

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **90** ze dne **19.11.2024**

Malvertising se nám skrývá přímo na očích

Škodlivé reklamy ve vyhledávání mohou šířit malware. Pro podvodníky je to lákavý způsob, jak nalákat co nejvíce obětí.

Někdy se za reklamou skrývá víc než jen lákavá nabídka produktu. Vývojáři malwaru se intenzivně věnují zdokonalování škodlivého kódu a zkoumání různých způsobů, jak okrást uživatele o peníze nebo data. Někdy se může jednat o malvertising – tedy propagaci škodlivého kódu.

Šíření malwaru prostřednictvím reklamy není nic nového, kyberzločinci se již dlouho zaměřují na online reklamní sítě jako na způsob, jak své podvody rozšířit. Poskytovatelé reklamního prostoru, jako Google nebo Meta, se je samozřejmě snaží blokovat. Ale jakmile vypnout jednu reklamu na podvodnou stránku objeví se jich 100 nových – zkrátka je to sisyfovská práce.

Šíření malware prostřednictvím reklam je velký problém – zejména pokud se vydávají za reklamy na legitimní weby. Pak stačí skutečně málo a můžete naletět nebo si můžete nevědomky do zařízení instalovat infikovaný program.

Malvertising

Jedná se o označení reklamy, která odkazuje na malware nebo škodlivou stránku. Útočníci pomocí takové reklamy rozšíří svůj škodlivý kód nebo podvod mezi více lidí. Jejich cílem jsou naše data, která mohou prodat na darkwebu nebo přímo peníze.

Blokování podvodné reklamy je jako hra na kočku a myš

V roce 2023 společnost Google zablokovala nebo odstranila více než 1 miliardu reklam, které zneužívaly její reklamní síť, včetně reklam propagujících škodlivý software.

Oběťmi se stali i další zadavatelé online reklamy. Vzhledem k povaze reklamního byznysu mohou útočníci manipulovat s celým reklamním řetězcem a ohrozit ho několika možnými způsoby – od nákupu reklam a vydávání se za poskytovatele vyhledávače až po hackování webových stránek a reklamních serverů.

Zatímco poskytovatelé vyhledávačů neustále odstraňují škodlivé reklamy nebo webové stránky z výsledků vyhledávání, hackeři jsou vytrvalí a stále nacházejí nové způsoby, jak všechna bezpečnostní opatření na filtrování obsahu obcházet. Bohužel v tomto ohledu mnohdy bezpečnostní opatření a moderování obsahu je o krok pozadu.

Jak se chránit před škodlivou reklamou

1. Prvním krokem ke zvýšení bezpečnosti je vždy to, že víte o daném riziku. Už jen to, že jste si přečetli tento článek, je jedním z preventivních opatření, abyste se nestali obětí.
2. Používejte renomovaný blokátor reklam. Pokud se vám žádné reklamy nezobrazí, nemohou vás ani ty infikované ohrozit. Blokátor samozřejmě není všemocný. Neumí zablokovat například sponzorované příspěvky na sítích nebo ve srovnávacích cen.
3. Dávejte si pozor na různá vyskakovací okna, žádosti o povolení a další nežádoucí chování prohlížeče.

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **90** ze dne **19.11.2024**

4. Aktualizujte svá zařízení a programy v něm. Některé zranitelnosti lze snadno zneužít a usnadnit tak práci hackerům.
5. Používejte silné bezpečnostní řešení s ochranou v reálném čase.
6. Buďte skeptičtí. Zejména pokud reklama nabízí drahý produkt za nezvykle nízkou cenu, pohádkové zbohatnutí nebo jiný zázrak na počkání.
7. Než zadáte na webové stránce svoje osobní údaje nebo údaje z karty, zkontrolujte, zda se jedná skutečně oficiální stránku.
8. Malvertising ve vyhledávačích je pro kyberzločince jen další cestou k šíření hrozeb. Útočníci umí být velmi kreativní. Buďte ostražití a dávejte pozor, protože i ta nejlákavější nabídka může někdy skrývat nečekané nebezpečí.

Zdroj: AVcentrum ČR