BIZCOMMUNITY

SA hospitality sector a target for new malware campaign

By Ross Anderson

15 Feb 2024

With a market size of more than $1.3bn, the hospitality industry in South Africa reflects just how popular the country has become as a tourist destination. In 2021, travel and tourism contributed nearly 3.2% to its GDP. This has made hospitality an attractive target for hackers. In light of this, Sophos, a British-based security software and hardware company has warned of a new campaign targeting hotels and other operators in the sector with password-stealing malware.

Source: Cottonbro studio via Pexels

The social engineering aspect of these attacks is significantly more advanced than what has been encountered before. Hackers initially contact the target over email that contains nothing but text, but with subject matter, that service-oriented businesses like hotels, guest houses, and restaurants would want to respond to quickly. Once the target responds to the threat actor's initial email, a follow-up message is sent linking to what the attackers claim are details about their request or complaint.

However, the link contains either a link to a public cloud storage site such as Google Drive or an attachment, both featuring a compromised password-protected file. Typically, the password will be numerals such as '123456' or something similar. When the attached archived documents (which are the supposed proof of the complaint or request for booking) are opened, the malware is triggered which then steals passwords from the business.

Varied subject matter and emotional narratives

Generally, the subject matter can be categorised either as complaints about serious issues the sender claims to have experienced in a recent stay, or requests for information to help with a potential future booking. Sophos has dubbed this the 'inhospitality' malspam campaign considering how the sector is committed to customer service.

Because the files are password protected, the cloud services provider is unable to scan them for malicious content. The unpacked files are also larger than the usual malware, making immediate detection even more difficult.

This campaign underscores a critical vulnerability within the hospitality industry – the human element. The attackers' narratives are emotionally charged, designed to get a swift response from staff eager to address guest concerns. Such tactics highlight the sophistication of social engineering techniques used by today's cybercriminals and underscore the necessity for heightened cybersecurity awareness and training within the hospitality sector.

For the South African market, this threat is a reminder of the global nature of cyber risks. Our hotels, from major chains to boutique establishments, must recognise the importance of cybersecurity as an integral component of their operational integrity. More than just protecting their data, those businesses must safeguard their reputation in the eyes of both local and international guests.

Cybersecurity strategies for defense

In response, Sophos South Africa, for example, advocates for a comprehensive cybersecurity strategy that includes regular staff training on recognising and handling suspicious emails, comprehensive email filtering systems, and advanced malware protection tools. Collaboration with cybersecurity experts can provide the insights and support necessary to navigate these challenges effectively.

The 'inhospitality' campaign must serve as a wake-up call for the local hospitality industry. It is a reminder that in the digital age, cyber defences must evolve as rapidly as the threats we face. By fostering a culture of cybersecurity awareness and investing in advanced protection measures, we can shield our businesses from such attacks and mitigate against the threat that this password-stealing malware provides.

ABOUT THE AUTHOR

Ross Anderson, Sophos Business Unit Manager at Duxbury Networking.