Waterstons
we're with you

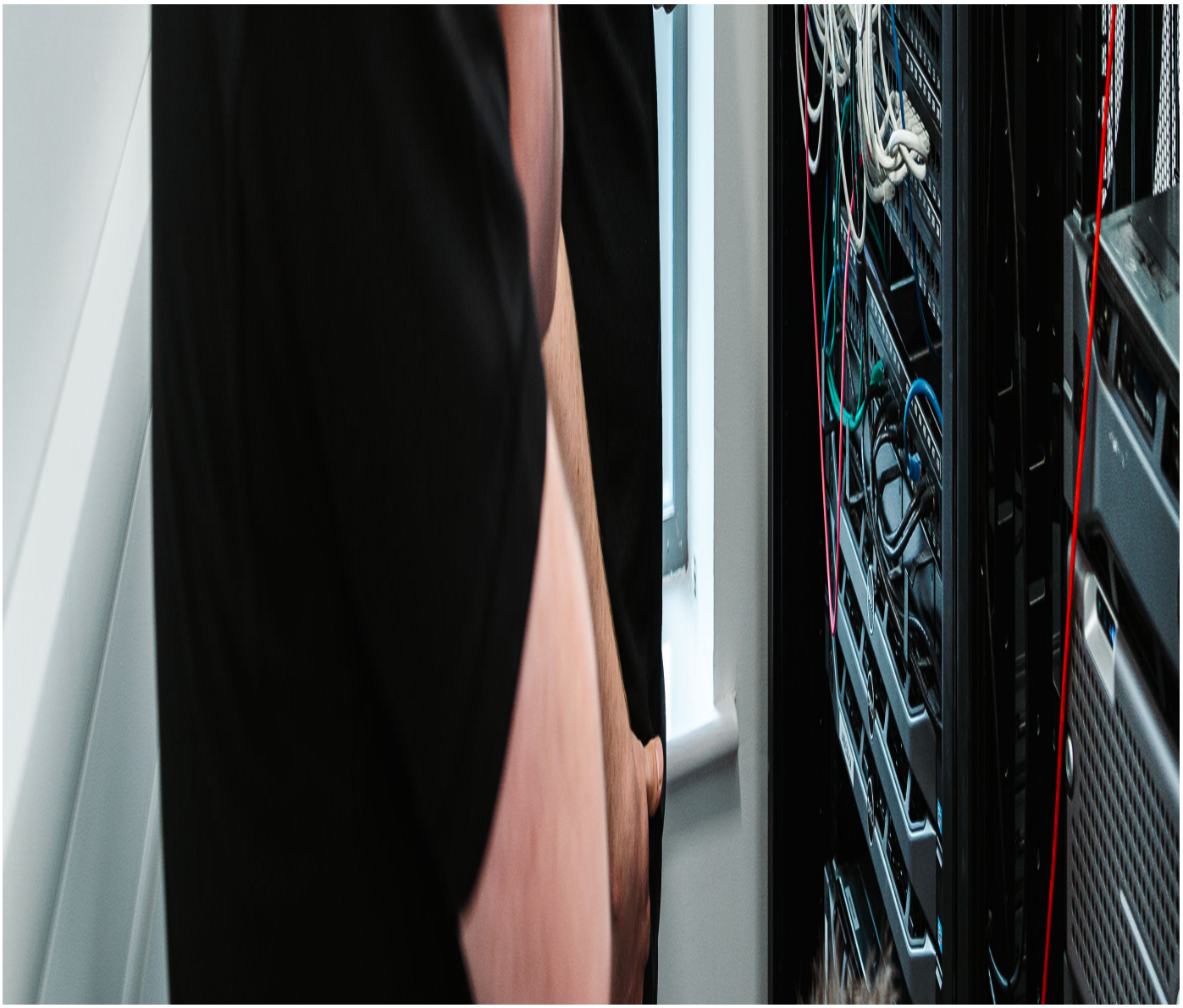
+44 345 094 0945
www.waterstons.com

News article

Dec 2023

Cyber Incident Review

Hotels' compromised Booking.com accounts used in phishing attacks on customers. Read about it here and how your organisation to stay vigilant and protected.



Hotels across the world using Booking.com have been targeted by threat actors attempting to steal their account credentials and carryout subsequent phishing attacks on the hotels' customers.

What Happened

Since March 2023, credentials used by hotels to manage their Booking.com business accounts have been appearing for sale on dark web forums. Hotels have been targeted by phishing emails in which the threat actor impersonates a guest who has left a passport or other item in their room. Once they have established communication with the hotel, the threat actor will send an email which includes a Google Drive link which they claim is a photo of their lost item, however, the link instead downloads malware, typically one of the Vidar, StealC, or Lumma Infostealer malware.

The malware automatically searches the hotel computer to harvest any credentials for its Booking.com account. An alternative version of this attack has the threat actor booking a stay with the hotel, before contacting the hotel by email and eventually sending a link which downloads a malicious file. Once the threat actors have access to the Booking.com credentials they can access the management portal, allowing them to carryout phishing attacks on hotel guests via the Booking.com app, and access guest email addresses for further phishing attacks.

It appears that the Booking.com accounts did not have MFA implemented. Since the threat actors are able to send phishing messages to guests using a hotel's official Booking.com account within the app, the messages appear legitimate, and it is more difficult for customers to identify the scam leading to a higher rate of success. This has led to threat actors offering up to £1,600 on the dark web for any stolen hotel Booking.com credentials.

Wider Implications

This incident highlights the significant risk posed by breaches of organisations' public accounts on third party services such as Booking.com or social media. While breaches of these accounts may not directly lead to any outage of an organisations' systems, or any financial loss, the use of official accounts to carryout social engineering on customers could lead to significant reputational damage. Social media accounts can be a sometimes overlooked weak spot for organisations' account security. Since they are often used by multiple people within the organisation, security controls such as MFA may not be consistently applied and therefore these accounts can become an attractive target for threat actors, who can use them to carryout convincing social engineering attacks on customers.

All Organisations Should

• Review the security of accounts on third party services such as social media, to ensure that all available security controls such as MFA have been applied. Where multiple users require access to the account, organisations should ensure that credentials are shared securely using an enterprise password manager some of which can also be used to securely share MFA tokens to improve access.

• Ensure they have implemented basic email and web security such as DMARC and DKIM, as well as internet filtering, to reduce employees' exposure to email and webbased phishing attacks.

• Implement an Endpoint Detection and Response (EDR) solution that is able to detect advanced threats that have infected a user device. These tools can quickly identify and quarantine threats if they are able to bypass the first line of security tooling.

• Ensure that where regular sharing of files via email is required with third parties or customers, secure processes have been implemented to ensure all files are scanned before being opened.

• Facilitate regular staff awareness training to ensure they are aware of how to spot phishing emails. This should include regular updates on the evolving phishing threat and new campaigns.

This article and other fantastic insights are shared in our monthly cyber threat report. You can join the mailing list to receive it here.

Waterstons has 25+ years' experience across the UK and Australia preparing and protection organisations from cyber threats. We are committed to assisting all organisations to stay agile and prepared in today's cyber conscious economy.

Empower your organisation today, get in touch with one of our team members.

info@waterstons.com.au | 02 9160 8430