Luxury Hotels Remain Major Target of Ongoing Social Engineering Attack

Archived: 2026-04-05 17:59:37 UTC

By: Dylan Duncan

85% of phishing emails from current campaign have come in the last 60 days; Hospitality Industry Still Very at Risk of Advanced Malware Capable of Ransomware Delivery

Cofense Intelligence has been tracking a well-crafted and innovative social engineering attack that targets the hospitality industry to deliver advanced information stealer malware. The campaign employs the use of reconnaissance emails and instant messages to bait hospitality email addresses into a response. Once a conversation has started, the threat actors follow up with a phishing email. This campaign uses social engineering tactics also recently seen during the MGM, Caesars and other luxury hotel resorts breaches.

Overall, the campaign uses several tried-and-true methods to bypass email security infrastructure which puts targets at risk of sophisticated information stealer malware like RedLine Stealer, Vidar Stealer, Stealc, and others, most of which can deploy ransomware after successfully infecting a host.

Key Points

- As of September 22, 85% of the phishing emails seen by Cofense Intelligence have happened in the last 60 days, with September seeing a higher percentage than August. This highlights that this campaign is still active and ongoing. See Figure 5 below for more details.
- The campaign most commonly starts with a **reconnaissance email (See Figure 1 and 2 below)**, also known as a bait email. This is the process of a threat actor sending a non-malicious email used as a way of checking to see if the address is live and responsive. Once the threat actor receives a response to the reconnaissance email, they will then follow up with a **phishing email (See Figure 3 and 4 below)**.
- As of now, the campaign only **targets the hospitality sector, primarily targeting luxury hotel chains and resorts**, and uses lures relative to that sector such as booking requests, reservation changes, and special requests. The lures for both the reconnaissance and phishing emails match accordingly and are well thought out.
- Phishing emails are **successfully reaching intended targets** due to several methods known to disrupt email security analysis and secure email gateways (SEGs). These tactics include the use of trusted domains within the malicious URLs in the emails, password-protected archives, and executable files that are so large they can disrupt analysis.
- The **overall goal of the campaign** is to infect employees and systems of hospitality organizations with advanced information stealer malware. The malware varies but the most used in this campaign are Vidar Stealer, RedLine Stealer, and Stealc.

A High-Risk and Well-Crafted Social Engineering Attack

From the reconnaissance email, all the way to the malicious payload, this campaign and its infection chain are both highly sophisticated and well thought out by the threat actors. As of this report, the campaign has only targeted the hospitality sector. Threat actors start by sending a reconnaissance email or an instant message to a hotel, resort, or other hospitality service or employee's email address. These emails, like the examples in Figure 1 and Figure 2, do not contain any malicious content and are just used to test if an email account is live. This example targeted a reservation email address suggesting they were a customer seeking a special medical request for their reservation.

