

Nowa kampania phishingowa po trzęsieniu ziemi w Turcji

08.02.2023

Niecałe 24 godziny po dwóch potężnych trzęsieniach ziemi, które pochłonęły życie tysięcy ludzi w Turcji i Syrii, cyberprzestępcy wykorzystali kryzys humanitarny do przeprowadzenia kampanii phishingowej. Bitdefender Antispam Lab opublikował raport ukazujący, jak bardzo hakerzy potrafią być pozbawieni skrupułów.

Podczas gdy tysiące osób zostało zabitych, a dziesiątki tysięcy innych przeszukuje zniszczone budynki w poszukiwaniu członków rodzin uwięzionych pod gruzami, oszuści starają się wykorzystać hojność ludzi na całym świecie. Sprawcami są przedstawiciele ukraińskiej Fundacji Charytatywnej im. WŁADIMIRA rzekomo zbierającej pieniądze na pomoc osobom dotkniętym klęskami żywiołowymi.

„Uruchamiamy wsparcie dla mieszkańców Turcji i Syrii poważnie dotkniętych trwającym trzęsieniem ziemi, które spowodowało przesiedlenie wielu rodzin i dzieci, pozostawiając je bez dachu nad głową.

FUNDACJA WŁADIMIRA podjęła się niesienia pierwszej pomocy na lądzie, aby pomóc jak największej liczbie osób.

Zachęcamy do wpłat na rzecz ofiar” – brzmi treść mailowej kampanii phishingowej.

Bitdefender ujawnia kulisy zorganizowanego cyberataku

Pierwsza partia próbek analizowana przez zespół Bitdefender Antispam Lab była skierowana do odbiorców w Korei Południowej (49%), Wietnamie (19%), Stanach Zjednoczonych i Indiach (po 7%), Danii (3%), Irlandii (2%) oraz Niemczech i Wielkiej Brytanii (po 1%), przy czym większość fałszywych wiadomości e-mail pochodziła z adresów IP w Pakistanie.

Zgodnie z raportem Bitdefender oszuści wykorzystują fikcyjną ukraińską organizację charytatywną do zwabienia osób, które, kierując się dobrym sercem, chcą pomóc ofiarom trzęsienia ziemi w Turcji i Syrii. Domena obsługująca tak zwaną Fundację Charytatywną im. Władimira została utworzona 3 października 2022 roku i jest już na czarnej liście filtrów antyspamowych Bitdefender.

Ta fałszywa organizacja charytatywna została utworzona oficjalnie w celu pomocy ofiarom rozdarłej wojny Ukrainy. Jednak w ciągu ostatnich kilku dni zmieniła treści na swoich stronach internetowych i otworzyła portfele kryptograficzne na darowizny dla ofiar niszczycielskiego trzęsienia ziemi.

Założyciele fundacji twierdzą, że jest ona „wiodącą internetową platformą zbierania funduszy na pomoc Ukrainie”. Jednak szybka weryfikacja platformy wskazuje, iż na ten cel przekazano tylko 4000 dolarów z darowizn. Z kolei jeden z portfeli kryptograficznych BTC pokazuje starsze transakcje do 100 000 dolarów, których prawdziwy cel jest do tej pory niejasny.

„W Turcji nie zdążył opaść jeszcze pył po ostatniej katastrofie naturalnej, co nie przeszkodziło cyberprzestępcom w natychmiastowym przygotowaniu nowej groźnej kampanii phishingowej. Co prawda te podstępne działania nie są niczym nowym, jednak mogą być skutecznym narzędziem do kradzieży pieniędzy życzliwych osób. Dlatego przypominamy o konieczności weryfikowania, czy zbiórki charytatywne są prawdziwe i stałym korzystaniu z oprogramowania antywirusowego, które zostało wyposażone w moduł antyphishingowy.” - stwierdził Dariusz Woźniak z firmy Marken, dystrybutora rozwiązań Bitdefender.

Źródło: <https://bitdefender.pl/nowa-kampania-phishingowa-po-trzesieniu-ziemi-w-turcji/>

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.

Data udostępnienia: 08.02.2023

Z pozdrowieniami Piotr Rozmiarek

E-mail: piotr.r@marken.com.pl | Tel. bezpośredni: 570 400 019

Informacje o firmie Bitdefender

Bitdefender to rumuński dostawca rozwiązań cyberbezpieczeństwa oraz światowy lider, chroniący miliony użytkowników. Bitdefender jest częstym zdobywcą wielu branżowych nagród i uznaną światową marką. Od 2001 roku konsekwentnie dostarcza najwyższej jakości produkty, służące do zapewnienia bezpieczeństwa zarówno użytkownikom domowym, wielkim korporacjom, jak i rządowym instytucjom. Bitdefender jest znany ze swojej innowacyjności oraz tego, że wyposażają swoje oprogramowanie w

najnowsze technologie takie, jak uczenie maszynowe, heurystyka oraz EDR i XDR.