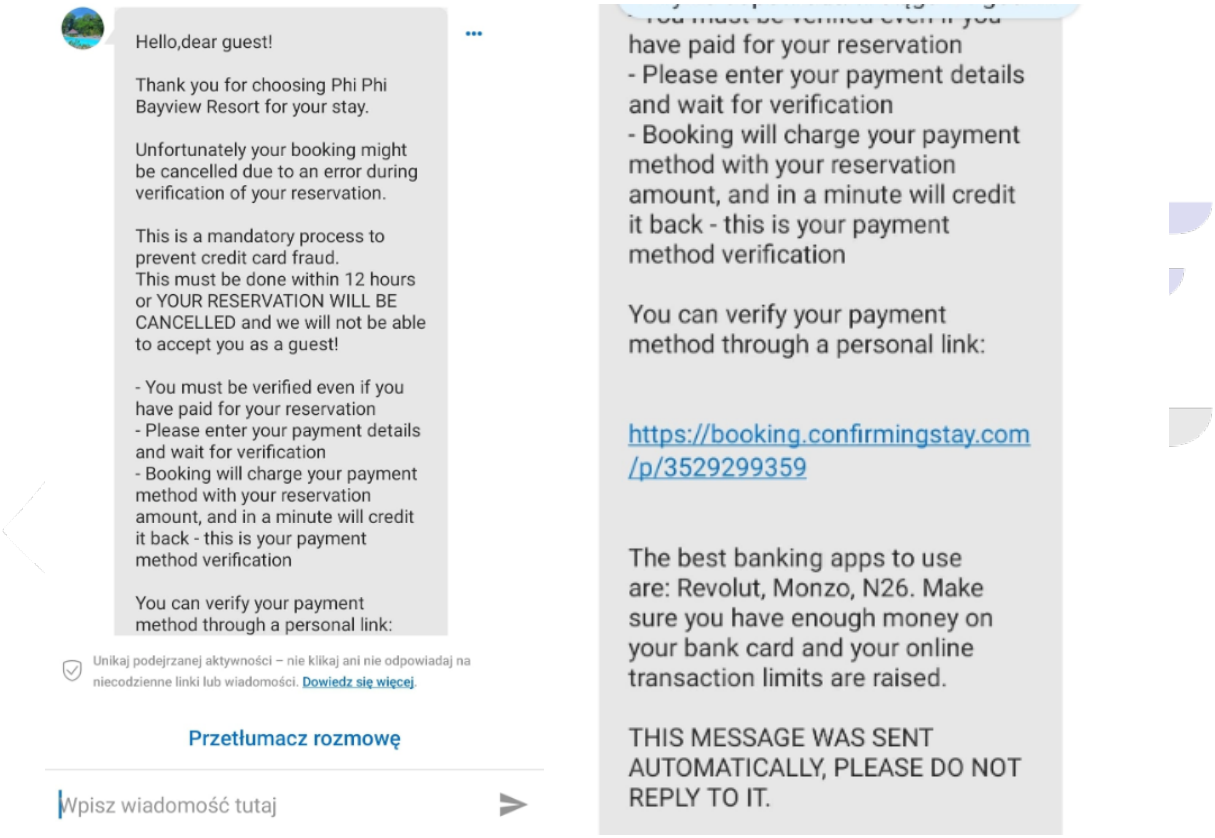
Booking.com – rezerwacja malware

W ostatnim czasie coraz częściej spotkać się można z oszustwami wymierzonymi zarówno we właścicieli hoteli jak i gości hotelowych. Cyberprzestępcy stosują nowe techniki do kradzieży poufnych informacji i pieniędzy. W obliczu rosnącego zagrożenia cyberprzestępczości, właściciele hoteli na całym świecie stają przed nowym wyzwaniem. Ten raport ujawnia metody oraz skalę działania cyberoszustów, którzy do przestępstwa coraz częściej wykorzystują portal Booking.com.

