Bitdefender

Wirus Balada Injector atakuje strony internetowe WordPress

11.04.2023

Szeroko zakrojona, długotrwała złośliwa kampania Balada Injector atakująca strony internetowe WordPress doprowadziła do zainfekowania około 1 miliona witryn od czasu swego powstania w 2017 roku.

Kampania wykorzystuje wszystkie znane i niedawno odkryte luki w zabezpieczeniach motywów i wtyczek Wordpress, aby zamieścić dla systemu Linux wirus backdoor, który umożliwia atakującym uzyskanie nieautoryzowanego dostępu do zainfekowanych stron internetowych. Głównym celem hakerów odpowiedzialnych za tę kampanię jest przekierowywanie użytkowników do fałszywych stron pomocy technicznej, fałszywych wygranych na loterii i fałszywych powiadomień push.

W jaki sposób Balada Injector atakuje strony internetowe WordPress?

Według firmy Sucuri zajmującej się bezpieczeństwem witryn internetowych sprawcy wykorzystują znane luki w kilku motywach i wtyczkach WordPress do zainstalowania backdoora, skutecznie omijając zabezpieczenia i przejmując kontrolę nad atakowanymi witrynami.

Po zainstalowaniu skrypty Balady próbują ukraść krytyczne informacje z zaatakowanych stron internetowych, w tym poświadczenia, dzienniki dostępu, archiwa kopii zapasowych, bazy danych i informacje debugowania.

WordPress, dobrze znany kreator stron internetowych i system zarządzania treścią (CMS), obsługuje ponad 40% witryn internetowych na świecie. Niestety jego popularność, rozległa baza użytkowników oraz ogromna liczba motywów i wtyczek często sprawiają, że staje się wygodnym celem dla cyberprzestępców.

W jaki sposób się bronić?

Niedawno odkryta kampania podkreśla potrzebę wzmocnienia cyberochrony i nawyków promujących bezpieczeństwo, takich jak regularne aktualizacje, edukacja użytkowników i rozpoznawanie zagrożeń, aby zminimalizować ryzyko przyszłych ataków.

Badacze z firmy Sucuri udostępnili wskaźniki kompromitacji (IoC) oraz wskazówki dotyczące identyfikowania i usuwania backdoora Balada

Injector. Jednak użytkownicy, którzy uważają, że ich strony internetowe mogły paść ofiarą złośliwej kampanii, powinni skontaktować się ze specjalistami ds. bezpieczeństwa w celu uzyskania pomocy.

„Ponieważ Balada Injector nadal wykorzystuje luki w zabezpieczeniach motywów i wtyczek WordPress, zespół Bitdefender poleca właścicielom witryn i administratorom zachowanie szczególnej czujności i podjęcie środków ostrożności celem chronienia swoich zasobów. Ochrona informacji i proaktywne podejście do bezpieczeństwa witryn internetowych mogą pomóc użytkownikom zminimalizować potencjalny wpływ obecnych i przyszłych cyberataków" – mówi Mariusz Politowicz z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Źródło:https://bitdefender.pl/wirus-balada-injector-atakuje-strony-internetowe-wordpress/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.
Data udostępnienia: 11.04.2023
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.