Bitdefender

S1deload Stealer – nowa kampania, której celem jest kradzież kont na Facebooku i YouTube

24.02.2023

Portale społecznościowe, które zajmują znaczną część naszego życia, od samego początku swego istnienia są wykorzystywane przez cyberprzestępców do wykradania danych oraz infekowania urządzeń niczego niespodziewających się użytkowników sieci. Dlatego zespół Bitdefender postanowił przyjrzeć się nowej globalnej kampanii o nazwie S1ideload Stealer, której celem jest kradzież kont na Facebooku i YouTube.

Dlaczego cyberprzestępcy korzystają z Facebooka i Youtube?

Obecnie media społecznościowe, takie jak Facebook, Instagram i Twitter, mają wielką moc opiniotwórczą i mogą być groźnym narzędziem w rękach cyberterrorystów.

Dysponując dostępem do wielu legalnych kont w mediach

społecznościowych, hakerzy mogą wyłudzać znaczne środki finansowe, a nawet manipulować opinią publiczną, polaryzować społeczeństwa i w efekcie np. zmieniać przebieg wyborów lub inicjować zamieszki.
Ponadto zmotywowane finansowo grupy cyberprzestępcze często tworzą wyrafinowane złośliwe reklamy i kampanie spamowe. W tym aspekcie wykazują się pełnym „profesjonalizmem", ponieważ – aby oszukać swoje ofiary – programują w pełni zautomatyzowane farmy fałszywych stron internetowych. Takie strony służą do udostępniania niebezpiecznych treści w celu kradzieży danych osobowych i kont użytkowników lub sprzedaży i wynajmu już skradzionych kont innym użytkownikom.

S1deload Stealer – nowa kampania cyberprzestępców

Zespół Bitdefender odkrył nową globalną kampanię o nazwie S1ideload Stealer, której celem jest kradzież kont na Facebooku i YouTube.

S1deload Stealer polega na technikach ładowania bocznego bibliotek DLL w celu uruchamiania niebezpiecznych plików. Wirus wykorzystuje legalny podpisany cyfrowo plik wykonywalny, który po kliknięciu ładuje złośliwy kod.

S1deload Stealer skutecznie infekuje systemy, ponieważ sideloading umożliwia omijanie zabezpieczeń. Ponadto plik wykonywalny prowadzi do rzeczywistego folderu obrazu i w ten sposób nie wzbudza podejrzeń internauty. Po zainfekowaniu systemu S1deload Stealer wykrada dane uwierzytelniające użytkownika i przekazuje je cyberprzestępcom.

S1deload Stealer – nowa kampania, której celem jest kradzież kont na Facebooku i YouTube

Bitdefender

W jaki sposób się bronić?

Pomimo tego, że nowa kampania cyberprzestępców jest niezwykle groźna, zespół Bitdefender uspokaja wszystkich użytkowników sieci, ponieważ zgodnie z ich najnowszym raportem produkty Bitdefender wykrywają kod S1deload Stealer i neutralizują potencjalne zagrożenie.

„Najnowsze kampanie phishingowe są niezwykle groźne dla wszystkich użytkowników sieci. Dlatego zawsze przestrzegamy przed otwieraniem podejrzanych plików wykonywalnych pobranych z niezaufanych źródeł. Ponadto powinniśmy pamiętać, aby nigdy nie ignorować alertów oprogramowania antywirusowego" – mówi Mariusz Politowicz z firmy Marken Systemy Antywirusowe, polskiego dystrybutora Bitdefender.

Źródło:https://bitdefender.pl/s1deload-stealer-nowa-kampania-ktorej-celem-jest-kradziez-kont-na-facebooku-i-youtube/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.
Data udostępnienia: 24.02.2023
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.