Vážené čtenářky, vážení čtenáři,

jedním z momentálně nejpalčivějších bezpečnostních rizik na internetu jsou tzv. phishingové útoky, tedy situace, kdy se útočníci vydávají za jiné, legitimní uživatele nebo weby za účelem získání přístupu či uživatelských dat oběti.

Zjistit takové útoky není vůbec jednoduché, a proto také tato metoda slaví takové „úspěchy". Obrana proti nim obvykle zahrnuje jak organizační, tak technické prostředky, přičemž její účinnost spočívá z velké míry i na disciplinovanosti samotných uživatelů. Mezi klíčové technické prostředky ochrany před phishingem přitom patří ověření reputace webových stránek.

Zdá se ale, že se lze nově bránit i jinou účinnou metodou. Jak totiž zjistili bezpečnostní experti ze společnosti Akamai, mnoho phishingových stránek v současnosti využívá jedinečné uživatelské ID (UID, Unique User ID), což obráncům umožňuje pomocí automatické analýzy detekovat phishingové útoky ještě před tím, než způsobí nějaké škody.

Jak je to možné? Rostoucí počet phishingových webů totiž pro zvýšení efektivity své nekalé činnosti využívá legitimní webové analytické služby, a proto má ve svém kódu tzv. tracking ID. A právě použití těchto ID může obhájcům pomoci rychle zjistit phishingové stránky, které se využívají při útočných kampaních.

Vědci z Akamai analyzovali téměř 55 tisíc aktivních phishingových stránek obsluhovaných z 29 tisíc domén a zjistili, že 874 domén k těmto útočným stránkám přiřadilo příslušné ID pro webovou analýzu (396 identit se vztahovalo ke Google Analytics, 75 bylo použitých na více webech).

Webové analytické služby např. sledují, jak návštěvníci interagují s webovými stránkami, či shromažďují informace o jejich prohlížečích, operačních systémech, geografické poloze a dalších podrobnostech.

Kybernetičtí zločinci pochopili hodnotu těchto údajů pro měření výkonu svých útoků a dosažení lepšího cílení, takže tvůrci phishingových sad začali do svých produktů začleňovat podporu pro webové analýzy.

Útočníci pro phishingové útoky jen zřídka využívají pouze jeden web – častěji jde o komplexní kampaně, které cílí na více webů najednou a tvoří je phishingové weby na více doménách, aby se lépe zabránilo detekci a pokusům o zastavení šíření.

Pokud například ručně blokujete phishingovou adresu URL, kterou nahlásil zaměstnanec, nezaručuje to, že se celý útok proti společnosti zmařil. Phishingový e-mail, který obdržel jiný zaměstnanec, může mít jinou adresu URL, i když je součástí stejné kampaně. Automatizovaná řešení pro blacklisting URL zase spoléhají na zdroje dodavatelů zabezpečení a ty se aktualizují až poté, co tito dodavatelé sami detekují útočné kampaně a identifikují škodlivé adresy URL.

Použití stejného analytického UID na více phishingových stránkách tak mohou obránci snadno využít k vytvoření detekčního podpisu nebo pravidla webového firewallu, které blokuje všechny stránky ze stejné kampaně.

Akamai uvedl i dva příklady, kde identifikátory UID webové analýzy pomohly identifikovat větší útoky – jedním byla kampaň zacílená na uživatele LinkedInu, druhý se zaměřil na uživatele AirBnB.

S přáním příjemně stráveného zbytku letošního roku a úspěšný vstup do toho příštího.

Pavel Louda
vedoucí projektu

Obsah