 Trustwave
SpiderLabs

Hospitality Sector **Deep Dive**

A DFIR Case Study

Contents

- The Case 5**
- Trustwave’s Findings 6**
- Analysis 7**
 - Basis7**
 - Initial Access7**
 - QR Code Analysis9**
 - Threat Actor Activity10**
 - Financial System/Network Access12**
 - Containment.....12**
- Conclusion 13**
- Recommendations 14**
- Appendix A 16**
- Appendix B 16**

The information in this report is derived from several incidents spread over multiple clients that Trustwave SpiderLabs' Digital Forensics and Incident Response (DFIR) investigated. However, to protect our client's privacy and to create a single case study, all the information was combined, and we will discuss it as a single entity under the false client's name of Five Star Hotels, and employee data, such as email addresses, will be generalized under that moniker.

This report is a supplement to the just released [2025 Trustwave Risk Radar Report: Hospitality Sector](#) report.

The Case

On December 13, 2024, Five Star Hotels contacted Trustwave SpiderLabs' Digital Forensics and Incident Response (DFIR) services team for assistance investigating an incident involving a compromised user account and targeted phishing attempts launched against multiple Five Star Hotels employees.

Five Star Hotels tasked Trustwave with investigating the incident and determining, to the extent possible, the following:

- The purpose of a QR code included in phishing messages sent to Five Star Hotels employees.
- Whether the threat actor accessed files using compromised user account(s).
- Identifying any further indicators of compromise in logs available on Five Star Hotels' Splunk platform.

At the end of Trustwave's interaction with Five Star Hotels, we also provided updates on findings outside the scope of the client's requests and recommendations for containment throughout the investigation. Five Star Hotels immediately implemented these recommendations to remediate and further harden their overall security posture.

Trustwave's Findings

Trustwave's investigators uncovered the following issues:

- A threat actor sent phishing emails to 14 Five Star Hotels employees during three separate phishing campaigns from November 10 to December 13, 2024.
- Four employees showed evidence of suspicious logins based on IP address geolocation.
- During the first targeted phishing campaign, which started on November 10, 2024, one employee, let's call this person User11@5starhotels[.]com, fell victim to a targeted phishing email sent from ThreatActor01@FakeDomain01[.]com. The campaign employed a fake DocuSign phishing link as part of its social engineering effort.
- Then, on November 17, 2024, another employee, User04@5starhotels[.]com, fell victim to a phishing email using a fake e-sign request with a subject that contained "Five Star Hotels Contract Agreement." Messages from this campaign were sent from ThreatActor02@FakeDomain02[.]com, ThreatActor03@FakeDomain03[.]com, and ThreatActor04@FakeDomain04[.]com between November 15 and 17, 2024.
- The threat actor compromised user accounts for User03@Five Star Hotels [.]com and User07@5starhotels[.]com on December 8 and 9, 2024, respectively. This targeted phishing campaign contained an "annual notice for 401(k) plan" and a QR code sent from ThreatActor05@FakeDomain05[.]com from December 8 to 11, 2024.
- The QR code link would take the victim to a phishing landing page where they would be prompted to enter their credentials and have their credentials stolen by the attacker.
- There is no evidence that the threat actor used any of the compromised user accounts to access Five Star Hotels' financial system, nor did the threat actor gain access to Five Star Hotels' network during the incidents. All malicious activities took place in a Microsoft 365 environment.

Analysis

Basis

Trustwave utilized Five Star Hotels' Splunk instance to perform searches and support the investigation. The primary index used for the investigation within Splunk was "o365." Five Star Hotels also provided a copy of the malicious PDF attachment containing a QR code, "*Employee Payroll Schedule.pdf*," for analysis.

All dates and times contained in this report were extracted directly from the logs available within Splunk. Splunk did not list the specific time zones but no conversion by any of the search queries utilized for the investigation was performed.