Goście hotelowi – kradzież środków

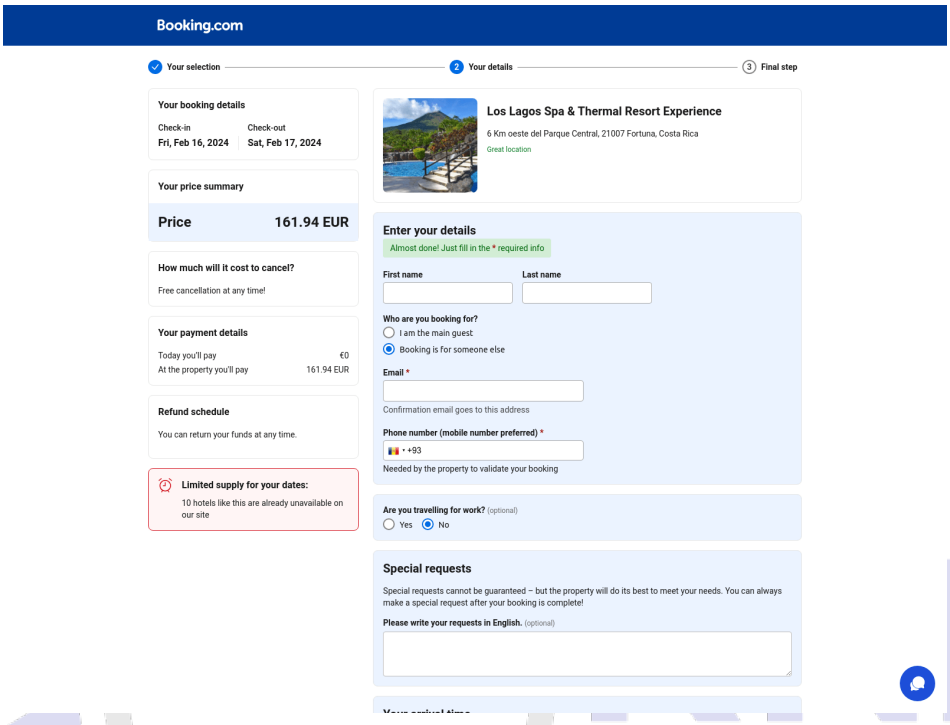
Na początku popatrzmy jak wspominane przestępstwo wygląda z perspektywy oszukiwanego gościa hotelowego. Poniżej sytuacja, w której ofiara otrzymuje wiadomość bezpośrednio przez aplikację w Booking.com, co na pierwszy rzut oka wydaje się wiarygodne. Oszust, podszywając się pod właściciela hotelu, wysyła wiadomość zawierającą link do strony phishingowej. Ta technika jest szczególnie niebezpieczna, ponieważ korzysta z zaufania użytkowników do oficjalnej aplikacji. Link prowadzi do fałszywej strony internetowej, której głównym celem jest kradzież danych karty płatniczej.



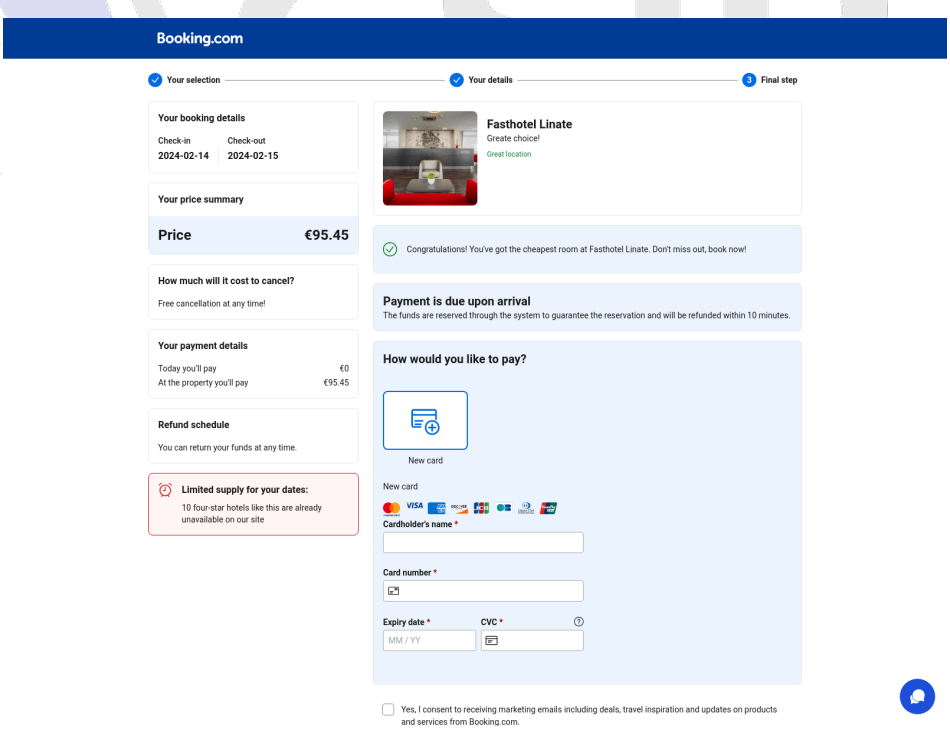
Rysunek 1 Wiadomość od przestępcy w aplikacji Booking.com

