Bitdefender

Google ostrzega przed exploitem „Google Calendar RAT”

08.11.2023

Najnowszy kwartalny raport Google dotyczący bezpieczeństwa wzbudził niepokój w społeczności zajmującej się cyberbezpieczeństwem w związku z rosnącym wykorzystaniem przez atakujących natywnych narzędzi chmurowych w celu ukrycia swoich złośliwych działań. Eksperci do spraw cyberbezpieczeństwa zidentyfikowali exploit weryfikujący koncepcję, znany jako „Google Calendar RAT”, który umożliwia wykorzystanie wydarzeń Kalendarza Google do operacji dowodzenia i kontroli (C2).

Nowy odkryty exploit w Google Calendar RAT

Exploit, opublikowany po raz pierwszy w czerwcu w serwisie GitHub, był wielokrotnie rozwidlony, co wskazuje na rosnące zainteresowanie cyberprzestępców. Chociaż nie zaobserwowano żadnych aktywnych ataków, udostępnianie exploita na forach cyberprzestępczych sugeruje,

że napastnicy rozważają jego potencjał.

Odpowiedź Google

Google wydało łatkę, aby przeciwdziałać nowemu zagrożeniu. Jednak Matt Shelton, szef działu badań i analiz zagrożeń w Google Cloud, ostrzega, że „każda usługa w chmurze może zostać wykorzystana przez osobę atakującą do zaatakowania jej użytkowników”, sygnalizując, że może to być początek nowego trendu w cyberatakach.

Mechanizm exploitów w Google

Exploit został odnaleziony przez badacza IT Valerio Alessandroniego i wyróżnia się prostotą, znacznie zmniejszając ilość infrastruktury potrzebnej dla koncentratora C2. Aby skorzystać z exploita, należy wykonać następujące kroki:

- Pobierz credentials.json plik i umieść go w tym samym folderze, co złośliwy skrypt.
- Utwórz nowy Kalendarz Google i udostępnij go kontu usługi Google.
- Edytuj skrypt, aby wskazywał adres kalendarza.
- Uruchamiaj polecenia, korzystając z pól opisu wydarzenia w kalendarzu.
- Po wdrożeniu na zaatakowanej maszynie RAT sprawdza polecenia, wykonuje je i zwraca dane wyjściowe w polu opisu zdarzenia, skutecznie wykorzystując kalendarz jako terminal.

„Prostota i poleganie na legalnej infrastrukturze chmury renomowanych firm sprawiają, że Google Calendar RAT jest szczególnie niebezpieczny i trudny do zidentyfikowania i ograniczenia. Dlatego zawsze warto kierować się zasadą ograniczonego zaufania i na bieżąco aktualizować wszystkie nasze aplikacje” – mówi Dariusz Woźniak z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

W jaki sposób bronić się przed exploitami?

W świetle tych zagrożeń zespół Bitdefender zachęca wszystkich użytkowników usług Google do podjęcia proaktywnych działań w celu ochrony przed RAT i innymi zagrożeniami cybernetycznymi. Zalecenia obejmują:

- Regularne aktualizowanie całego oprogramowania, aby mieć pewność, że zostaną zainstalowane najnowsze poprawki zabezpieczeń.
- Używanie specjalistycznego oprogramowania zabezpieczającego, takiego jak Bitdefender Total Security, do wykrywania i neutralizowania RAT oraz innych zagrożeń cyfrowych.
- Zachowanie ostrożność w przypadku zaproszeń na wydarzenia w kalendarzu i linków z nieznanych źródeł.
- Wdrażanie silnych, unikalnych haseł i rozważenie uwierzytelniania wieloskładnikowego w celu uzyskania dodatkowej warstwy bezpieczeństwa.

- Zdobywanie wiedzy o najnowszych zagrożeniach cybernetycznych i bycie na bieżąco z nowymi aktualizacjami i praktykami w zakresie bezpieczeństwa.

Źródło: https://bitdefender.pl/google-ostrzega-przed-exploitem-google-calendar-rat/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.
Data udostępnienia: 08.11.2023
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.