Bitdefender

Nowa kampania phishingowa – hakerzy atakują użytkowników Facebooka i Instagrama

07.04.2023

Począwszy od 4 kwietnia badacze z Bitdefender Antispam Lab wykrywają nową falę wiadomości phishingowych wymierzonych w posiadaczy kont biznesowych Meta. Fałszywe wiadomości rzekomo pochodzące od pracowników Facebooka i Instagrama są skierowane do mieszkańców Ameryki Północnej i Europejczyków.

Twoje konto na Facebooku zostanie usunięta, chyba że…

Jedna próbka spamu przeanalizowana przez badaczy Bitdefender została skierowana do wegańskiej firmy kosmetycznej w USA. Wiadomość e-mail powiadamia właściciela tego przedsiębiorstwa, że jego stronie na Facebooku grozi usunięcie z platformy z powodu naruszenia standardów społeczności Meta.

„Traktujemy te naruszenia bardzo poważnie i musimy podjąć kroki w celu zapewnienia bezpieczeństwa i dobrego samopoczucia naszych użytkowników” – ostrzega fałszywy e-mail. – „Jeśli nie podejmiesz odpowiednich działań, możemy usunąć Twoją stronę z Facebooka”.

Aby uniknąć zamknięcia i usunięcia konta przez Facebook, odbiorca powinien „złożyć roszczenie wzajemne”, klikając osadzony przycisk „Potwierdź”.

Oto, co dzieje się, gdy użytkownik postanowi działać zgodnie z instrukcją oszustów:

1. W pierwszej kolejności napotyka dostosowaną fałszywą weryfikację podobną do CAPTCHA.
2. Po kliknięciu pola „Jestem człowiekiem” i przycisku „Kontynuuj”, użytkownik zostaje skierowany do sfałszowanej wersji strony „Centrum pomocy biznesowej” firmy Meta z prośbą o odwiedzenie innego złośliwego łącza.
3. Link kieruje użytkowników do fałszywej strony internetowej, która zawiera również fałszywy numer raportu. Następnie odbiorca zostaje poproszony o podanie danych osobowych, w tym imienia, nazwiska, służbowego adresu e-mail, osobistego adresu e-mail, numeru telefonu komórkowego i loginu do konta na Facebooku.
4. Po wyrażeniu zgody na „Warunki dotyczące danych i plików cookie” oraz kliknięciu przycisku „Prześlij” odbiorca jest proszony o podanie hasła do konta i kodów bezpieczeństwa MFA, które dadzą hakerom wszystko, czego potrzebują do przejęcia konta.

5. Po przesłaniu wszystkich informacji wyskakujące okienko radzi użytkownikom, aby poczekali, aż ich sprawa zostanie „sprawdzona”, co oznacza, że prawdziwy właściciel konta musi poczekać, aż atakujący zablokuje mu dostęp do strony.

Celem są również użytkownicy Instagrama

Bitdefender Antispam Lab wykrył podobną kampanię phishingową wymierzoną w użytkowników Instagrama za pomocą podobnej fałszywej wiadomości. Jedna z analizowanych próbek została wysłana na konto na Instagramie muzyka reggae, które obserwuje ponad 80 000 osób.

Hakerzy atakują użytkowników Facebooka – jak się bronić?

Próby phishingu rozpoczynające się od groźby usunięcia lub zablokowania kont w mediach społecznościowych to bardzo skuteczna taktyka stosowana przez cyberprzestępców do infiltracji kont w celu rozpowszechniania złośliwego oprogramowania, siania dezinformacji i oszukiwania innych.

„Żadnego ataku polegającego na przejęciu konta nie należy lekceważyć. Jeśli damy się oszukać, przestępcy mogą wykorzystać przejęte konto nie tylko do przechowywania naszych poufnych informacji, lecz także do przeprowadzania kolejnych ataków skierowanych przeciwko naszym znajomym, członkom rodziny lub klientom. Takie działania mogą mieć bardzo negatywny wpływ na naszą reputację i relacje towarzyskie lub służbowe. Dlatego jeśli korzystamy z mediów społecznościowych,

koniecznie musimy zadbać o takie czynniki jak unikalne hasła i odpowiedni antywirus, który zablokuje podejrzane i sfałszowane strony” – mówi Dariusz Woźniak z firmy Bitdefender Systemy Antywirusowe, polskiego oprogramowania Bitdefender.

Aby zapobiec przejęciom kont w mediach społecznościowych, zarówno zwykli użytkownicy, jak i posiadacze kont firmowych powinni:

1. Przestrzegać odpowiedniej cyfrowej higieny.
   Nigdy nie używaj tych samych haseł w różnych serwisach i nie udostępniaj o sobie zbyt wielu informacji w sieci.
2. Zachować czujność wobec wszelkich form niechcianych wiadomości z prośbą o podanie poufnych informacji, haseł oraz kodów 2FA lub MFA.
3. Sprawdzać konta pod kątem powiadomień lub alertów.
   Korzystaj z aplikacji na urządzeniu inteligentnym, zanim wykonasz instrukcje otrzymane pocztą e-mail lub SMS-em.
4. Sprawdzać adres e-mail nadawcy pod kątem nieznanych lub podejrzanych domen.
5. Zachowywać środki ostrożności.
   Zawsze korzystaj z oprogramowania antywirusowego z modułem antyphishingowym, aby blokować złośliwe ataki i łącza phishingowe oraz monitorować wszystkie konta pod względem podejrzanej aktywności.

Źródło: https://bitdefender.pl/hakerzy-atakuja-uzytkownikow-facebooka-i-instagrama/

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

Data udostępnienia: 07.04.2023

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.