Bitdefender

Fałszywy poradnik bezpieczeństwa WordPress używany do wdrażania złośliwego oprogramowania i backdoorów

06.12.2023

Fałszywy poradnik WordPressa krąży po sieci, próbując przekonać administratorów stron internetowych, że zespół ds. bezpieczeństwa WordPressa kontaktuje się z nimi, ponieważ muszą zainstalować łatkę w celu wzmocnienia ochrony ich witryny. Łatka jest oczywiście złośliwym oprogramowaniem, które ma na celu zainfekowanie i przejęcie danej strony.

Wordpress znów pada ofiarą złośliwego oprogramowania

Kiedy zespół ds. bezpieczeństwa WordPress skontaktuje się z Tobą

bezpośrednio, można pomyśleć, że sprawa musi być poważna. Nikt nie chce, aby jego witryna internetowa zawierała lukę w zabezpieczeniach, więc administratorzy witryn mogą skorzystać z okazji, aby wyprzedzić konkurencję i naprawić wszelkie problemy związane z bezpieczeństwem. Problem w tym, że jeśli zainstalują nową „niezbędną" łatkę, to stworzą zagrożenie dla bezpieczeństwa ich strony. Poradnik WordPressa wysyłany przez phisherów jest sfałszowany i wprowadził złośliwe oprogramowanie na swoje strony internetowe.

Badacze bezpieczeństwa z Wordfence odkryli nowe oszustwo typu phishing polegające na wyświetlaniu fałszywego ostrzeżenia dotyczącego nieistniejącego kodu CVE-2023-45124, który rzekomo nęka witryny WordPress.

Jak na ironię, wiadomość dostarczona w wyniku ataku phishingowego ostrzega przed kradzieżą danych.

„Zespół ds. bezpieczeństwa WordPressa odkrył w Twojej witrynie lukę w zabezpieczeniach umożliwiającą zdalne wykonanie kodu (RCE), która umożliwia atakującym wykonanie złośliwego kodu i kradzież Twoich danych, szczegółów użytkownika i nie tylko" – wyjaśniają napastnicy w e-mailu . Na marginesie należy pamiętać, że zarówno „Wordpress", jak i słowo „Wykonanie" zawierają w oryginale literówki.

„Ponieważ pracujemy nad złagodzeniem tej krytycznej luki w zabezpieczeniach w następnej aktualizacji Wordpressa, zachęcamy do natychmiastowego użycia łatki CVE-2023-45124, wtyczki stworzonej przez zespół Wordpress. Wszystko, co musisz zrobić, to po prostu

pobrać, zainstalować i aktywować wtyczkę, aby zapewnić szybką i bezproblemową ochronę bezpieczeństwa Twojej witryny przed potencjalnymi exploitami i złośliwymi działaniami związanymi z tą luką" – głosi treść phishingowego e-maila.

Phishing – jak się przed nim bronić?

Do wiadomości phishingowej dołączony jest link do pobrania, który prowadzi do strony internetowej, która wygląda bardzo przekonująco. Jeśli jest zainstalowana, wtyczka dodaje nowego użytkownika administratora o nazwie „wpsecuritypatch" i ponownie łączy się z serwerem dowodzenia i kontroli za pomocą adresu strony internetowej. Według badaczy wtyczka pobiera również backdoora, menedżera plików, klienta SQL, konsolę PHP i terminal wiersza poleceń.

„W ostatnim roku zaobserwowaliśmy co najmniej kilka groźnych kampanii skierowanych przeciwko właścicielom stron wykorzystujących WordPress. Do najważniejszych elementów strategii ochronnych przed złośliwym oprogramowaniem skierowanym przeciwko Wordpress należy korzystanie z unikatowych i silnych haseł oraz zabezpieczenie urządzeń, z których korzystają administratorzy i moderatorzy stron za pomocą skutecznych systemów antywirusowych wyposażonych w moduły antyphishingowe i antymalware" – mówi Arkadiusz Kraszewski z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Wydaje się, że atak phishingowy nie pochłonął jak dotąd żadnych ofiar i nie jest jasne, co atakujący zamierzają zrobić ze wszystkimi narzędziami

i dostępem. Biorąc pod uwagę poziom dostępu, mogą wykorzystać witrynę do hostowania złośliwego oprogramowania na potrzeby innych ataków, a nawet wprowadzić złośliwe oprogramowanie bezpośrednio na stronę ofiary.

Źródło:https://bitdefender.pl/falszywy-poradnik-bezpieczenstwa-wordpress-uzywany-do-wdrazania-zlosliwego-oprogramowania/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.
Data udostępnienia: 06.12.2023
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.