RICHTER GUARDIAN

RGSA 10-03-23-01
Date: October 3, 2023

Check-In Safely – Phishing Campaigns Target Hotels and Travel Agencies

INTRODUCTION

The tourism industry is crawling back to pre-pandemic numbers thanks to travel and lockdown restrictions being lifted globally. Unfortunately, cybercriminals have also come up with a new and sophisticated campaign to breach the systems of booking sites, hotels, and travel agencies. Subsequently, the cybercriminals use the systems of the compromised hotel or travel agency to send phishing emails to existing customers.

SUMMARY OF INCIDENT

1. The Entry Point – The campaign starts with the threat actor inquiring about a reservation with the hotel or travel agency. Upon booking the stay, the threat actor uses 'advanced social-engineering techniques' to inquire about specific or special accommodations.

2. Tricking Employees – After establishing a sense of urgency with the hotel employee, the threat actor sends over a URL via email, which supposedly contains crucial documents relevant to their accommodations. The URL provided directs the hotel employee to a genuine hosting site (Google Drive, Dropbox, etc.) and the hotel employee downloads an archive file thinking that it contains important documents.

3. Malicious Executables – The archive file that was downloaded by the hotel employee contained malicious executables (malware) that would infiltrate the hotel employee's computer. From there, the malware operates stealthily to capture login credentials, financial information, and other sensitive data without the hotel employees being aware.

4. New Target – Once threat actors have successfully compromised the hotel's system, the threat actors can move onto using the hotel's communication channel to target legitimate customers.

5. Phishing – The threat actors can now send phishing messages disguised as legitimate requests from the compromised hotel or travel agency. The phishing messages will ask for additional credit card verification from the customer. Since the message comes directly from the booking site through a legitimate communication channel, the customer has no reason to doubt the legitimacy of the email.

HOW TO STAY SAFE

1. Avoid Clicking on Unsolicited Links – Always be skeptical of unsolicited links, even when they originate from a trusted source. Check URLs for any indicators of deception.

2. Take Your Time – Threat actors, phishing emails, and sketchy requests for payments will typically call for immediate action. Take your time to discern any emails that require you to transfer sensitive information.

3. Trust Your Instincts – If you are suspicious about a suspicious email, call the hotel or travel agency directly to confirm that the communication is indeed legitimate.