Vážené čtenářky, vážení čtenáři,

sofistikované útoky APT (Advanced Persistent Threats), které probíhají skrytě a za účelem dlouhodobé kompromitace oběti, se zpravidla spojovaly s velkými organizacemi. Důvod byl nasnadě – protože jde o poměrně technicky i časově náročný projekt, musel se hackerům finančně vyplatit, a proto obvykle cílil na rozsáhlejší podniky.

To se však v poslední době mění – na trhu se totiž začínají objevovat služby APT na zakázku, které vykonání takového útoku výrazně usnadňují a zpřístupňují širokému okruhu zájemců. Na pozoru tak musejí být i menší či střední podniky a novým nebezpečím své modely hrozeb přizpůsobit. Jejich současné strategie totiž s takovými ataky nepočítají, a je tak reálné, že se stanou snadnou kořistí.

V posledních dnech vydaly hned dvě významné bezpečnostní firmy – Kaspersky a Bitdefender – zprávu o skupinách, které nabízejí vykonání APT útoků na zakázku. Zatímco v prvním případě se služba zaměřila na finanční a právnické firmy, druhá cílí na architektonická studia a videoprodukční společnosti.

Skupina, kterou odhalil Kaspersky, nese označení DeathStalker a vyznačuje se především velkou schopností adaptace a používáním iterativního rychlého přístupu ve vývoji softwaru, který jim umožňuje dělat efektivní kampaně.

Experti dokázali díky analýze propojit aktivity této skupiny se třemi malwarovými rodinami – Powersing, Evilnum a Janicab. Taktika, techniky a postupy se přitom v průběhu let takřka nezměnily: spoléhají se na rozesílání spear-phishingových e-mailů, které obsahují škodlivé soubory. Díky tomu získají útočníci kontrolu nad zařízením oběti.

Například Powersing je malware, který umožňuje pravidelně pořizovat snímky obrazovky a vykonávat libovolné powershellové skripty. Pomocí různých technik se dokáže vyhnout detekci a umožňuje i svou aktualizaci.

Pro svou činnost také využívá známou veřejnou službu, díky níž splyne backdoor komunikace s legitimním síťovým přenosem, čímž se minimalizuje šance obránců zablokovat tento provoz. Aktivity skupiny DeathStalker byly zjištěné po celém světě včetně Evropy.

Bitdefender zase objevil falešný plug-in pro 3D modelovací řešení Autodesk 3DS Max. To ukazuje, jak specificky se útočníci zaměřují na cíl a jak obtížné je takový typ ataku detekovat.

Jen o pár týdnů dříve Bitdefender odhalil jinou další podezřelou skupinu, StrongPity, jež má rysy zločineckého sdružení s finančními i geopolitickými cíli. Dalšími skupinami spojenými s útoky APT jsou podle zjištění Bitdefenderu například Barium nebo Winnti.

Zdá se tedy, že doba, kdy APT využívali především zločinci, za nimiž stojí státní zájem, už je pryč – tyto služby si v současnosti může pronajmout kdokoliv, aby například znemožnil konkurenci nebo od ní získal strategické informace. Na velikosti oběti už tolik nezáleží, protože díky detailnímu zaměření je výtěžnost takových útoků velice slušná.

A co vy – zvážili jste už útoky APT jako riziko, které reálně ohrožuje i vás?

S přáním příjemně stráveného podzimu, pokud možno bez virů (kybernetických i těch biologických),

Pavel Louda
vedoucí projektu

Obsah