Po kliknięciu w link zawarty w wiadomości, ofiara przekierowywana jest na starannie zaprojektowaną fałszywą stronę, która na pierwszy rzut oka wygląda jak oficjalna strona Booking.com. Ta strona to jednak misternie wykonana pułapka – każdy jej element, od układu po szczegółowe grafiki, jest zaprojektowany tak, aby przekonać użytkownika o jej autentyczności. Na tej stronie ofiara proszona jest o podanie danych swojej karty płatniczej, pod pretekstem potwierdzenia rezerwacji lub dokonania płatności za pobyt w hotelu. Niestety, podanie tych danych oznacza, że wpadają one w ręce oszustów, którzy mogą następnie wykorzystać je do nieautoryzowanych transakcji finansowych.

Poniżej przykłady fałszywych stron, podszywających się pod serwis Booking.com:



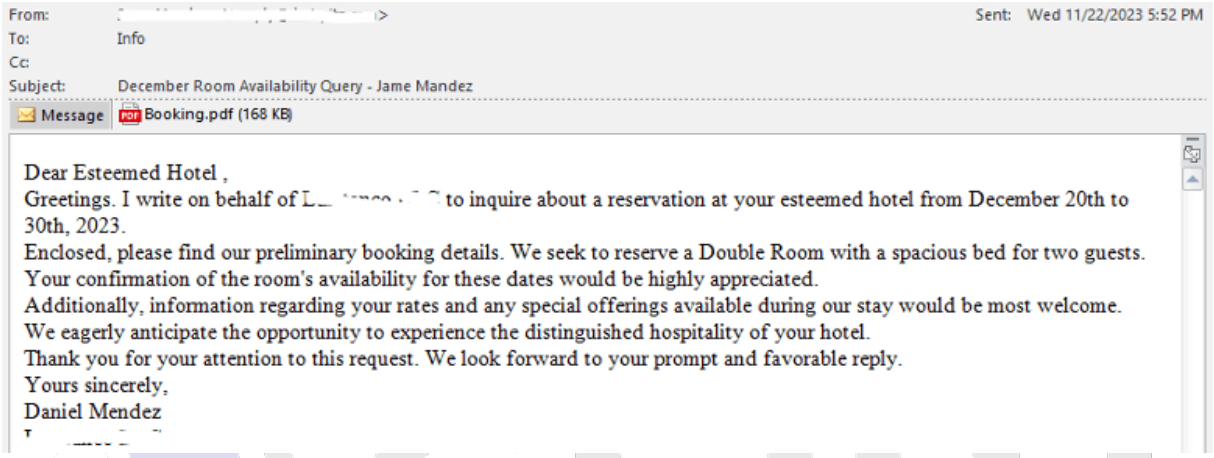
Rysunek 2 Fałszywa strona - hxxps://hotel2491[.]com/p/254753555