Initial Access

The Threat Actor obtained unauthorized access to four (4) Five Star Hotels accounts beginning November 10, 2024. The initial compromise, affecting a single user, resulted from a separate phishing campaign than those received by users in December. The November phishing campaign purported to be a DocuSign document. The clickable image in the email, shown in Appendix A, linked victims to a malicious site to capture user credentials. At the time of analysis, the site was no longer active.

User11@5starhotels[.]com

- Threat Actor logged into the user account for User11 on November 10, 2024, at 03:07:52 from IP address XXX.XXX.180. At the time of the investigation, this IP geolocated to Helsinki, Finland.
- The login occurred approximately two (2) hours after a phishing email was received by the user with the subject: User11, Document awaiting Your Review & Signature on Thursday-November-2024 16:57 PM at 00:59.
- The email was sent by ThreatActor01@FakeDomain01[.]com from IP address XXX.XXX.XXX.124, which geolocated to Frankfurt, Germany at the time of the investigation.

User04@5starhotels[.]com

- User04 received a phishing email with a subject purporting to be an e-sign for a “Hospitality Contract Agreement” on November 15, 16, and 17, 2024.
- On November 17, 2024, at 10:02:42, Threat Actor logged into the user account User04@5starhotels[.]com from IP address XXX.XXX.XXX.211.
- At the time of the investigation, the IP address geolocated to New York City, New York and was registered to IPXO LIMITED.

User03@5starhotels[.]com

- On December 8, User03@5starhotels[.]com received phishing emails with subjects involving “Payroll Disbursements & Pending Direct Deposit”.
- Threat Actor’s login to User03’s account from thirteen (13) suspicious IP addresses were made on December 8.

User07@5starhotels[.]com

- On December 9, 2024, User07@5starhotels[.]com received phishing emails with subjects involving “Payroll Disbursements & Pending Direct Deposit”.
- Threat Actor’s login to User07’s account from ten (10) suspicious IP addresses were made on December 9.

QR Code Analysis

Five Star Hotels provided Trustwave with the malicious attachment extracted from one of the phishing emails sent to employees during the December phishing campaign that contained a QR code. Trustwave completed an analysis of the PDF document to understand and record the attack flow and purpose of the QR code in the attack. Appendix B shows a screen capture of the malicious PDF document.

The PDF purports to be an annual notice for a 401(k) plan and instructs victims to scan a QR code in the document to access the new plan. The QR code takes victims to a phishing landing page. The phishing attack uses a service known as “Greatness Phishing Kit,” which operates as a Phishing-as-a-Service (PaaS) provider.

The base URL `hxxps://syeta[.]com/cio/cio` sends victims to a compromised website hosting a simple HTML code. This HTML code, in turn, loads the rest of its content from another server hosting the phishing kit at `https://workinghome.top/`. The design of this setup helps hide the true host of the phishing kit.

The phishing page content mimics a Microsoft 365 login page, usually pre-filled with the victim’s email address.

After the victim submits their email and password, the phishing kit verifies whether the email is a targeted one. Then it connects to Microsoft 365, assumes the victim’s identity, and attempts to log in. In the case of multi-factor authentication (MFA) usage, the phishing kit service operates discreetly, interacting with the legitimate Microsoft 365 login page, masquerading as the victim. The victim is then prompted to authenticate using the MFA method specified by the real Microsoft 365 page, such as an SMS code, voice call code, or push notification — an effort to circumvent MFA. Figure 1 shows the attack flow for the phish.

