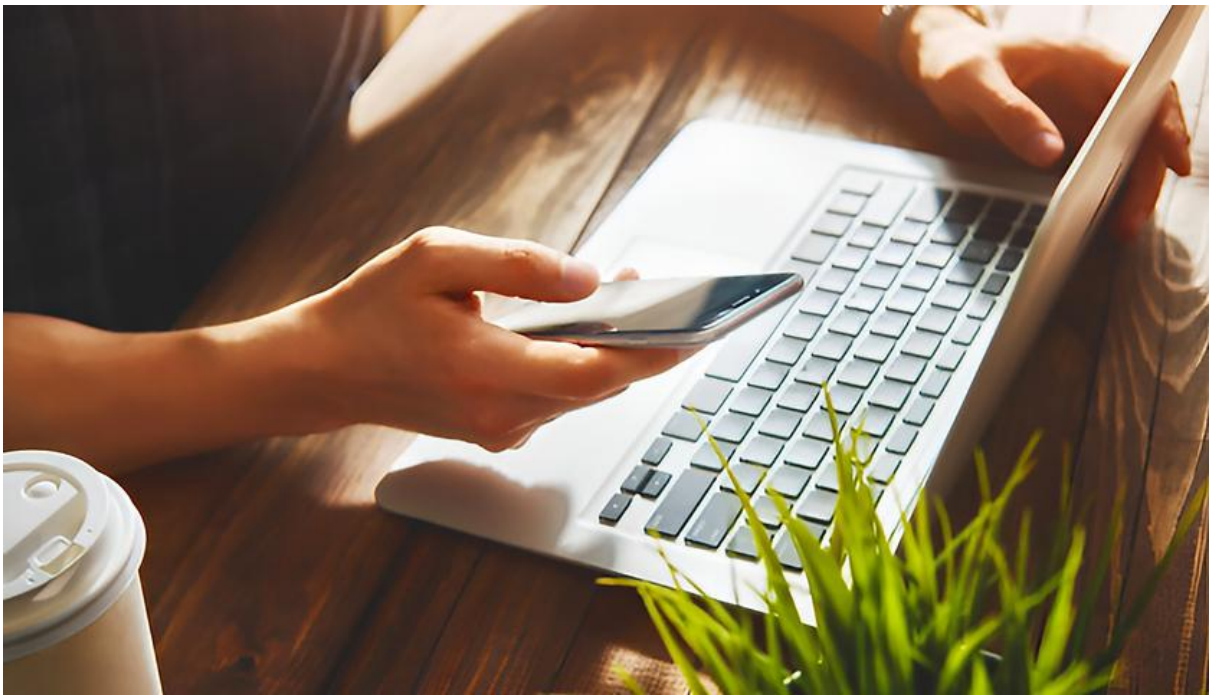
CERT Orange Polska podsumowuje krajobraz zagrożeń pierwszego półrocza. Liczba zablokowanych fałszywych domen wciąż rośnie

Informacja prasowa, 16 lipca 2026



Rekordowe 330 tys. fałszywych domen używanych do wyłudzeń danych lub pieniędzy zablokował w pierwszym półroczu 2026 CERT Orange Polska. To o 30% więcej niż w tym samym czasie ubiegłego roku. Wciąż dominują fałszywe oferty inwestycji, pojawiają się też nowe schematy oszustw. CyberTarcza Orange ochroniła 3,2 mln klientów - próbując wejść na fałszywe strony, otrzymali oni informację, że witryna została wcześniej zablokowana. W ten sposób uniknęli utraty danych lub pieniędzy.

Statystyki z CyberTarczy Orange są zbliżone do ubiegłorocznych - ponad połowa osób próbowała wejść na fałszywe strony z inwestycjami. Obietnice szybkiego zarobku w fałszywych reklamach są niestety nadal skuteczne. Choć scenariusze najpopularniejszych oszustw nie zmieniają się znacząco, pojawiają się także nowe kampanie, które potrafią odbiegać od znanych schematów.