Rysunek 3 Fałszywa strona - hxxps://hotel8918[.]com/3dsecure/4278000646

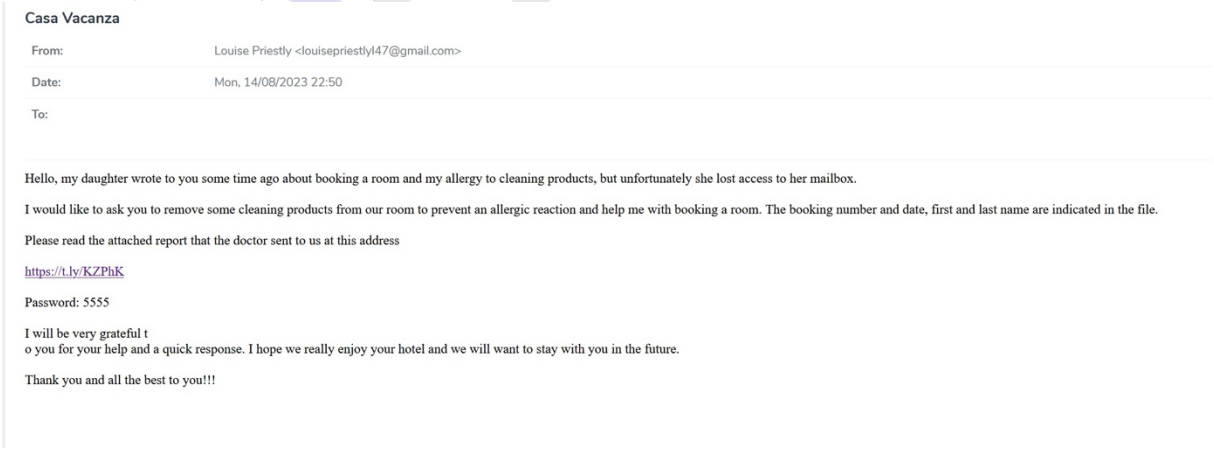
Właściciele hoteli – kradzież danych

Nasuwa się pytanie w jakiś sposób przestępcy uzyskują dostęp do kont hoteli w serwisach takich jak Booking.com. Kluczową metodą stosowaną przez cyberprzestępców jest użycie tzw. 'stealerów' - złośliwego oprogramowania służącego do kradzieży danych uwierzytelniających. Atakujący często wysyłają do hotelarzy zainfekowane wiadomości e-mail lub linki, które, gdy zostaną otwarte, instalują na komputerze ofiary oprogramowanie pozwalające, na kradzież danych logowania. Po przejęciu konta, oszuści uzyskują dostęp do szerokiego zakresu informacji i możliwości zarządzania hotelem na platformie, włącznie z rezerwacjami i danymi klientów.


From: >
Sent: Wed 11/22/2023 5:52 PM
To: Info
Cc:
Subject: December Room Availability Query - Jame Mandez
Message Booking.pdf (168 KB)

Dear Esteemed Hotel ,
Greetings. I write on behalf of L to inquire about a reservation at your esteemed hotel from December 20th to 30th, 2023.
Enclosed, please find our preliminary booking details. We seek to reserve a Double Room with a spacious bed for two guests.
Your confirmation of the room's availability for these dates would be highly appreciated.
Additionally, information regarding your rates and any special offerings available during our stay would be most welcome.
We eagerly anticipate the opportunity to experience the distinguished hospitality of your hotel.
Thank you for your attention to this request. We look forward to your prompt and favorable reply.
Yours sincerely,
Daniel Mendez

Rysunek 4 Fałszywy email ze złośliwym załącznikiem.
Źródło: https://www.fortinet.com/blog/threat-research/mranon-stealer-spreads-via-email-with-fake-hotel-booking-pdf


Casa Vacanza

From: Louise Priestly <louisepriestlyl47@gmail.com>
Date: Mon, 14/08/2023 22:50
To:

Hello, my daughter wrote to you some time ago about booking a room and my allergy to cleaning products, but unfortunately she lost access to her mailbox.

I would like to ask you to remove some cleaning products from our room to prevent an allergic reaction and help me with booking a room. The booking number and date, first and last name are indicated in the file.