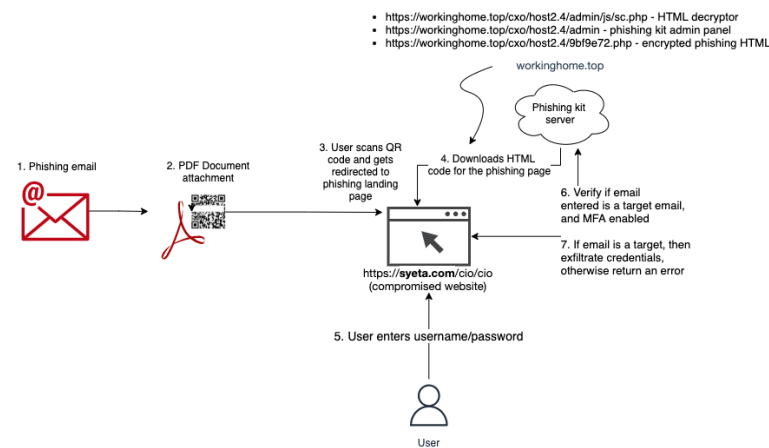


Figure 1: Attack Flow

Threat Actor Activity

The window of compromise lasted from initial access to User11's account on November 10, 2024, until Five Star Hotels completed containment activities for compromised accounts between December 12 and 14, 2024. During the window of compromise, the Threat Actor set up mailbox rules in three (3) of the compromised user's mailbox and utilized User11's account to access files stored in Microsoft 365 ("M365").

To identify Threat Actor activity, Trustwave extracted login activity for the compromised user accounts, removed trusted IP addresses from the results, and crafted searches that specifically targeted suspicious IP addresses. Table 1 lists Threat Actor activities performed on M365.

Date	Operation	User
11/10/2024	FolderCreated	User11@5starhotels[.]com
11/10/2024	FolderModified	User11@5starhotels[.]com
11/12/2024	FileAccessed	User11@5starhotels[.]com
11/12/2024	FilePreviewed	User11@5starhotels[.]com
11/14/2024	FileAccessed	User11@5starhotels[.]com
11/14/2024	FilePreviewed	User11@5starhotels[.]com
11/15/2024	FileAccessed	User11@5starhotels[.]com
11/19/2024	New-InboxRule	User11@5starhotels[.]com
11/25/2024	New-InboxRule	User11@5starhotels[.]com
11/29/2024	FileAccessed	User11@5starhotels[.]com
11/29/2024	FilePreviewed	User11@5starhotels[.]com
11/29/2024	Set-InboxRule	User11@5starhotels[.]com
12/8/2024	FileAccessed	User03@5starhotels[.]com
12/12/2024	New-InboxRule	User03@5starhotels[.]com
12/12/2024	New-InboxRule	User07@5starhotels[.]com

Table 1. List of operations by suspicious IP addresses grouped by date and user

IPXO Limited is the registered owner of most of the IP addresses observed in the incident. IPXO Limited is registered in the UK and offers IP address leasing services that allows users to select IP addresses based on location, quantity, and pricing.

The operations: *FolderCreated*, *FolderModified*, *FileAccessed*, and *FilePreviewed*, shown in Table 1 are specifically the operations completed by the identified suspicious IP addresses.

Two (2) *FileAccessed* operations occurred from suspicious IP addresses for User03’s account. The two (2) files were located in the base URI <https://hospitality-my.sharepoint.com/personal/REDACTED/Documents/REDACTED/Accounting/ACCOUNTING>. One (1) document was named “12 December 2024 – Chargeback Report.xlsx” and the other “12 December Recap.xlsm.” Five Star Hotels has compiled a full listing of the files with *FileAccessed* operations during the window of compromise for User11.

Threat Actor activities such as messages sent and received from compromised mailboxes and a legal review of files potentially accessed during the window of compromise were outside the scope of this investigation.

Adversaries commonly use inbox rules to conceal malicious activities within a compromised mailbox. The *New-InboxRule* operation indicates the creation of a new rule. The *Set-InboxRule* operation indicates updates and modifications to existing rules. Table 2 provides each of the mailbox rule modifications made by the Threat Actor during the window of compromise.

