WZROST LICZBY CYBERATAKÓW NA USŁUGI CHMUROWE

Cyberprzestępcy posługują się nieznaną do tej pory techniką ataków phishingowych, w ramach której wykorzystują popularne usługi chmurowe, w tym Google Cloud, do podszywania się pod rozpoznawalne instytucje w celu infekowania komputerów.

Dzięki hostingowi w popularnych chmurach, jak Google Cloud czy Microsoft Azure, hakerzy tworzą strony podszywające się pod znane instytucje, które mogą nie wzbudzać podejrzeń nawet wśród ekspertów ds. cyberbezpieczeństwa i w ten sposób infekują komputery – ostrzegają analitycy firmy Check Point, specjalizującej się w sektorze cyberbezpieczeństwa. Dodają, że technikę tę zaobserwowano również w atakach phishingowych, w których do hostowania stron wyłudzających dane wykorzystywane są usługi przechowywania w chmurze.

I tak np. w przypadku jednego z ataków wykrytego przez Check Point hakerzy przesłali na Dysk Google dokument PDF zawierający łącze do strony phishingowej i poprosili użytkownika o zalogowanie się do witryny przy użyciu konta Office 365 lub adresu e-mail organizacji. Po wprowadzeniu danych użytkownik zostawał przekierowany do prawdziwego raportu PDF opublikowanego przez renomowaną globalną firmę konsultingową. W rzeczywistości jednak jego dane logowania trafiły do hakerów. Jako, że strona phishingowa znajdowała się w Google Cloud Storage, nie wzbudzała żadnych podejrzeń, zaś atak udało się wykryć dopiero po wyświetleniu kodu źródłowego witryny.

W tamtej sytuacji Google zablokowało adres URL powiązany z atakiem i zatrzymało projekt hakerski. Eksperci ostrzegają jednak, że liczba tego typu złośliwych ataków rośnie. Dlatego też internauci powinni zwracać szczególną uwagę na podejrzanie wyglądające domeny (np. z błędem w nazwie) lub strony internetowe bez certyfikatu HTTPS, czyli symbolu kłódki wyświetlającego się po lewej stronie paska adresu przeglądarki.

Czytaj też: Koronawirus głównym tematem ataków phisingowych