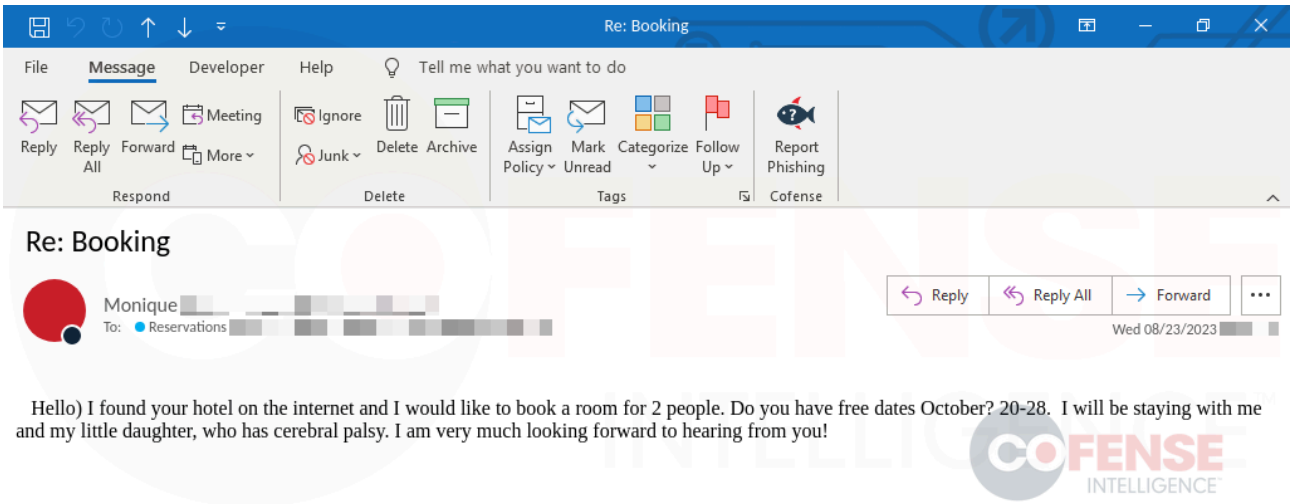

Figure 1: Example 1 - "Reconnaissance" or "Bait" Email used in real phishing example.

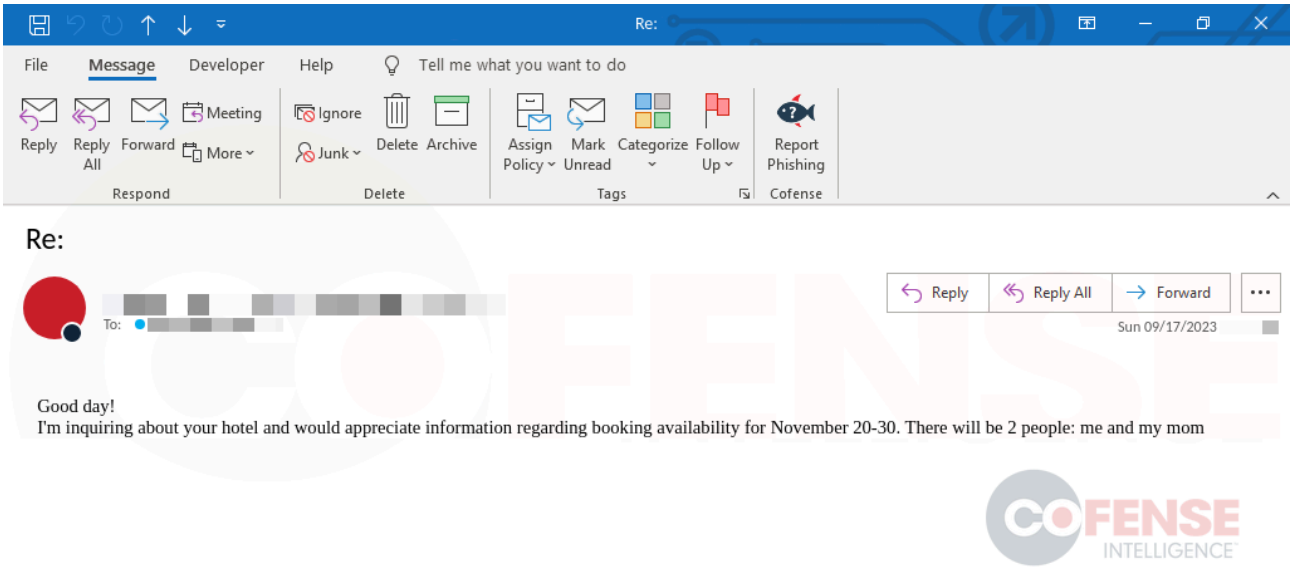

Figure 2: Example 2 - "Reconnaissance" or "Bait" Email used in real phishing example.

Once the threat actor received a response from the reservation email, they followed up the same day with a phishing email sent to the account. The phishing email, shown in Figure 2 and Figure 3, follow the same lure as used in the reconnaissance email. The phishing emails in this campaign start with an infection URL, hosted on a

trusted domain, which is used to download a password-protected archive that contains malicious files. This specific example delivered the Vidar Stealer malware.