Date Time	User	Command	Parameters
11-19-2024 22:03:54	User11	New-InboxRule	Name: “.” MoveToFolder: “RSS Subscriptions” FromAddressContainsWords: “@domain01[.]com” MarkAsRead: “True”
11-25-2024 11:44:27	User11	New-InboxRule	Name: “.” From: “User15@5starhotels[.]com” MoveToFolder: “RSS Subscriptions” MarkAsRead: “True”

Date Time	User	Command	Parameters
11-29-2024 00:49:28	User11	Set-InboxRule	Name: “.” From: “User15@5starhotels[.]com; User165starhotels[.]com”
11-29-2024 15:09:21	User11	Set-InboxRule	Name: “.” From: “User15@5starhotels[.]com; User16@5starhotels[.]com; User17@5starhotels[.]com”
11-30-2024 11:39:29	User11	Set-InboxRule	Name: “.” FromAddressContainsWords: “@domain01[.]com”
11-30-2024 11:39:37	User11	Set-InboxRule	Name: “.” From: “User15@5starhotels[.]com; User165starhotels[.]com; User17@5starhotels[.]com”
11-30-2024 11:40:03	User11	New-InboxRule	Name: “.” MoveToFolder: “RSS Subscriptions” SubjectContainsWords: “Deposit Report” MarkAsRead: “True”
12-12-2024 13:31:07	User03	New-InboxRule	Name: “Move all messages from User18 to Archive” From: “5starhotels[.]com”, MoveToFolder: “Archive” SubjectContainsWords: “”
12-12-2024 14:28:24	User07	New-InboxRule	Name: “Move all messages from Tonya Pegram to Archive” From: “User03@5starhotels[.]com” MoveToFolder: “Archive” SubjectContainsWords: “”

Table 2. Mailbox rules for compromised users from Nov. 10 to Dec. 15, 2024

Financial System/Network Access

Trustwave's investigation included queries specific to Five Star Hotels' financial system. This system is only accessible when physically on site or through Five Star Hotels' VPN. A search of all connections involving the compromised accounts showed no suspicious connections during the identified window of compromise to either the financial systems or Five Star Hotels' network. All identified Threat Actor activities took place in M365.

Containment

Five Star Hotels performed containment actions while initially responding to the incident. Trustwave also provided recommendations during their investigation to help further harden and secure Five Star Hotels against similar threats.

Five Star Hotels performed the following containment actions immediately upon identifying accounts with suspicious activity:

- Revoke all active sessions
- Disable account prior to credential reset as necessary
- Reset user credentials
- Clear MFA devices and force re-registration of devices

Five Star Hotels also reported initiating a "seek and destroy" for all identified phishing messages to eradicate the identified emails from the environment. Table 3 below identifies the date and time of credential resets for each user.

Date Time UTC	User	Operation
2024-12-12 15:26:02	User03@5starhotels[.]com	Change user password.
2024-12-12 15:26:43	User03@5starhotels[.]com	Change user password.
2024-12-13 16:50:52	User07@5starhotels[.]com	Change user password.
2024-12-14 19:00:32	User11@5starhotels[.]com	Change user password.
2024-12-27 18:46:15	User04@5starhotels[.]com	Account Disabled

Table 3. User credential reset

Five Star Hotels provided Trustwave with documentation sufficient to confirm that the malicious email addresses used in the phishing attacks were blocked within Mimecast on December 22. Mimecast was also configured to block all emails originating from Bulgaria. Many other countries such as Brazil, China, Germany, Finland, and Russia are already blocked within Mimecast.

Five Star Hotels reported performing searches for all indicators of compromise across the environment using their SIEM and Mimecast to ensure containment.

There were no further indicators of compromise identified based on Five Star Hotels' internal investigation and the investigation performed by Trustwave.

