**Microsoft, Google, Apple. Cyberprzestępcy podszywają się pod gigantów technologicznych.**

**Microsoft, Google oraz Apple to marki, pod które cyberprzestępcy najchętniej podszywali w swoich próbach kradzieży danych osobowych i uwierzytelniających – donosi Check Point Research. Wizerunek trzech amerykańskich gigantów technologicznych pojawiał się w ponad połowie kampanii phishingowych w drugim kwartale 2023 roku.**

W drugim kwartale roku Microsoft stał się marką, pod którą najczęściej podszywali się cyberprzestępcy. Wcześniej, pierwszym kwartale 2023, zajmował trzecie miejsce w niechlubnym rankingu. Wizerunek firmy z Redmond odnotowany był w 29 proc. wszystkich prób tzw. brand phishingu. Wynik ten można częściowo wytłumaczyć kampanią phishingową, w ramach której hakerzy atakowali posiadaczy kont za z wykorzystaniem fałszywych wiadomości dotyczących nietypowej aktywności na ich koncie – zaznaczają autorzy raportu z firmy Check Point.

Na drugim miejscu znalazł się Google, którego wizerunek wykorzystany został w 19,5 proc. wszystkich prób, a na trzecim Apple, z 5% wszystkich zdarzeń phishingowych w ostatnim kwartale. To właśnie pod branżę technologiczną najczęściej podszywali się przestępcy. W dalszej kolejności była to bankowość oraz sieci społecznościowe.

*- Marki, pod które podszywają się cyberprzestępcy, zmieniają się z kwartału na kwartał, jednak stosowane taktyki już niekoniecznie. Dzieje się tak dlatego, że metoda zalewania naszych skrzynek pocztowych przy jednoczesnej próbie upewnienia nas w fałszywym poczuciu bezpieczeństwa z pomocą renomowanego logo wielokrotnie okazywała się skuteczna* – mówi Omer Dembinsky, Data Group Manager w Check Point Software.

Na początku roku analitycy Check Point Research ostrzegali przed tendencją wzrostową wykorzystania branży finansowej w atakach cybernetycznych. Również w drugim kwartale był to intensywnie eksploatowanych przez hakerów sektor. Przykładowo amerykański holding finansowy Wells Fargo zajął czwarte miejsce w zestawieniu z powodu serii złośliwych e-maili z prośbą o potwierdzenie informacji o koncie. Podobną taktykę zaobserwowano w innych oszustwach imitujących marki, takie jak Walmart i LinkedIn, które również znalazły się w pierwszej dziesiątce tego raportu, zajmując odpowiednio szóste i ósme miejsce.

- *Powinniśmy poświęcić chwilę przed kliknięciem dowolnego łącza, którego nie rozpoznajemy, i zastanowić się czy czasem coś nie wydaje się nam podejrzane. Możliwe, że w wiadomości pojawiają się błędy lub ma charakter zachęcający do natychmiastowej reakcji. W takim wypadku powinna zaświećiś się nam czerwona lampka* – dodaje ekspert Check Pointa. Podczas ataku phishingowego związanego z marką przestępcy próbują naśladować oficjalną witrynę dobrze znanej marki, używając podobnej nazwy domeny lub adresu URL oraz projektu strony internetowej, który przypomina oryginalną witrynę. Łącze do fałszywej strony internetowej może zostać wysłane do odbiorców za pośrednictwem wiadomości e-mail lub SMS-a. Fałszywa witryna często zawiera formularz służący do kradzieży danych uwierzytelniających użytkownika, szczegółów płatności lub innych informacji osobistych.

**Najpopularniejsze marki phishingowe w II kwartale 2023 r**

1. Microsoft (29%)

2. Google (19,5%)

3. Apple (5,2%)

4. Wells Fargo (4,2%)

5. Amazon (4%)

6. Walmart (3,9%)

7. Roblox (3,8%)

8. LinkedIn (3%)

9. Home Depot (2,5%)

10. Facebook (2,1%)