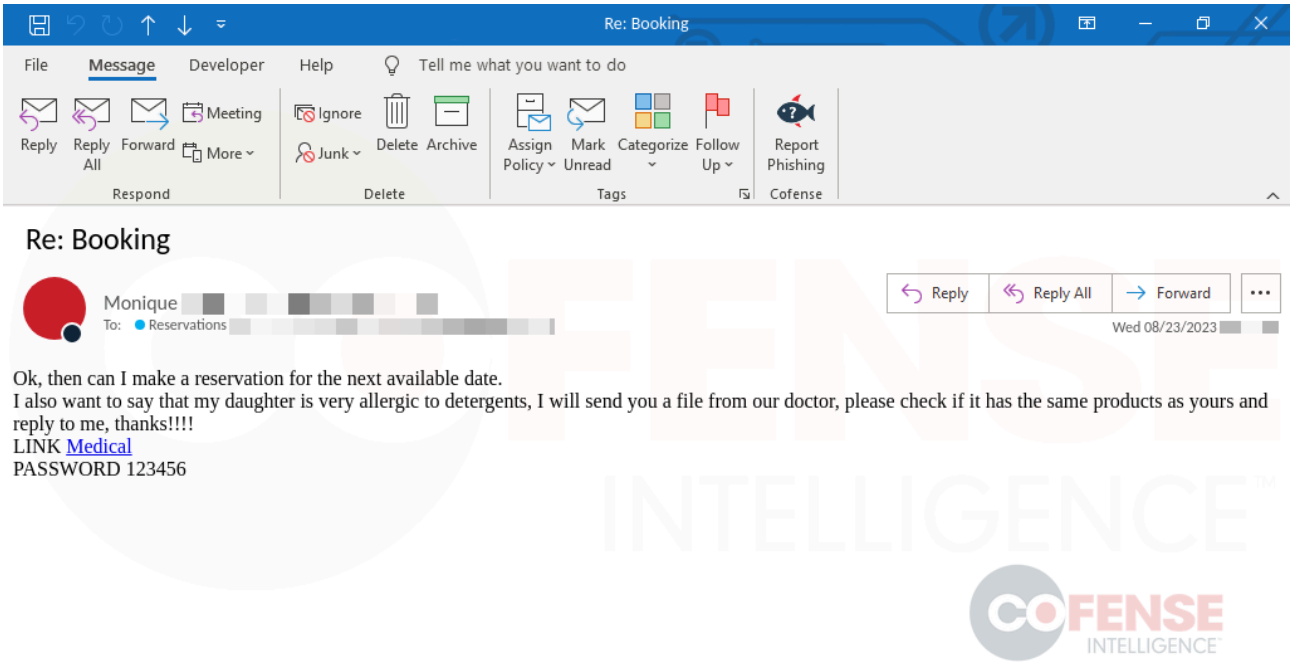

Figure 3: Example 1 - Phishing Email that Followed the Reconnaissance Email.

