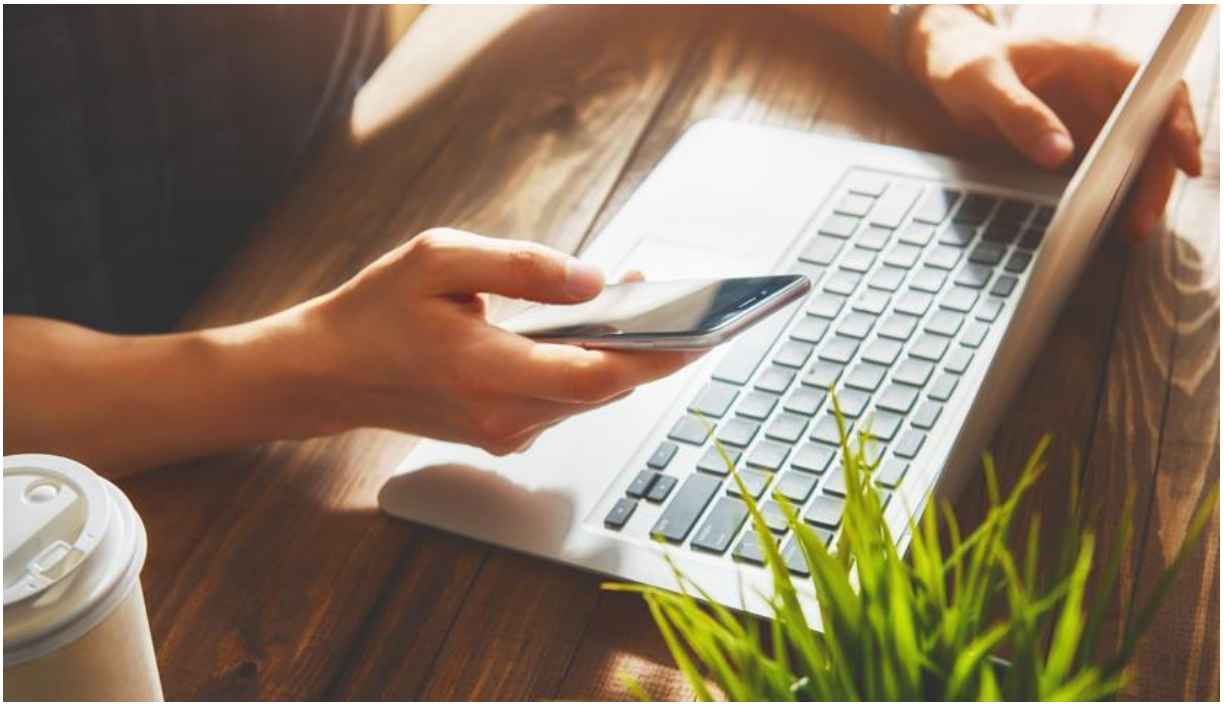
Pierwsze półrocze w sieci wg CERT Orange Polska: fałszywe inwestycje nadal numerem jeden wśród cyberoszustw. Rekordowy atak DDoS.

Informacja prasowa, 08 lipiec 2025



Ponad 250 tys. fałszywych domen używanych do wyłudzeń danych lub pieniędzy zablokował w pierwszym półroczu 2025 CERT Orange Polska. To niemal dwa razy więcej niż w tym samym czasie ubiegłego roku. W czołówce zagrożeń nadal znajdują się fałszywe oferty inwestycji i oszustwo „na kupującego". CyberTarcza Orange ochroniła 3,25 mln klientów. Zespół CERT Orange Polska odparł rekordowy atak DDoS o sile 1,3 Tb/s.

Ponad połowa osób ochronionych przez CyberTarczę Orange próbowała wejść na fałszywe strony z inwestycjami. Obietnice szybkiego zarobku głównie w fałszywych reklamach nieistniejących giełd zamieszczanych m.in. w mediach społecznościowych, wciąż okazują się bardzo skuteczne. Jak zauważają eksperci CERT Orange Polska, cyberprzestępcy wciąż doskonalą metody działania, choć scenariusze oszustw nie zmieniają się w znaczący sposób.

- *Z naszych analiz wynika, że cyberprzestępcy dostosowują się do mechanizmów blokujących fałszywe domeny i projektują automatyczne systemy, które mają zapewnić ciągłość działania oszustwa. Potwierdza to nasze przewidywania odnośnie coraz większej profesjonalizacji biznesu cyberprzestępczego. Zauważamy coraz większą automatyzację i ścisłą specjalizację tych grup na każdym etapie dokonywanego oszustwa* – mówi Robert Grabowski, szef CERT Orange Polska.

Firmy i instytucje też powinny zwracać uwagę na podatności, aktualizacje i bezpieczeństwo infrastruktury. - *W maju odparliśmy największy DDoS w historii polskiego internetu - ponad 1,3 Tb/s. To niewątpliwie rekordowa siła uderzenia, jednak dziś liczy się głównie jego precyzja. Atakujący wykorzystują różnorodne techniki ataku z bardzo rozproszonej,*

zmieniającej się infrastruktury. Takie ataki są często trudniejsze do odparcia i bardziej dewastujące – podkreśla Robert Grabowski.

Cyberprzestępcy nie mają wakacji

Zwykle w czasie wakacyjnych miesięcy eksperci notują wzmożoną aktywność oszustów, którzy liczą na naszą obniżoną czujność w czasie odpoczynku od codziennych obowiązków. Jak co roku można się spodziewać oszustw związanych z ofertami pakietów wakacyjnych, kwater, hoteli czy zniżek na bilety lotnicze. Odpowiadając na niespodziewaną ofertę pracy można stracić konto w mediach społecznościowych, a korzystając z niesamowitej przeceny kupić towar, którego nie ma. - *Bądźmy ostrożni, nie działajmy pochopnie, nie korzystajmy z każdej superokazji, bo wtedy stajemy się łatwym celem* – dodaje 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.

Warto śledzić bieżące ostrzeżenia na stronie https://cert.orange.pl/, a także na Twitterze @CERT_OPL.

Źródło: blog Orange Polska https://biuroprasowe.orange.pl