Cyberdefence 24

aut. Szymon Palczewski 28.10.2020

FIKCYJNA FAKTURA Z WIRUSEM. ALARM DLA KLIENTÓW ORANGE POLSKA

Cyberprzestępcy rozsyłają wiadomości phishingowe, w których podszywają się pod Orange Polska. Hakerzy naśladują e-maile z fakturami od operatora, aby skłonić użytkowników do pobrania zainfekowanego pliku. Zainstalowanie wirusa na urządzeniu ofiary umożliwia kradzież danych logowania do witryn bankowości elektronicznej.

W ramach najnowszej kampanii cyberprzestępcy chcą wykorzystać koniec miesiąca jako okres rozsyłania do klientów Orange Polska faktur za usługi. „Przestępcy znów podszywają się pod naszą firmę, załączając zamiast prawdziwych dokumentów złośliwe pliki zawierające bankera ZLoader" – ostrzega CERT operatora.

> Znów podszywają się pod nasze faktury, uważajcie i ostrzeżcie tych, co do których uważacie, że trzeba.https://t.co/dLXAdekX6p
>
> — CERT Orange Polska (@CERT_OPL) October 26, 2020

Firma apeluje do wszystkich klientów, aby zachowali szczególną ostrożność podczas odbierania korespondencji online. Każda wiadomość pochodząca od Orange Polska posiada „Strefę Bezpieczeństwa", która informuje użytkownika o konieczności upewnienia się, że e-mail rzeczywiście pochodzi od operatora.

W przypadku, gdy w otrzymanej wiadomości nie ma konkretnych personaliów lub jeśli są fikcyjne bądź numer ewidencyjny jest inny, niż ten na poprzednich fakturach, nie należy otwierać żadnego załącznika zamieszczonego w e-mailu.

„Jeśli nie macie pewności – zadzwońcie na infolinię Orange Polska, a jeśli jesteście pewni, że macie do czynienia z oszustwem – prosimy, wyślijcie tego maila jako załącznik na adres cert.opl@orange.com" – czytamy w alercie CERT Orange Polska.

Na urządzeniu użytkowników, którzy niestety kliknęli w zamieszczony plik uruchamiane jest makro, pobierające złośliwe oprogramowanie. Zainstalowany wirus następnie „wstrzykuje" zainfekowany kod bezpośrednio do przeglądarki. W ten sposób cyberprzestępcy wykradają bez wiedzy ofiary dane logowania do witryn bankowości elektronicznej.

Phishing. Prosty sposób hakerów

CERT Orange Polska wskazuje, że zazwyczaj cyberatak rozpoczyna się od zainfekowanego e-maila. „To najpopularniejszy wektor ataku" – czytamy w komunikacie CERT-u. Cyberprzestępcy za pomocą

wiadomości wykorzystują metody socjotechniki, podszywając się pod popularne marki (jak np. Allegro) lub samego operatora.

Aby wzbudzić zaufanie ofiary hakerzy często zamieszczają w e-mailu jej dane, takie jak chociażby imię i nazwisko. Wrażenie spersonalizowanej wiadomości ma uśpić czujność użytkowników, tym samym ułatwiając działanie cyberprzestępcom. Rozsądek i ograniczone zaufanie w sieci to podstawa cyberbezpieczeństwa.

> Trafił do Was podejrzany mail? Weszliście na stronę phishingową albo podejrzewacie, że taka jest? Napiszcie o tym na cert.opl@orange.com, pomożecie sobie i wielu innym internautom. Dzięki!
>
> — CERT Orange Polska (@CERT_OPL) March 23, 2020

CERT Orange Polska prosi klientów o zgłaszanie wszelkich podejrzanych wiadomości lub komunikatów. Pozwoli to na skuteczniejszą walkę z cyberprzestępcami, co może uchronić innych użytkowników przed zagrożeniem.

Czytaj też: Kradzież danych użytkowników Forum Play