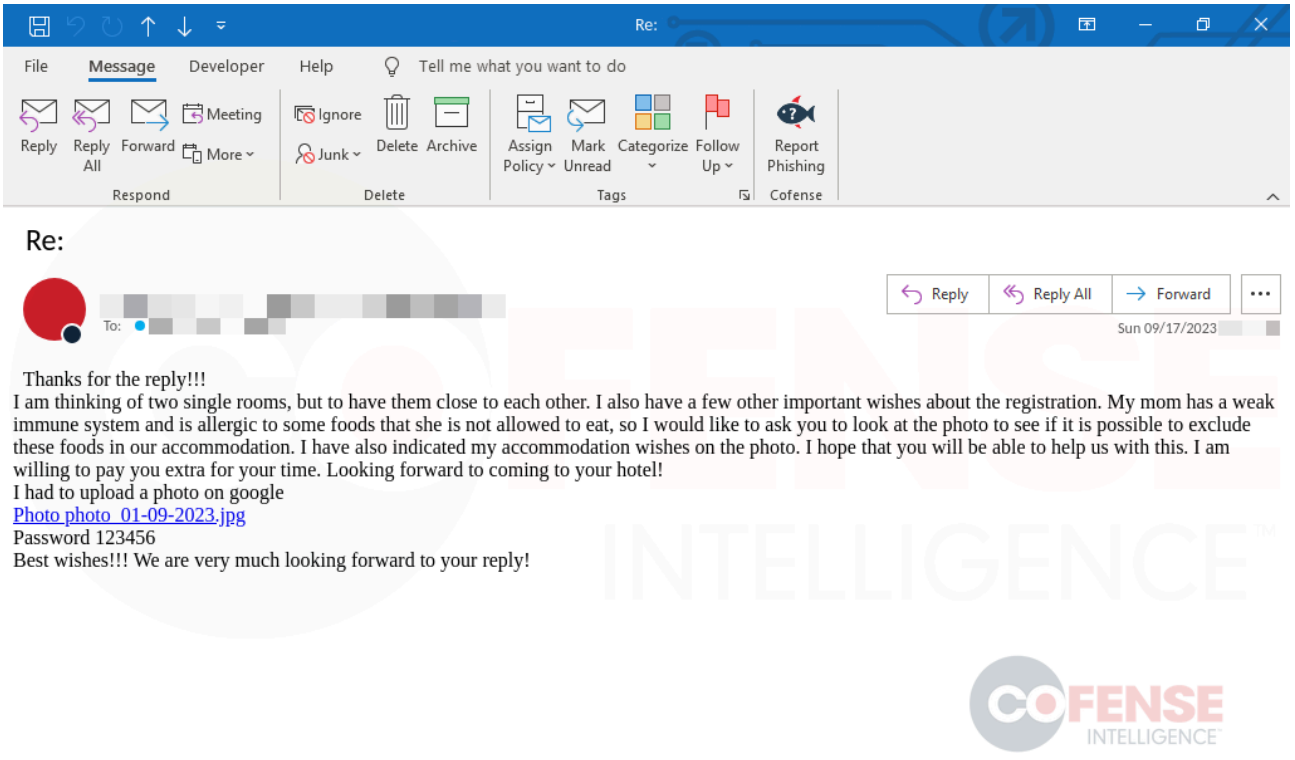

Figure 4: Example 2 - Phishing Email that Followed the Reconnaissance Email.

The emails disseminated by the threat actors behind this campaign all follow unique lures. The following shows a list of lures used in this campaign, each one following the same pattern from the reconnaissance email to the phishing email. The lures all warrant some sort of response from the targeted hospitality organization and are most likely very similar to what the employee is accustomed to seeing, such as a booking request or reservation change.

Hospitality-Themed Phishing Emails

A list of themes used in the social engineering attacks.

- Booking
- Reservation Changes
- Wedding Stays
- Hotel Requests
- Special Accommodations

Successfully Reaching Intended Targets

The attention to detail as well as the tactics, techniques, and procedures (TTPs) used in this campaign go way beyond the average phishing campaign. By utilizing TTPs known to help emails bypass email security options like SEGs, the emails in this campaign are successfully reaching their intended targets. When the campaign uses a reconnaissance email, the email does not contain any malicious indicators so it’s no surprise that those are getting through, however, the phishing emails and instant messages do pose a major threat to targets. Within the phishing emails, threat actors are hosting the malware on trusted domains like Google Drive, Dropbox, Discord app, and others. The abuse of these legitimate sites to host malicious content is common in the phishing threat landscape, but the threat actors also have additional tactics to disrupt analysis.

The infection URL downloads a password-protected archive, relatively small, but contains a very large executable for most of the emails we have observed. The use of a password-protected archive also disrupts analysis as not all security infrastructure can do analysis on files with passwords. In addition, the large file size of the executables (~600MB to 1GB) can also disrupt analysis since most sandboxes and other analysis tools are limited in the size of files that can be scanned. The success of these emails reaching intended targets can be attributed to these TTPs. Figure 5 below shows the volume of the phishing campaign by percentage of the total campaign volume. The campaign has picked up heavily throughout the month of August and has continued at an alarming rate as we have entered September.

