Bitdefender

Nowa kampania phishingowa – hakerzy podszywają się pod dostawcę gazu

30.01.2023

Specjaliści do spraw cyberbezpieczeństwa z Bitdefender Labs odkryli, że w dniach 13-20 stycznia 2023 roku cyberprzestępcy, podszywając się pod kanadyjskiego dostawcę gazu, wykorzystywali dokumenty programu OneNote do rozsyłania trojana kradnącego dane uwierzytelniające AsyncRat w ramach nowej kampanii phishingowej.

Treść wiadomości e-mail zawierała jedynie krótkie wprowadzenie do faktury w języku angielskim i francuskim oraz zachęcała odbiorców do przejrzenia załączonego pliku w celu uzyskania szczegółowych informacji. Choć wiadomości phishingowe same w sobie nie zawierały żadnej niezwykłej treści, uwagę badaczy Bitdefender przykuł niecodzienny format pliku, który został użyty przez hakerów.

Nowe kampanie Phishingowe – coraz trudniejsze do wykrycia

„Wyraźnie widać, w jaki sposób cyberprzestępcy wykorzystują nowe wektory ataków lub rzadziej wykrywane środki do naruszania bezpieczeństwa urządzeń użytkowników” – powiedział Adrian Miron, menedżer Bitdefender's Cyber Threat Intelligence Lab. „Kampanie te

prawdopodobnie będą się mnożyć w nadchodzących miesiącach, a cyberprzestępcy będą testować nowe sposoby na oszukanie ofiar”.

Co ciekawe, domeny złośliwego oprogramowania hostingowego wykorzystywane w kampaniach złośliwego spamu, przeanalizowane przez specjalistę do spraw cyberbezpieczeństwa Victora Vrabiego, wydają się należeć do Kościoła katolickiego w Kanadzie i dostawcy usług cyfrowych w Indiach. To kolejna klasyczna taktyka stosowana przez hakerów, którzy używają legalnych, zainfekowanych serwerów internetowych do hostowania złośliwego oprogramowania.

Nowa kampania phishingowa była skierowana do internautów mieszkających w Kanadzie, Stanach Zjednoczonych, Wielkiej Brytanii oraz na Węgrzech, przy czym większość wiadomości e-mail pochodziła z adresów IP w Stanach Zjednoczonych.

AsyncRAT to sprytne narzędzie do zdalnego dostępu zaprojektowane w celu ukradkowego umożliwienia atakującemu infiltracji urządzeń docelowej ofiary. Złośliwe oprogramowanie umożliwia łatwe monitorowanie i kontrolowanie zainfekowanych maszyn poprzez przechwytywanie naciśnięć klawiszy, nagrywanie ekranu i zdalne uruchamianie plików.

Cyberprzestępcy wykorzystują funkcje tego narzędzia do kradzieży loginu i poufnych informacji finansowych w celu popełnienia oszustwa lub zainfekowania systemu ofiary jeszcze bardziej niebezpiecznymi plikami zawierającymi oprogramowanie typu ransomware.

W jaki sposób się bronić przed phishingiem?

„Nowe kampanie phishingowe są coraz trudniejsze do wykrycia, dlatego użytkownicy powinni zwracać uwagę na wszystkie podejrzane wiadomości e-mail zawierające niechciane załączniki oraz przestrzegać zasad higieny cybernetycznej i korzystać z oprogramowania

antywirusowego, które zostało wyposażone w odpowiednie moduły antyphishingowe.” – mówi Mariusz Politowicz z firmy Marken, dystrybutora rozwiązań Bitdefender.

Zgodnie z raportem Bitdefender Labs „Wszyscy klienci Bitdefender są chronieni przed AsyncRAT. Załączniki wiadomości e-mail (Invoice_32566.one i Invoice_76562.one) są wykrywane jako Trojan.Generic.33078815 i Trojan.GenericKD.65021348 i natychmiastowo blokowane.”

Źródło:https://bitdefender.pl/nowa-kampania-phishingowa-hakerzy-podszywaja-sie-pod-dostawce-gazu/

Data publikacji: 30.01.2023

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 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, wielkim korporacjom, jak i rządowym instytucjom. Bitdefender jest znany ze swojej innowacyjności oraz tego, że wyposażają swoje oprogramowanie w najnowsze technologie takie, jak uczenie maszynowe, heurestyka oraz EDR i XDR.