Conclusion

Trustwave's investigation found:

- The Threat Actor targeted Five Star Hotels with at least three phishing campaigns that appeared to focus on specific users within the organization.
- The Threat Actor compromised four user accounts using phishing emails in November and December 2024. User11@5starhotels[.]com on November 10, 2024, User04@5starhotels[.]com on November 17, and User03@5starhotels[.]com, and User07@5starhotels[.]com on December 8 and 9, 2024, respectively.
- There is no evidence that the Threat Actor used any of the compromised user accounts to access Five Star Hotels' network or financial system.
- The phishing campaigns used e-Signing and/or HR-related subjects (i.e., payroll, direct deposit) to lure victims into clicking on malicious links. The links would redirect users to malicious websites designed to capture their credentials and circumvent MFA as necessary.
- The QR code contained in malicious PDF documents took victims to a malicious credential harvesting site. As discussed in a recent Trustwave [blog](#)¹, QR codes in phishing emails are more challenging to detect via conventional filters that heavily rely on message content for blocking as there are fewer red flags present, leaving only the malicious URL visible for detection. Cell phones, frequently lacking the same network security controls as internal network connected devices, are also targeted in these attacks.
- Only User11 and User03 accounts contained "File Accessed" operations.
- User11's account had a window of compromise from November 10 to December 14.
- Threat Actor compromised User04's account on November 17. The investigation found no additional suspicious activity following the initial compromise. Five Star Hotels reset User04's credentials on December 27, the same day it was identified as compromised.
- Five Star Hotels reset credentials as soon as the compromise was identified. The credentials for User03 were reset on December 12, User07's credentials were reset on December 13, followed by User11s on December 14.
- IPXO Limited was the register for nearly all the suspicious IP addresses identified during the investigation.

All conclusions are based on Trustwave's experience, and the evidence provided for analysis. We reserve the right to amend our conclusions should new evidence be made available for further analysis.

¹ [Think Before You Scan: The Rise of QR Codes in Phishing](#)

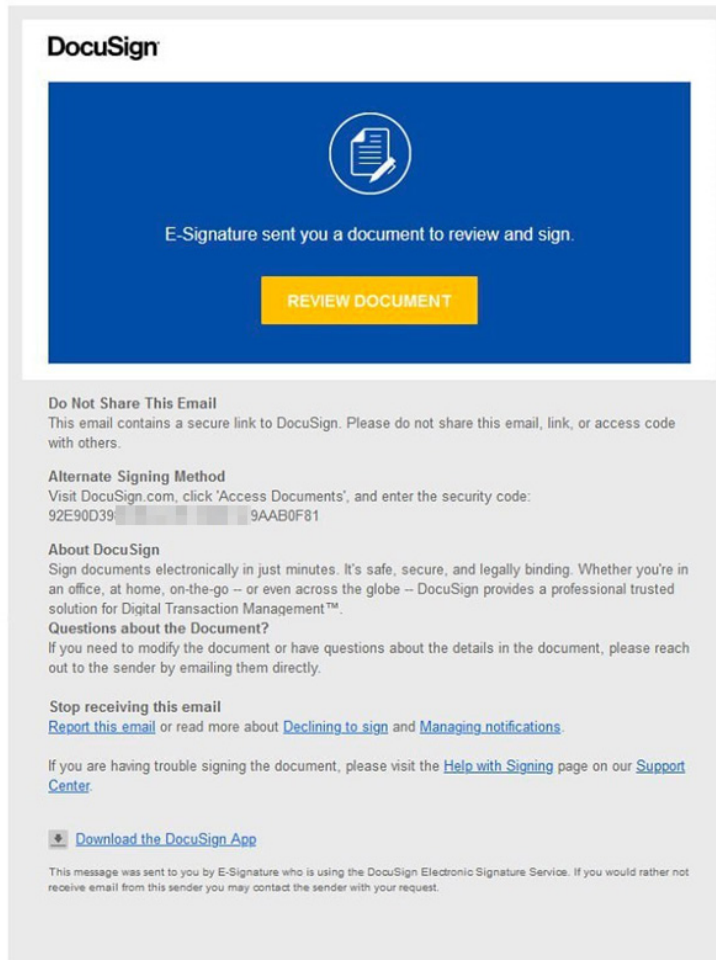
Recommendations

Trustwave's investigation has found the following recommendations should be implemented to further harden Five Star Hotels' security posture.

