Bitdefender

Oszustwa na YouTube – jak nie paść ofiarą?

13.10.2023

Kanały YouTube ze znaczną liczbą subskrybentów są wysoce pożądanym celem dla cyberprzestępców, którzy mogą na nich zarobić, żądając okupu od prawowitego właściciela lub rozpowszechniać oszustwa i złośliwe oprogramowanie wśród subskrybentów. Cykl życia oszustw YouTube rozprzestrzenianych za pośrednictwem głośnych reklam może być różny, ale niezależnie od przypadku hakerzy zwykle postępują według tego samego sposobu – przyciągając swoją ofiarę, wykorzystując znane marki lub osobistości do oszukiwania nieostrożnych widzów. Dlatego zespół Bitdefender przygotował krótki poradnik, dzięki któremu dowiesz się, jak nie stracić swojego konta na YouTube oraz jak nie dać się oszukać przez hakera, który podszywa się pod Twojego ulubionego youtubera.

Jak przebiegają oszustwa na YouTube?

Oszustwa, z którym spotyka się coraz więcej kanałów YouTube, często mają swoje źródło w ukierunkowanych atakach phishingowych.

Cyberprzestępcy wysyłają e-maile przedstawiające możliwości, od współpracy z markami i umów sponsorskich po fałszywe powiadomienia o prawach autorskich z YouTube.

Oszustwo polega na autentyczności wiadomości e-mail. Wiadomość jest przedstawiana jako uzasadniona propozycja biznesowa. Cyberprzestępcy, zwłaszcza ci, którzy atakują popularne kanały, naśladują komunikację od zaufanych zewnętrznych dostawców lub korzystają z adresów e-mail, które nie budzą natychmiastowych podejrzeń.

„Głównym celem osoby atakującej jest nakłonienie odbiorcy do pobrania szkodliwego pliku. Plik ten jest prezentowany jako integralny element współpracy z marką lub ważny dokument. Choć wygląda jak zwykły plik PDF, zawiera złośliwe oprogramowanie, np. Redline Infostealer. To złośliwe oprogramowanie jest znane w niektórych kręgach internetowych i jest przedmiotem handlu na podziemnych rynkach. Jego duży rozmiar, czasami przekraczający 300 MB, został zaprojektowany tak, aby prześlizgnąć się przez wiele standardowych kontroli bezpieczeństwa” – mówi Mariusz Politowicz z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Gdy odbiorca otworzy ten plik, nie ma to natychmiastowych widocznych efektów. Jednak w ciągu zaledwie 30 sekund złośliwy kod zbiera ważne dane z komputera ofiary, koncentrując się na tokenach sesji, plikach cookie i innych cennych informacjach.

Po zebraniu tych danych nawet przy włączonym uwierzytelnianiu

dwuskładnikowym, skradzione tokeny sesji zapewniają atakującemu bezpośredni dostęp do konta YouTube, eliminując potrzebę podawania haseł lub innej weryfikacji. W rezultacie kanał zostaje zagrożony.

Sygnały ostrzegawcze, na które należy zwrócić uwagę w wiadomościach e-mail

- Nieoczekiwane e-maile lub SMS-y, które wyglądają, jakby pochodziły od firmy, którą znasz lub której ufasz.

- E-maile zawierające ogólne powitania, takie jak „Drogi Użytkowniku”, zamiast nazwy/kanału.

- Adresy e-mail, które wyglądają podobnie do prawidłowych, ale mogą zawierać drobne błędy ortograficzne lub inne rozszerzenia domeny.

- E-maile zachęcające do podjęcia pilnych działań za pośrednictwem załączonych łączy lub dokumentów.

- Wiadomości z zauważalnymi błędami ortograficznymi lub gramatycznymi.

- Promocje lub oferty, które wydają się zbyt atrakcyjne lub nieprawdopodobne.