Please read the attached report that the doctor sent to us at this address

https://t.ly/KZPhK

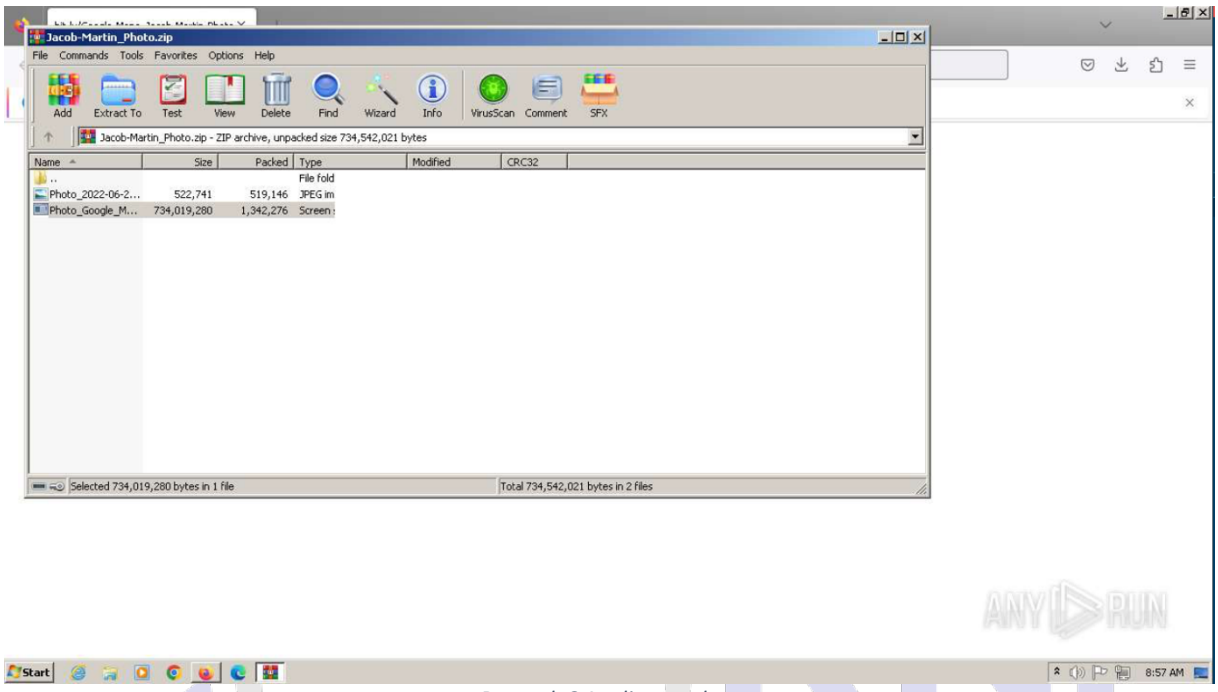
Password: 5555

I will be very grateful t
o you for your help and a quick response. I hope we really enjoy your hotel and we will want to stay with you in the future.

Thank you and all the best to you!!!

Rysunek 5 Fałszywy email ze złośliwym załącznikiem.
Źródło: https://twitter.com/JAMESWT_MHT/status/1691222682698747904/photo/1

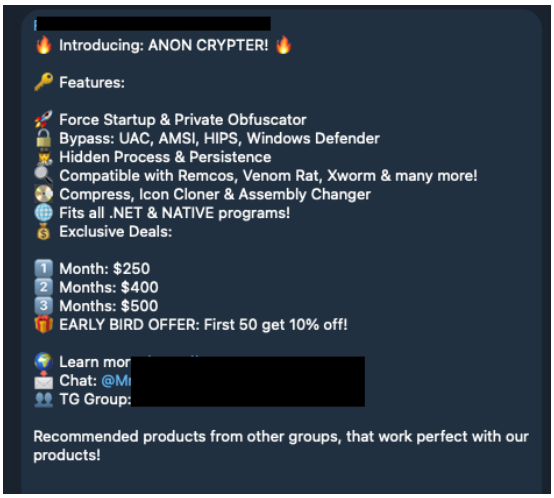
Analiza losowej próbki, przesyłanej przez przestępców w tym oszustwie dostępna jest tutaj: https://app.any.run/tasks/14d062bf-1162-4d06-9a18-1272ab2f43f0/