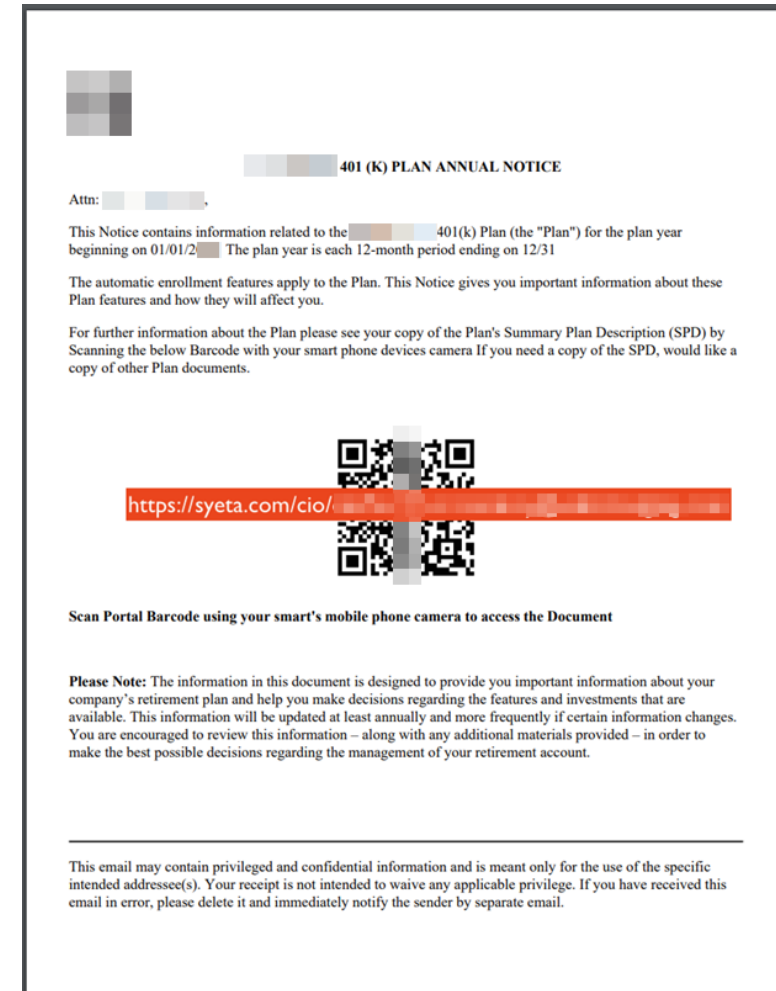
- Given the number of phishing messages encountered, user response to phishing messages should be regularly tested to ensure awareness and adherence to security best practices involving emails.
- SPF, DKIM and DMARC failed to validate the malicious phishing emails. This is often a strong indicator of a spoofed or malicious sender and can be used to filter malicious emails in the future.
- M365 identified each of the malicious phishing emails as phishing and malicious. It is recommended that a review is conducted on the configuration between Mimecast and M365 to determine if spam protection in M365 can be increased.
 - Determine if Mimecast can investigate or block messages containing QR codes.
- It is recommended to review the current MFA policy and consider enabling number matching as an MFA method for all users. This method improves sign-in security by enforcing number matching between the sign in device and MFA registered device and is a strong deterrent to business email compromise.
 - Create alerts to monitor when users register new MFA devices. If a user account is compromised, ensure no MFA devices have been added as part containment and remediation.
- Consider risk-based conditional access that enforces security measures like MFA or blocking access based on user risk levels calculated using factors like location, device, and sign-in patterns.
 - Create alerts for atypical and impossible travel detection.
 - If available, use threat intelligence to flag sign-ins associated with known attack patterns or malicious IP addresses.
 - Create alerts specific to new mailbox rules being created and ensure new rules are audited in a timely manner.

As phishing techniques continue to adapt — leveraging QR codes, credential harvesting kits, and MFA bypass tactics — organizations must remain agile in their defenses. This case serves as a reminder that effective detection and response hinge on continuous monitoring, user awareness, and control validation.

Appendix A



Appendix B





Trustwave
SpiderLabs