- Cyberprzestępcy są niezwykle elastyczni i dostosowują się do mechanizmów blokujących fałszywe domeny, a automatyczne systemy zapewniają ciągłość działania oszustwa. Stąd naszej weryfikacji podlega coraz większa liczba domen, a profesjonalizacja grup cyberprzestępczych i automatyzacja ich działań wymaga od nas większej precyzji w wychwytywaniu fałszywych domen. Rekordowy wynik blokad potwierdza naszą skuteczność - mówi Robert Grabowski, szef CERT Orange Polska.

Eksperci zauważyli m.in. nowy, nieznany wcześniej schemat oszustwa poprzez SMS. Podszywając się np. pod firmę kurierską, cyberprzestępcy dążą do tego, by przejąć dostęp do konta ofiary na WhatsApp i wykorzystać je do dalszych oszustw,

w tym „na kupującego”. Do tej pory kampanie z takim podszyciem zmierzały do wykradzenia danych z karty ofiary lub poświadczeń logowania do banku.

- Im bardziej ufamy i się spieszymy, tym łatwiej przeoczyć fałszywy link w komunikatorze czy SMS-ie, który prowadzi nas w ręce oszustów. Stąd jako odpowiedź przygotowaliśmy aplikację CyberTarcza Go, której zadaniem jest zatrzymać użytkownika smartfona w porę i uchronić go przed wejściem na złośliwą stronę. Narzędzie dostarcza też aktualnej wiedzy na temat cyberzagrożeń - dodaje Robert Grabowski.

Firmowe bezpieczeństwo

Firmy i instytucje powinny zwracać uwagę na podatności, aktualizacje i bezpieczeństwo infrastruktury. Obserwowane przez ekspertów incydenty jednoznacznie wskazują na przyspieszoną eskalację cyberzagrożeń, w której czas reakcji obrońców staje się kluczowy. Automatyzacja ataków wspierana przez duże modele językowe umożliwia np. przejmowanie środowisk chmurowych w czasie liczonym w minutach, nawet przy ograniczonym udziale człowieka po stronie atakującej. Nie brakuje też wyrafinowanych kampanii wymierzonych w firmowe dane. Cyberprzestępcy znacząco skrócili drogę od podatności do przejęcia całkowitej kontroli operacyjnej nad systemem.

Cyberprzestępcy w wakacje nie odpoczywają

Wzmożona aktywność oszustów, którzy liczą na naszą obniżoną czujność w czasie odpoczynku to już niemal standard. Podszycia, fałszywe wiadomości z serwisu do rezerwacji noclegów to od lat element wakacyjnego krajobrazu. W ostatniej kampanii do ofiar trafiały wiadomości zawierające faktyczne numery ich rezerwacji oraz personalia osoby, która ją składała - przychodziły przez komunikatory (np. WhatsApp), a dane nadawcy były zgodne z danymi właściciela miejsca noclegowego. Takie precyzyjne dane w rękach oszustów to wg ekspertów efekt wcześniejszych włamań do serwisu.

W czasie wakacyjnych wyjazdów można się spodziewać oszustw związanych z ofertami kwater, hoteli czy zniżek na bilety lotnicze. Ale nie tylko - odpowiadając np. na niespodziewaną ofertę pracy można stracić konto w mediach społecznościowych, a korzystając z „niezwykle atrakcyjnej promocji” zapłacić za towar, który nie istnieje.

- Bądźmy rozsądni i uważni, zadbajmy o swoje dane, nie działajmy pochopnie, nie korzystajmy z każdej superpromocji, bo wtedy stajemy się łatwym celem - podkreśla Robert Grabowski.

Internauci mogą liczyć na wsparcie zespołu CERT Orange Polska. Wiadomości, które budzą wątpliwość odbiorcy można przesłać na adres cert.opl@orange.com lub SMS-em na nr 508 700 900. To tylko chwila, a może przyspieszyć blokadę potwierdzonych stron phishingowych i pomóc ochronić także innych użytkowników internetu. W serwisie Hasło Alert lub Centrum Bezpieczeństwa w aplikacji Mój Orange internauci mogą sprawdzić, czy nie wyciekły ich dane logowania.

Bieżące ostrzeżenia na stronie cert.orange.pl, a także na Twitterze @CERT_OPL.

Źródło: https://biuroprasowe.orange.pl