Bitdefender

Fala oszustw po katastrofie OceanGate

28.06.2023

Wyprawa zmierzającej do Titanica łodzi podwodnej obsługiwanej przez OceanGate Expeditions zakończyła się tragedią dla pięciu odkrywców, którzy postanowili zbadać szczątki liniowca pasażerskiego spoczywającego w głębinach w pobliżu Nowej Funlandii od czasu swego nieudanego dziewiczego rejsu w 1912 roku. Podczas gdy świat w napięciu obserwował desperackie wysiłki odnalezienia łodzi podwodnej Titan i uratowania pasażerów, hakerzy postanowili działać. W ciągu 24 godzin od ogłoszenia przez amerykańską straż przybrzeżną znalezienia szczątków łodzi głębinowej oszuści znaleźli już sposoby na wykorzystanie tragedii, w której zginęło wszystkich pięciu członków ekspedycji.

Kampania phishingowa po katastrofie OceanGate

Od 23 czerwca Bitdefender Antispam Lab śledzi oszustwa wykorzystujące katastrofę batyskafu firmy Oceangate. W pierwszej wersji oszustwa e-mailowego hakerzy podszywają się pod panią

Christine Dawood, której mąż Shahzada i syn Suleman zginęli na pokładzie łodzi podwodnej OceanGate.

Fałszywe e-maile, w większości wysyłane z adresów IP z USA, były kierowane do użytkowników z krajów anglojęzycznych.

E-mail rozpoczyna przedstawienie się „pani Dawood", później następuje wzmianka o jej stracie i rzekomej decyzji o wykorzystaniu ogromnej sumy (18,5 miliona dolarów) zdeponowanej przez jej zmarłego męża w banku w Kanadzie na cele charytatywne.

Wygląda na to, że oszuści wykorzystali artykuły medialne i plotki o stanie zdrowia pani Dawood.

„Szczerze mówiąc, zdecydowałam się przekazać te pieniądze, aby pomóc osieroconym dzieciom lub tym znajdującym się w niekorzystnej sytuacji, ponieważ zdiagnozowano u mnie raka, umieram i nie sądzę, żebym mogła kontrolować ten zły okres w moim życiu" – czytamy w fałszywym e-mailu. – „Niedługo będę miała operację, potrzebuję twojej pilnej odpowiedzi, aby wiedzieć, czy będziesz w stanie wykonać ten projekt. Udzielę ci więcej informacji, w jaki sposób środki zostaną przelane na twoje konto bankowe".

W drugiej wersji oszustwa cyberprzestępcy kontaktują się z użytkownikami, rzekomo w imieniu prawników nieżyjącego już Shahzady Dawooda. Korespondencja ma zapewniać użytkownikom część rodzinnej fortuny i wzywa odbiorców do natychmiastowej odpowiedzi z danymi osobowymi, które pozwolą im zabezpieczyć transfer środków.

W przeciwieństwie do poprzedniej wersji kampanii phishingowej – w tej cyberprzestępcy proszą użytkowników o podanie imienia i nazwiska, numeru telefonu i adresu oraz podanie oddzielnego adresu e-mail, za pośrednictwem którego będą kontynuować rozmowę.

„Chcę, żebyś wiedział, że wszystko zaplanowałem tak, że wyjdziemy z tego zwycięsko. Mam adwokata, który przygotuje niezbędny dokument stwierdzający, że jesteś najbliższym krewnym zmarłego Shahzady Dawooda. Wszystko, czego potrzebujesz na tym etapie, to podanie mi swoich pełnych danych, w tym imienia i nazwiska oraz adresu, aby adwokat mógł rozpocząć swoją pracę" – czytamy w wiadomości phishingowej.

„Po tym jak zostaniesz najbliższym krewnym zmarłego, adwokat wypełni również roszczenia w twoim imieniu, zapewni niezbędną zgodę i zmieni testament na twoją korzyść w celu przeniesienia środków na konto, którego numer podasz. W tej sprawie nie ma żadnego ryzyka, ponieważ zamierzamy przyjąć metodę zalegalizowaną, a adwokat przygotuje wszystkie niezbędne dokumenty"

Tragiczne wypadki i kataklizmy a kampanie phishingowe

Obie wersje oszustw opartych na wiadomościach e-mail wyraźnie ilustrują, w jaki sposób oszuści stale aktualizują swoje taktyki, dostosowując ataki do wykorzystywanych bieżących wydarzeń, dodając nowe zwroty akcji do już istniejących oszustw.

„Trwająca kampania phishingowa związana z wypadkiem OceanGate jest niestety kolejną wersją tradycyjnego systemu opłat zaliczkowych. W tego rodzaju oszustwach ofiary są proszone o przelewanie pieniędzy jako gwarancji bankowych, podatków, opłat prawnych lub innych opłat bankowych, zanim otrzymają to, co im obiecano. Odbiorcy, którzy odpowiedzą na wiadomość e-mail lub podadzą jakiekolwiek informacje kontaktowe, prawdopodobnie zostaną skłonieni do przeniesienia rozmowy do aplikacji obsługującej wiadomości błyskawiczne, takich jak WhatsApp, gdzie oszust będzie próbował przekonać ich do podania poufnych informacji i przelania pieniędzy" – mówi Mariusz Politowicz z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Tragiczne wydarzenia stanowiły w ostatnich latach jeden z najczęściej wykorzystywanych tematów przez cyberprzestępców, od pandemii po wojnę na Ukrainie i kryzys humanitarny w Turcji i Syrii.

Źródło: https://bitdefender.pl/fala-oszustw-po-katastrofie-oceangate/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.
Data udostępnienia: 28.06.2023
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 z zakresu 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, jak i wielkim korporacjom i rządowym instytucjom. Bitdefender jest znany ze swojej innowacyjności oraz wyposażania swojego oprogramowania w najnowsze technologie, takie jak uczenie maszynowe, heurystyka oraz EDR i XDR.