Seznamte se - APT

Vložil/a RubberDuck [1], 4 Červen, 2013 - 19:01

- Security [2]
- Unsorted [3]

APT, nebo-li Advanced Persistent Threat, je stále poměrně nový pojem. I přes vysokou frekvenci výskytu tohoto pojmu v IT médiích dokáže jen málo lidí skutečně vysvětlit, co se za tímto slovním spojením ukrývá.

APT je označení pro skupinu útočníků (pokud se jedná o jednotlivce, neoznačuje se jako APT), která cíleně napadá konkrétní společnosti s cílem získat úplný přístup k celé síti a všem jejím datům. Jinými slovy, APT lze považovat za špionážní skupinu. APT skupiny postupují systematicky a využívají pestrou škálu útoků známých ze všedního života.

Celý útok začíná sběrem informací o oběti. Následně probíhá první fáze útoku. Pokud jsou systémy společnosti napadnutelné z venku, dojde k jejich napadení, eskalování práv a postupné obsazení celé vnitřní sítě. Pokud jsou systémy z venku nedostupné, přechází tým k útoku s využitím sociotechniky. Pak se stáváme svědky pokročílé/vylepšené podoby klasického phishingu, tzv. spear-phishingu, nebo-li cíleného phishingu. Při cíleném phishingu je oběť pozvolna vmanipulována do situace, kdy má pocit, že mailová zpráva skutečně patří jí. Toho je dosaženo vytvořením mailu tzv. "na míru". Takový mail obsahuje informace úzce související se společností (např. nové nařízení EU ke konkrétním úkonům, žádost o rozhovor, potvrzení informací z poslední tiskové konference a tak dále). V okamžiku, kdy oběť uvěří, že je mail skutečný (odepíše na mailovou adresu, ze které ji zpráva přišla, zda se skutečně jedná o reálný mail a útočník odpoví, že mail je reálný), nebrání útočníkovi nic v zaslání podvržené přílohy obsahující exploit. Běžně jsou využívány dokumenty typu PDF, DOC, XLS, HTML a podobně. Po otevření dokumentu dojde k vykonání exploitu a stažení trojského koně, jenž okamžitě začne jednat. Připojí se ke command centru a začne přijímat příkazy od útočníka. Během toho také prozkoumává síť společnosti a získané informace zasílá do command centra.

Ve chvíli, kdy útočník převezme kontrolu nad celou sítí, nastává fáze dvě. Během ní jsou ze serverů a počítačů shromažďovány důležité informace a následně odesílány útočníkovi. Ten je dále přeprodává nebo předává.

APT týmy většinou pracují s využitím vlastních nástrojů, případně v kombinaci vlastních a veřejně dostupných nástrojů. Detekce jimi používaných exploitů a malwaru je velmi náročná vzhledem k nízkému počtu zasažených cílů (řádově jednotky, maximálně desítky), tedy dostupných vzorků. Proto může mít APT tým přístup do systémů společnosti i po dlouhé roky, aniž by kdokoliv cokoliv zjistil. Velmi důležité je rovněž si uvědomit, že vyčištění celé sítě v případě detekce narušení APT týmem nemění nic na stavu věcí. Obecně platí heslo: Jednou cílem APT, navždy cílem APT. Tedy, pokud se jednou dostane společnost do hledáčku APT týmu, pokusy o její napadení budou probíhat i po úplném odstranění 'nákazy' v síti a můžeme téměř stoprocentně předpokládat, že bude tato společnost opět kompromitována.

V současnosti se velmi často skloňuje v médiích otázka využití národních APT týmů v rámci špionáže nejen zahraničních společností, ale i vládních serverů. V tomto ohledu je nejdiskutovanější zemí Čína a její údajné útoky na americké servery a společnosti na území USA.

URL článku: https://security-portal.cz/clanky/seznamte-se-apt

Odkazy:
[1] https://security-portal.cz/users/rubberduck
[2] https://security-portal.cz/category/tagy/security

[3] https://security-portal.cz/category/tagy/unsorted