Fałszywe bilety na festiwal Burning Man

ID artykułu: 59562 / 2264

URL: http://www.publikuj.org/59562

26 lutego rozpoczyna się oficjalna sprzedaż biletów na festiwal Burning Man trudne do zdefiniowania, a zarazem niezwykle popularne wydarzenie społecznościowo-artystyczne, które trwa tydzień i odbywa się co roku na pustyni w Nevadzie. Eksperci z firmy Kaspersky wykryli stronę phishingową poświęconą festiwalowi, za pośrednictwem której od końca stycznia realizowano sprzedaż fałszywych biletów za 225 dolarów, czyli dwukrotnie taniej niż w oficjalnej sprzedaży. Phishing rodzaj cyberataku przeprowadzanego w celu zdobycia poufnych danych poprzez podszywanie się pod legalne organizacje to jedna z najpopularniejszych metod wykorzystywanych przez cyberprzestępców w celu gromadzenia danych, które mogą zostać następnie wykorzystane do uzyskania dostępu do kont finansowych ofiar. Całkiem niedawno, bo w IV kw. 2019 r., spośród wszystkich ataków phishingowych, 52, 61% stanowiło próbę załadowania phishingowych stron internetowych stworzonych w celu kradzieży danych finansowych oraz kont w bankach i sklepach internetowych o 9, 42% więcej w stosunku do wcześniejszego kwartału. W atakach phishingowych wykorzystuje się głównie popularne wydarzenia, takie jak festiwal Burning Man, które cieszą się ogromnym zainteresowaniem oraz ograniczoną liczbą biletów (liczba uczestników została ograniczona w zeszłym roku do 80 000).

Dlatego też eksperci z firmy Kaspersky nie byli zaskoczeni, gdy odkryli fałszywą stronę internetową tego festiwalu. Odwiedzającym oferowano możliwość zakupu rzekomo oficjalnych biletów na wydarzenie Burning Man, które w rzeczywistości pojawiają się w sprzedaży dopiero 26 lutego. Ofiary tego phishingu mogą nie tylko stracić kilkaset dolarów, ale również nieumyślnie zdradzić swoje informacje osobowe, takie jak nazwisko, numer telefonu oraz adres e-mail, które posłużą cyberprzestępcom do przeprowadzenia przyszłych ataków.

Strona główna stanowi niemal idealną replikę oficjalnej witryny, jednak po bliższym przyjrzeniu się ujawnia się jej prawdziwa natura: została zarejestrowana 26 stycznia 2020 r. na jeden rok na nazwisko osoby prywatnej. Ponadto, jeśli ofiara pochodzi z Rosji lub kraju Wspólnoty Niepodległych Państw, zostaje przekierowana na lokalną stronę e-waluty, na której zostaje ostrzeżona, że płatność zostanie przekazana osobie prywatnej zamiast podmiotowi prawnemu. Oba te fakty są wysoce podejrzane, zważywszy na to, że Burning Man to projekt na ogromną skalę organizowany przez dużą organizację zlokalizowaną w Stanach Zjednoczonych gdzie rosyjskie firmy obsługujące płatności stanowią rzadkość.

Użytkownicy odwiedzający fałszywą stronę mogą zakupić bilet za 225 dolarów. Zostają następnie przekierowani na bezpieczną stronę płatności, na której mogą podać szczegóły dotyczące swojej karty i zrealizować zakup. Oszuści mogą potencjalnie wykorzystać przekazane informacje osobowe oraz dane dotyczące karty w celu dokonania dodatkowych zakupów na konto właściciela karty lub odsprzedać te informacje innym cyberprzestępcom na czarnym rynku do wykorzystania w różnych szkodliwych celach.

Ataki phishingowe nie bez powodu cieszą się popularnością wśród cyberprzestępców: są stosunkowo łatwe do opracowania, ich ofiarą może paść każdy i przynoszą ogromne zyski. W słowniczku związanym z festiwalem Burning Man znajduje się słowo Obitainium. Oznacza coś przydatnego uzyskanego za darmo. Bilet, który jest znacznie tańszy niż zwykle, to coś, co ufna osoba może uznać za takie właśnie Obitanium. Na to liczą oszuści w tej konkretnej kampanii. Mają nadzieję, że ludzie chwycą przynętę i wydadzą pieniądze na nic. Osobom, które planują wziąć udział w festiwalu Burning Man w tym roku, zalecamy dokładnie sprawdzić, czy strona z biletami jest autentyczna powiedziała Tatiana Sidorina, ekspert ds. cyberbezpieczeństwa z firmy Kaspersky.

Więcej informacji na temat opisywanej kampanii phishingowej znajduje się na oficjalnym blogu firmy Kaspersky Kaspersky Daily: https://kas.pr/f9xj.

Jak nie dać się złapać na phishing Eksperci z firmy Kaspersky przygotowali wskazówki, dzięki którym

użytkownicy mogą uchronić się przed oszustwami phishingowymi:

Nie odwiedzaj stron internetowych, jeśli nie masz pewności, że są autentyczne. Ich nazwy powinny rozpoczynać się od https.

Po wejściu na stronę sprawdź jej autentyczność przyjrzyj się uważnie formatowi adresu URL lub pisowni nazwy firmy, jak również poczytaj recenzje i sprawdź dane rejestracyjne domeny, zanim rozpoczniesz pobieranie.

Monitoruj informacje dotyczące oficjalnej sprzedaży biletów na wydarzenia, którymi się interesujesz.

Subskrybuj newslettery wydarzeń, które są oficjalnym medium informacyjnym i zawierają najnowsze informacje, łącznie ze szczegółami dot. dostępności biletów.

Dowiedz się, ile kosztuje oficjalny bilet, żeby nie skusić się na fałszywkę.

Załóż dodatkową kartę bankową z myślą o zakupach online.

Jeśli otrzymasz odsyłacz od znajomego, który ma rzekomo przekierować Cię na stronę wydarzenia, upewnij się, że rzeczywiście został on wysłany przez tę osobę.

Stosuj niezawodne rozwiązanie bezpieczeństwa, takie jak Kaspersky Total Security, w celu zapewnienia ochrony swoim urządzeniom przed szerokim wachlarzem zagrożeń, łącznie z aktywnością phishingową.

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Kaspersky jako źródła.

Wszystkie informacje prasowe są dostępne na stronie https://www.kaspersky.pl/nowosci.

Piotr Kupczyk
Dyrektor biura komunikacji z mediami, Kaspersky Lab Polska
E-mail: piotr.kup czyk@kaspersky.pl
Tel. 34 390 94 00