Rysunek 6 Analiza stealera

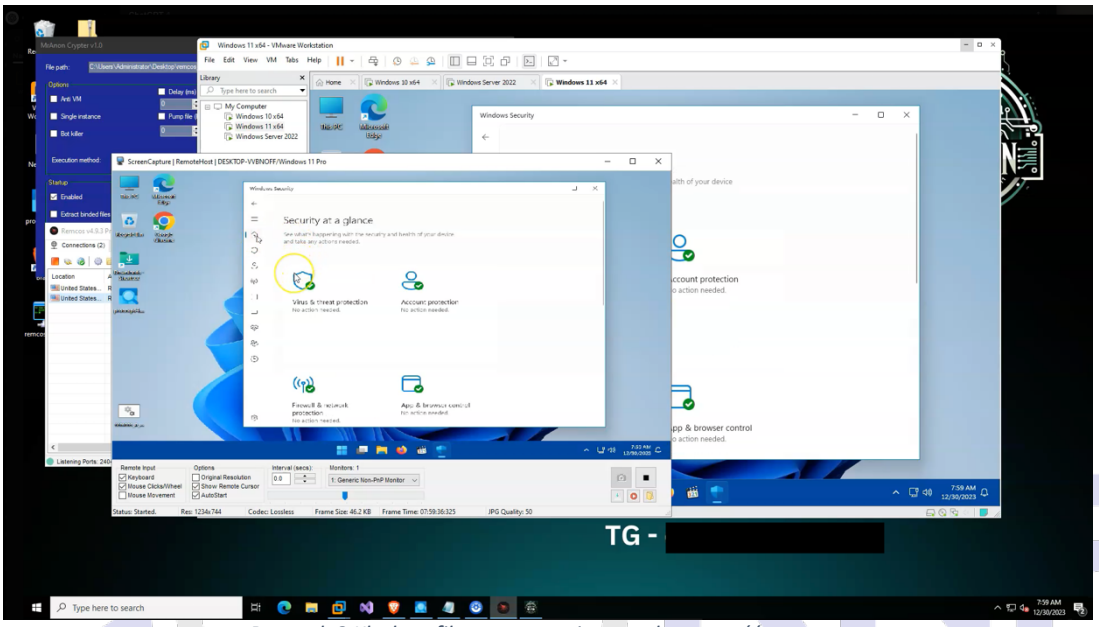
Po udanej instalacji stealera na komputerze właściciela hotelu lub pracownika recepcji, urządzenie to staje się niezauważalnie kontrolowane przez cyberprzestępców. Stealer działa w ukryciu, zbierając cenne informacje, takie jak dane logowania, hasła, informacje o kartach kredytowych i inne poufne dane.

Kluczowym elementem, który umożliwia niezauważalną instalację i działanie tego złośliwego oprogramowania, jest użycie 'FUD Cryptera' (Fully Undetectable Crypter). Narzędzie to jest szczególnie skuteczne podczas pierwszego uruchomienia malware, umożliwiając jego instalację bez wykrycia przez programy antywirusowe.



Rysunek 7 Wiadomość z kanału Telegram

Popularnym narzędziem wykorzystywanym w tych oszustwach stał się crypter od 'Mr. Anon Tools'. Dzięki zaawansowanym technikom szyfrowania, crypter ten zapewnia, że złośliwy plik, na przykład w formacie PDF, zostanie uruchomiony na urządzeniu ofiary bez wykrycia przez standardowe oprogramowanie antywirusowe.