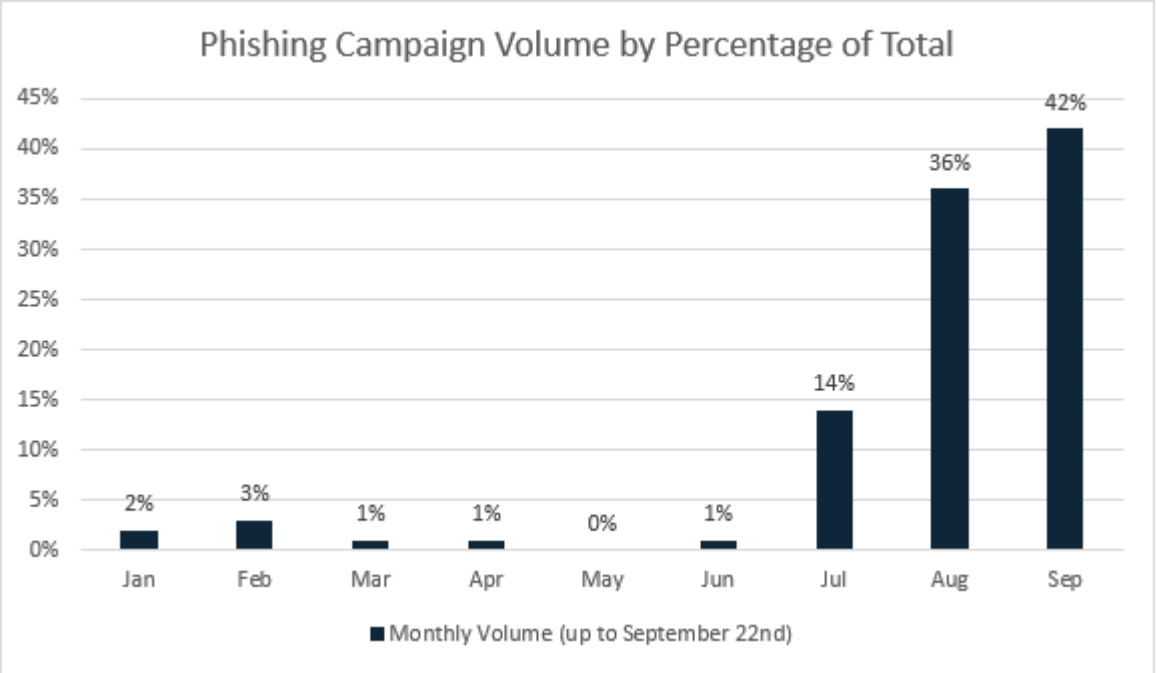

Figure 5: Monthly Campaign Volume by Percentage up to September 22nd.

Figure 6 below is a breakdown of the different domains abused in the campaign. Google Drive makes up more than half of the emails we have seen. Dropbox and Discord app are the next most abused services in this campaign making up a similar percentage. The remaining percentage is made up of 8% using the t.ly link shortener and 6% "other" which is made up of various other services used to host the malware.

