když pravděpodobně zatím k méně zajímavým systémům.

Druhá fáze – administrátorem snadno a rychle

Jakmile jsou útočníci uvnitř sítě, začnou se dívat po důležitých strojích a přístupu na ně. Jasným cílem je získat přístupové údaje pro uživatele s co nejvyšším oprávněním. Nabízí se použít klasické nástroje, jako jsou keyloggery, ty jsou ale často nalezeny antivirovým softwarem a hlavní je se neprozradit. Legitimní nástroje pro administraci nejsou detekovány a poslouží ke sběru informací (včetně hashů hesel uživatelských účtů). Ty mohou útočníci lámat na svých strojích (a pro urychlení využít např. GPU), takže systémy oběti ani nezaznamenají pokus o brute-force útok.

Třetí fáze – já bych si s dovolením také vzal

Ve chvíli, kdy má útočník kompletní přístup k interním systémům, začne probírat data, která si chce odnést. Fáze vyhledávání a vynášení dat může být poměrně dlouhá, může být komplikována i maličkostmi, jako je webová proxy po cestě do Internetu. Útočníci se budou snažit najít přímou cestu s minimem kontrol a komplikací, skrz kterou by mohli data kopírovat na své stroje. Cílem bude určitě emailová komunikace, veškeré dokumenty, know-how (např. ve formě zdrojových kódů, výkresů, návrhů atd.)

Obrana perimetru zdaleka nestačí

První fáze bude časově pravděpodobně velmi náročná. Společnosti se soustředí hlavně na obranu perimetru a méně již na detekci a prevenci útoků uvnitř sítě. Jakmile je jednou perimetr překonán, tak se útočník může cítit jako ryba ve vodě a mapovat si topologii sítě, hledat zajímavé servery a otevírat si další zadní dvířka.

Jak dokazují i výše zmíněné Advanced Persistent Threats, nelze přistupovat k interní síti jako k bezpečnému prostředí. Naopak je nutné přísně kontrolovat jak pohyb dat, tak zabezpečení a nastavení interních systémů a komunikaci mezi nimi. Dobrým přístupem je také oddělování rolí – proč by měl mít administrátor přístup ke všem datům? Využitím šifrování zamezíme i superuživateli v přístupu ke všem dokumentům, emailům atd.; nasazením [DLP](#) zase zabráníme jejich odeslání po síti na stroje útočníků (i kdyby se jim nakonec povedlo DLP obejít, tak do té vygenerují tolik upozornění, že budou odhaleni).

Na problémy se zabezpečením a otevřená zadní vrátka upozorní [Vulnerability Manager](#) nebo [Policy Auditor](#) – software, který umí automatizovaně reportovat stav zabezpečení strojů a upozorňovat na změny vůči minulosti. Na aplikačních serverech není důvod neprovozovat [Application Control](#), software který nedovolí spuštění cizího kódu, ani např. při útoku typu buffer-overflow a přitom je jeho nasazení otázkou minut.

Kontrola interního a odchozího provozu je přinejmenším stejně důležitá, jako kontrola toho příchozího. **Webová proxy a firewall s aplikačními signaturami** nám pomohou výrazně lépe identifikovat, co vlastně komunikuje z uživatelských počítačů. Vnitřní síť lze elegantně pokrýt kvalitní [IPS sondou](#), která zamezí oblíbeným útokům a na podezřelé chování aspoň upozorní.

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