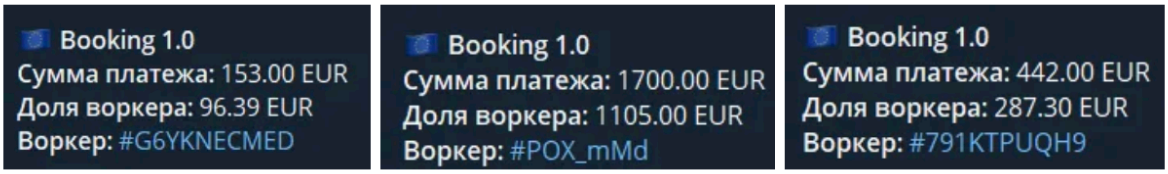


Rysunek 8 Klatka z filmu prezentującego skuteczność cryptera

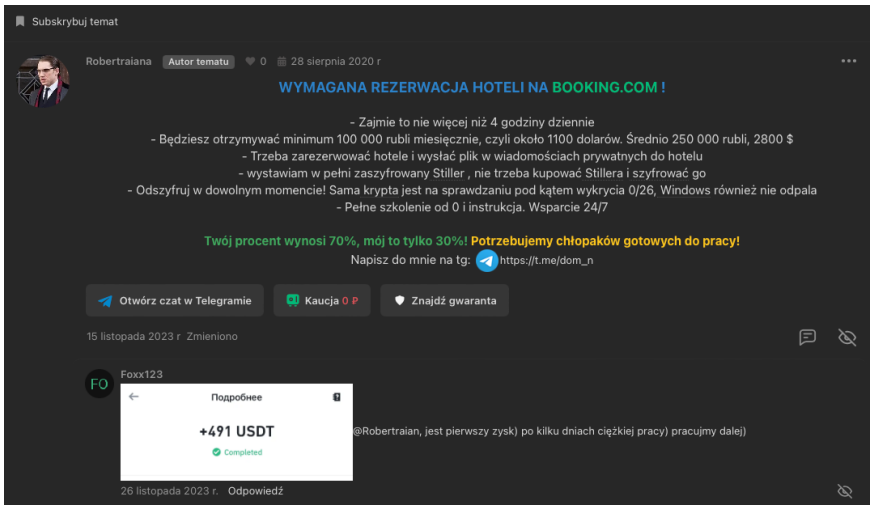
Po tym etapie, stealer może działać w tle systemu operacyjnego, bez wyraźnych oznak swojej obecności, zbierając poufne informacje przez długi czas, zanim właściciel hotelu lub pracownik zauważy jakiekolwiek niepokojące symptomy lub działania.

Kim są oszuści?

Przestępcy zajmujący się tym rodzajem oszustwa wydają się być dobrze zorganizowanymi cyberprzestępcami, którzy specjalizują się w wykorzystywaniu platform rezerwacyjnych hoteli, takich jak Booking.com, do własnych nielegalnych celów. Ich działalność obejmuje tworzenie i rozpowszechnianie stealera — rodzaju złośliwego oprogramowania służącego do kradzieży danych uwierzytelniających — a także wdrażanie skomplikowanych schematów phishingowych, mających na celu wyłudzenie poufnych informacji finansowych od użytkowników platformy.

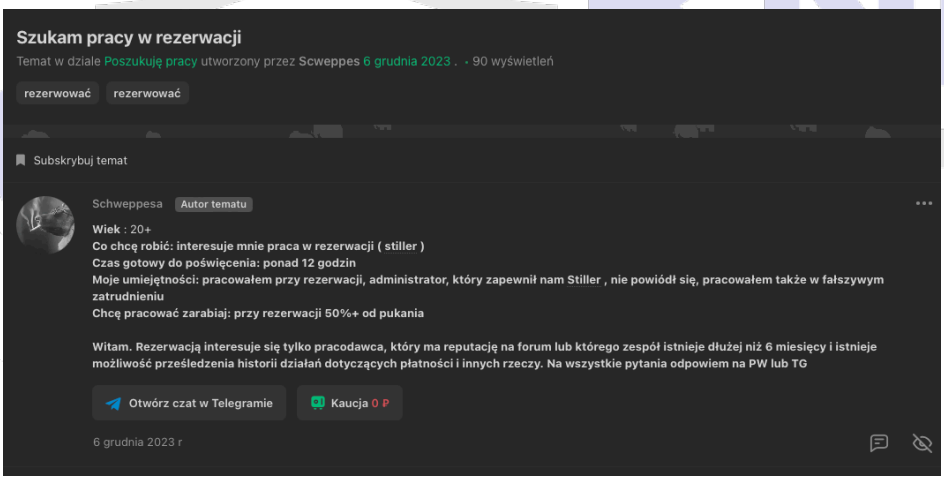


Rysunek 9 Zarobki oszustów.
Źródło: https://g0njxa.medium.com/un-booking-a-scam-8f8058eb7200



