Bitdefender

Bitdefender Labs ostrzega przed kampanią phishingową Agent Tesla

31.07.2023

Bitdefender Labs wykryło złośliwą kampanię phishingową próbującą zainfekować użytkowników niesławnym trojanem zdalnego dostępu Agent Tesla. Kampania złośliwego spamu ma na celu przemycenie złośliwego ładunku pod postacią prośby o wycenę (która jest dołączana jako załącznik) od firmy, która wydaje się być południowokoreańską firmą z branży wydobywczej i metalowej. Bliższe przyjrzenie się adresowi dostawy pokazuje jednak domenę dostarczania wiadomości phishingowych podszywających się pod grupę naftowo-gazową w Kazachstanie.

Powrót kampanii phishingowej Agent Tesla

Jak donoszą specjaliści do spraw cyberbezpieczeństwa z firmy Bitdefender, większość ataków pochodziła z adresów IP w Holandii (42%) i Stanach Zjednoczonych (38%). Wiadomości mają wyglądać jak

niepozorny e-mail biznesowy z prośbą do odbiorcy o przekazanie potencjalnemu klientowi lub dostawcy dodatkowych informacji i kosztów poszczególnych towarów oraz usług wymienionych w załączniku. Poniżej zamieszczamy, jego treść.

"Cześć,
jesteśmy firmą handlową z Korei.
Teraz otwieramy nowy kierunek i szukamy nowych dostawców.
Czy możesz przesłać ofertę cenową tych produktów,
cen i warunków pracy?
Czekamy na Twoją opinię.
Dziękuję."

Złośliwy załącznik jest w rzeczywistości dokumentem RTF wykorzystującym lukę CVE - 2018-0802, który zawiera link 3f1f8ef6e454f2631b42c29a0ac1c4aa do zewnętrznego łącza http://87.121.221[.]212/yugozx.doc. Dokument po uzyskaniu dostępu poprosi o pobranie złośliwego oprogramowania Agent Tesla na maszynę ofiary.

Poniżej przedstawiamy wskaźniki kompromisu:
3f1f8ef6e454f2631b42c29a0ac1c4aa
http://87.121.221[.]212/yugozx.doc

Po zainstalowaniu agenta Tesla na zainfekowanej maszynie złośliwe oprogramowanie zaczyna zbierać poufne informacje z systemu, eksfiltrując dane za pośrednictwem protokołu SMTP (e-mail) z powrotem na konto e-mail zarejestrowane wcześniej przez atakujących

lub na konto Telegram.

Infekcje agenta Tesla rozprzestrzeniają się głównie poprzez kampanie phishingowe. Dobrze znany złodziej danych, często widziany w ofertach grup cyberprzestępczych typu złośliwe oprogramowanie jako usługa, jest również znany jako złośliwe oprogramowanie pierwszego etapu ataku, ponieważ trojan zdalnego dostępu zapewnia przestępcom zdalny dostęp do wszelkich zaatakowanych systemów i pozwala im wdrażać bardziej wyrafinowane lub niszczycielskie ataki, takie jak ransomware.

Agent Tesla jest atrakcyjnym wyborem dla cyberprzestępców oraz może być dostarczany w różnych formach załączników, w tym .zip, .cab, .msi, .img i dokumentów Microsoft Office.

Wydaje się, że w tej konkretnej kampanii napastnicy nie włożyli wiele pracy w ton wizualnego szablonu wiadomości, najprawdopodobniej mając nadzieję, że odbiorcy z ciekawości sprawdzą fałszywy załącznik.

Oprogramowanie antywirusowe Bitdefender wykrywa załącznik jako Trojan.GenericKD.68349949.

Jak można chronić się przed kampanią phishingową Agenta Tesli?

„Najlepszym sposobem na ograniczenie i ochronę przed złośliwymi atakami, w tym infekcjami agenta Tesla, jest zainstalowanie na urządzeniu rozwiązania zabezpieczającego, które może wykrywać i blokować rozprzestrzenianie się złośliwego oprogramowania na naszych urządzeniach. Ponieważ trojan zdalnego dostępu ma na celu kradzież

danych logowania z maszyn i umożliwienie atakującym dostępu do poufnych kont i danych, użytkownicy powinni egzekwować MFA (uwierzytelnianie wieloskładnikowe) tam, gdzie to możliwe” – mówi Dariusz Woźniak z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Źródło:https://bitdefender.pl/bitdefender-labs-ostrzega-przed-kampania-phishingowa-agent-tesla/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.
Data udostępnienia: 31.07.2023
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.