Kampania podszywająca się pod platformę Booking

W związku ze zbliżającym się okresem feryjnym oraz koniecznością rezerwowania miejsc noclegowych dla kilkudniowych szkoleń/ delegacji chciałabym Państwu przybliżyć temat kampanii podszywającej się pod platformę Booking.

Poniżej przedstawiam schemat działania tego ataku:

1. Właściciele hoteli otrzymują fałszywe zapytania rezerwacyjne w formie wiadomości email ze złośliwym oprogramowaniem.
2. Po zainfekowaniu urządzenia, przestępcy kradną dane logowania do platformy Booking.
3. Następnie tworzą fałszywe oferty i strony phishingowe, oszukując klientów hoteli.
4. Fałszywe strony są przesyłane do klientów poprzez Booking lub inne kanały.

Ministerstwo Cyfryzacji opublikowało raport dotyczący tego działania. Zachęcam do zapoznania się z nim:
https://cebrf.knf.gov.pl/images/Booking_-_rezerwacja_malware.pdf

Jak powinni się bronić klienci 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.

Jak powinni się bronić właściciele 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.