Rysunek 10 Oferta pracy przy oszustwach na booking.com

Przestępcy publikują ogłoszenia w poszukiwaniu współpracowników lub osób gotowych wykonać określone zadania w ramach ich nielegalnych operacji, często oferując procent od "udanych" oszustw jako wynagrodzenie. Posługują się otwartymi kanałami komunikacji, takimi jak Telegram czy fora, aby rekrutować nowych członków i koordynować swoje działania.



Rysunek 11 Poszukiwanie pracy przez użytkownika forum przy oszustwach na Booking.com

Oszuści komunikują się w sposób, który sugeruje posiadanie sieci współpracowników i wydają się być częścią większej, zorganizowanej grupy cyberprzestępców. Ich działania nie ograniczają się do pojedynczych ataków — tworzą przestępczy ekosystem, który może mieć wpływ na globalną skalę, stwarzając poważne zagrożenia dla osób fizycznych i biznesów związanych z branżą hotelarską.

Warto dodać, że podobne metody były stosowane w atakach na użytkowników popularnych platform handlowych takich jak OLX, Vinted czy Allegro. Obserwujemy, że te same grupy przestępcze, które skutecznie celowały w użytkowników tych serwisów, teraz przeniosły swoje cyberprzestępcze działania na arenę międzynarodową, wybierając Booking.com jako nowy cel do wykorzystania swoich złośliwych umiejętności.

Jak się bronić?

Cyberoszustwa stają się coraz bardziej wyrafinowane, a hotele oraz ich klienci są atrakcyjnymi celami dla przestępców. Zarówno klienci hoteli, jak i ich właściciele muszą być czujni i świadomi potencjalnych zagrożeń, aby chronić swoje dane i finanse. Poniżej przedstawiamy zestaw najlepszych praktyk, które mogą pomóc w zabezpieczeniu się przed najczęstszymi metodami oszustw, takimi jak phishing, malware i inne techniki wykorzystywane przez cyberprzestępców.

Dla klientów hoteli:

1. Weryfikacja adresu strony: Sprawdź URL strony, na którą zostałeś przekierowany. Upewnij się, że jest to oficjalna strona Booking.com.
2. Podwójne sprawdzanie: Jeśli masz wątpliwości co do autentyczności wiadomości, skontaktuj się bezpośrednio z obsługą klienta Booking.com przez oficjalną stronę lub aplikację.
3. Nie działaj w pośpiechu: Pamiętaj, że pośpiech to zły doradca. Wszystkie płatności wykonuj w dogodnym dla Ciebie momencie – nie dla przestępcy.

Dla właścicieli hoteli:

1. Szkolenie personelu: Regularnie przeprowadzaj szkolenia pracowników z zakresu cyberbezpieczeństwa, aby potrafili rozpoznawać próby phishingu i inne oszustwa.
2. Silne hasła i uwierzytelnianie wieloskładnikowe: Używaj silnych, unikatowych haseł dla każdego konta i włącz uwierzytelnianie wieloskładnikowe, gdzie to możliwe.
3. Regularne aktualizacje oprogramowania: Upewnij się, że wszystkie systemy są regularnie aktualizowane, w tym systemy operacyjne i antywirusowe, aby chronić przed **znanymi** zagrożeniami.
4. Zarządzanie uprawnieniami: Ogranicz dostęp do systemów rezerwacyjnych i danych klientów tylko do autoryzowanych pracowników.
5. Backup danych: Regularnie wykonuj kopie zapasowe ważnych danych, aby w razie ataku móc szybko przywrócić system do działania.