- Nieoczekiwane załączniki do wiadomości e-mail, takie jak pliki PDF

lub pliki .scv (zwykle złośliwe oprogramowanie zamaskowane jako zrzut ekranu), zwłaszcza jeśli nie zostały o to poproszone.

Znaki, które wskazują na to, że Twój kanał YouTube został przejęty

- Nie możesz zalogować się na swoje konto.
- Ustawienia Twojego konta zostały zmienione.
- Twoje zdjęcie profilowe, opis i nick zostały zmienione.
- Filmy, które nie zostały przesłane, pojawią się na Twoim kanale.
- Otrzymujesz powiadomienia o nieznanych urządzeniach lub lokalizacjach, które uzyskują dostęp do Twojego konta.

Wskazówki, które pomogą chronić Twój kanał YouTube przed porywaczami

- Upewnij się, że Twoje konto jest skonfigurowane przy użyciu unikalnego i silnego hasła – nigdy nie powtarzaj haseł, możesz zdecydować się na dedykowaną usługę menedżera haseł, która pomoże w generowaniu bezpiecznych haseł i zarządzaniu nimi do wszystkich Twoich kont online.
- Włącz dodatkowe warstwy zabezpieczeń, takie jak 2FA lub MFA.

- Zachowaj ostrożność podczas korzystania z linków widocznych w sekcji komentarzy do swoich filmów i zainstaluj rozwiązanie antywirusowe chroniące przed phishingiem oraz złośliwymi atakami.

- Natychmiast skontaktuj się z zespołem pomocy technicznej platformy, aby zgłosić podejrzaną aktywność lub wylogowanie z konta.

- Okresowo przeglądaj listę osób, które mają dostęp do Twojego kanału YouTube i upewnij się, że dostęp mają tylko niezbędni użytkownicy, a także ogranicz uprawnienia w oparciu o role i obowiązki.

- Przejrzyj listę aplikacji innych firm połączonych z Twoim kontem i usuń te, których nie używasz. Zachowaj tylko te, które są godne zaufania i niezbędne dla Twojego kanału.

- Rozważ skorzystanie z usług ochrony tożsamości cyfrowej. Usługi te monitorują sieć pod kątem wszelkich naruszeń danych związanych z Twoimi informacjami. Jeśli Twoje dane zostaną naruszone, natychmiast zmień hasła do kont, których to dotyczy.

- Przestrzegaj zasad higieny haseł, zmieniając hasło do konta YouTube co trzy miesiące.

Użytkownicy Internetu również muszą zachować czujność i nauczyć się

rozpoznawać zainfekowane lub podejrzane konta

- Unikaj filmów, które zachęcają do inwestowania w kryptowaluty lub obiecują ogromne zyski z inwestycji w Bitcoin.

- Jeśli oferta lub tytuł brzmi zbyt dobrze, aby mógł być prawdziwy, to prawdopodobnie jest oszustwem! Zatrzymaj się i pomyśl, zanim pochopnie klikniesz w linki, które widzisz w opisach filmów.

- Nigdy nie skanuj kodów QR, które widzisz w filmach promujących bezpłatne rozdania kryptowalut.

- Dokładnie sprawdź kanał pod kątem podejrzanych działań, takich jak brakujące lub ukryte filmy.

- Zwróć szczególną uwagę na sekcję komentarzy w filmach lub transmisjach na żywo – jeśli sekcja komentarzy zostanie zamknięta, może to być oznaką, że oszust chce uniemożliwić bardziej doświadczonym użytkownikom ostrzeżenie innych obserwujących kanał.

- Skorzystaj z rozwiązania antywirusowego z technologią antyphishingową, która wykrywa i blokuje próby phishingu, zanim zdążą zaszkodzić Twoim finansom i tożsamości.

Źródło: https://bitdefender.pl/oszustwa-na-youtube-jak-nie-pasc-ofiara/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.
Data udostępnienia: 13.10.2023
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.