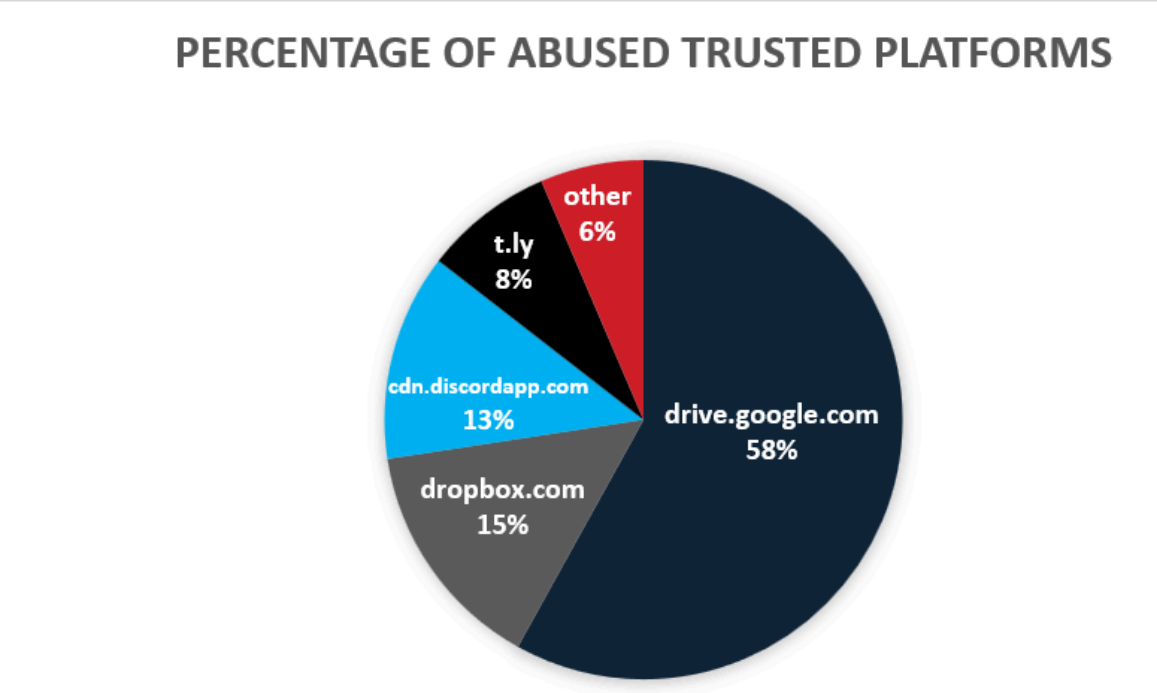

Figure 6: Breakdown of Trusted Domains Abused as Infection URLs to Host Malware.

The infection URLs in the emails all deliver a password-protected archive. The type of archive does change, the threat actors are primarily using ZIP, RAR, and 7-ZIP. As seen in Table 2, a password-protected ZIP archive is the most common archive seen in this campaign.

Archive	Percentage of Emails
ZIP	49%
RAR	32%
7-ZIP	19%

The Final Infection – Advanced Information Stealer Malware

The overall goal of the campaign is to infect hospitality systems and/or employees with information stealer malware. This is a generic malware type used to describe certain malware families. The most common form of information stealer malware generally does just that, steals information. This typically means that the malware steals login information from various applications on the infected host such as passwords stored in browsers. At a more advanced level, some information stealers can deliver additional payloads once successfully planted on a host.

A total of five different information stealer malware families have been utilized in this campaign.

- **Lumma Stealer**, also known as LummaC2, is a subscription-based information stealer that was first seen in 2022. It is written in C and has a wide array of capabilities. This malware is primarily used for stealing cryptocurrency wallets and sensitive information such as usernames and passwords. Lumma Stealer also has the ability to deliver additional payloads.
- **Vidar Stealer** is a well-known information stealer that was first seen in 2018 operating as malware-as-a-service. It is used for targeting a particularly wide variety of information including downloaded or saved sites. The targeted information includes credit card, autofill, and password data stored in local programs and browsers. Vidar Stealer can act as a malware downloader to deliver additional payloads.
- **RedLine Stealer**, first seen in 2020, is probably the most well-known stealer on this list. It uses Simple Object Access Protocol (SOAP) for communication with its command-and-control center and can use a variety of plugins. It's used to collect information from various installed programs including credentials stored in browsers, email applications, as well as cryptocurrency wallet data. RedLine Stealer is often associated with sophisticated phishing campaigns that, after a successful infection, can deliver additional payloads like ransomware or more advanced malware.
- **Stealc** is a relatively new malware family that was first seen in early 2023. It is known as a copycat information stealer because it has a suite of features that is ostensibly based on Vidar, Raccoon, Mars, and RedLine stealers. By default, Stealc targets data in web browsers, browser extensions, cryptocurrency applications, and email messaging software.
- **Spidey Bot** is a less common information stealer first seen in 2019. It is designed to collect stored passwords and other data from a variety of distinct sources within infected environments. The targeted information can include VPN, internet browsers, email clients, gaming software, and cryptocurrency.

Source: https://cofense.com/blog/luxury-hotels-remain-target-of-social-engineering-attack/