Technical Incident Response Report

Date	Dec 12, 2024
Prepared By	Scott Maclean
Contributor(s)	
Department	Forensic & IT
Incident Name	Data Breach - Starwood
Incident Number	#362

Table of Contents

Purpose

This report outlines key sections of deliverables associated with technical documentation and tracking of an incident during all phases of incident response, including detection, containment, eradication, recovery and lessons learned.

Incident Summary

This report investigates the Marriott International data breach that occurred from 2014 to 2018, impacting an estimated 500 million guests. The attackers, believed to be working on behalf of the Chinese Ministry of State Security, used sophisticated tools and techniques to infiltrate the Starwood Hotels reservation system. This incident highlights the severe consequences of inadequate cybersecurity measures and the importance of proactive threat detection and response.

Attack Timeline

2014:

- Initial Compromise: Likely occurred in the first half of 2014, potentially exploiting a vulnerability in the Starwood reservation system's web application or a phishing campaign targeting Starwood employees.
- Attackers gain a foothold, possibly with limited access initially.
- Establishing Foothold: Attackers deploy malware, like a Remote Access Trojan (RAT), to maintain persistent access and explore the network.
- They begin to map the network, identify valuable data, and escalate privileges.
- Lateral Movement: Attackers move laterally within the Starwood network, compromising additional systems and accounts to gain access to the reservation database.
- They may use tools like Mimikatz to steal credentials and escalate privileges.

2015 - 2016:

- Starwood informs Marriott of first data breach just four days after acquisition. (Competition, B. of, & Staff at the Office of Technology. (2024, October 9). FTC takes action against Marriott and Starwood over multiple data breaches. Federal Trade Commission)
- Data Exfiltration: Attackers begin exfiltrating data from the reservation database, likely in small batches to avoid detection.
- They may use encryption and other techniques to hide the stolen data within normal network traffic.
- Maintaining Persistence: Attackers maintain their presence on the network, updating their malware and adapting their tactics to avoid detection.
- They may create backdoors and establish alternative access methods in case their primary access is discovered.
- Marriott Acquisition:In 2016, Marriott acquires Starwood, inheriting the compromised network. It's unknown whether the attackers actively tried to hinder or exploit the merger process itself.

2017 - September 2018:

- Continued Data Exfiltration: Attackers likely continue to exfiltrate data from the reservation database, potentially expanding their access to other Marriott systems.
- They may have adapted their tactics to blend in with the merged network environment.
- Evasion and Anti-forensics: Attackers actively work to evade detection by security tools and personnel.
- They may have deleted logs, modified timestamps, or used obfuscation techniques to hide their activity.

September 2018:

- Breach Detection: Marriott's security team detects suspicious activity within the Starwood reservation database, triggering an investigation.
- Marriott detects there was a second data breach that went undetected since 2014
- This may have been due to anomalies in network traffic, unusual database access patterns, or alerts from security tools.

November 2018:

- Public Disclosure: Marriott publicly discloses the data breach, revealing the scope of the compromise and the potential impact on guests.

Systems Targeted

Marriott hasn't released a complete inventory of the targeted systems, but we can deduce likely targets based on the nature of the breach and common hotel IT infrastructure.

1. Starwood Guest Reservation Database:
This was the primary target, containing sensitive guest information like names, addresses, passport numbers, payment card details, and travel histories. The attackers likely focused on this system to gather valuable personal and financial data for espionage or potentially for financial gain.

2. Web Servers:
Web servers hosting the Starwood booking application were likely compromised. This could have been the initial point of entry for the attackers, allowing them to exploit vulnerabilities in the web application or install malware like web shells for persistent access.

3. Database Servers:
In addition to the main reservation database, other database servers might have been targeted. These could include databases storing employee information, financial records, or other sensitive data.

Attacker Motivation

Given the suspected involvement of the Chinese Ministry of State Security, the primary motivation was likely espionage, aiming to gather information on individuals, including government and business travelers. There was no known ransom that was demanded of Marriot to release or decrypt information so it doesn't appear that the attack was financially driven.

Outcome of the Attack

The Marriott data breach resulted in severe consequences, including the exposure of personal and financial data belonging to roughly 500 million guests. This massive breach significantly damaged Marriott's reputation and brand image, leading to substantial financial losses associated with investigation, remediation efforts, legal actions, and regulatory fines of up to $52 Million (Competition, B. of, & Staff at the Office of Technology. (2024, October 9). FTC takes action against Marriott and Starwood over multiple data breaches. Federal Trade Commission)

Technologies and Tools used in the Attack

.

- Attackers likely exploited vulnerabilities in the Starwood Hotels' IT infrastructure to gain initial access. This aligns with MITRE ATT&CK tactic TA0001: Initial Access and techniques like T1190: Exploit Public-Facing Application or T1078: Valid Accounts.

- Malware was likely used to establish persistent access, exfiltrate data, and potentially cover their tracks. This aligns with MITRE ATT&CK tactic TA0003: Persistence and techniques like T1505.003: Web Shell or T1050: New Service.

- Credential Theft:
- Phishing: Tricking employees into revealing their passwords through deceptive emails or websites.
- Credential Stuffing: Using stolen credentials from other breaches to try and access Starwood systems.
- Mimikatz: This tool can extract passwords from memory on compromised systems.
- Example: Attackers could have used Mimikatz to obtain the password for the "sql_svc" account, granting them access to the database server.

- Social engineering: May have been used to gain initial access or to move laterally within the network. This aligns with MITRE ATT&CK tactic TA0001: Initial Access and technique T1566.001: Spearphishing Attachment.

Mitigation Techniques & Nist Controls Recommended for Future

Do a complete and thorough scan of each server, endpoint device and network traffic log of the system you are inheriting before integrating it with your current system.

Implement robust firewalls (NIST 800-171 3.13.1), intrusion detection and prevention systems (NIST SI-4), and regular vulnerability scanning and patching (NIST RA-5).

Enforce strong passwords (NIST IA-5), multi-factor authentication (NIST IA-5), and least privilege access to sensitive data (NIST AC-6).

Encrypt sensitive data both in transit and at rest (NIST SC-28).

Educate employees about cybersecurity threats and best practices to prevent social engineering attacks (NIST AT-2).

Employ security information and event management (SIEM) systems (NIST SI-4) and threat intelligence (NIST RA-1) to identify and respond to potential threats proactively.

Conduct regular security assessments to identify and address vulnerabilities (NIST CA-2, CA-3).

Develop and regularly test an incident response plan to minimize damage and ensure a swift recovery in case of a breach (NIST IR-1, IR-8).

Citations and References

Competition, B. of, & Staff at the Office of Technology. (2024, October 9). FTC takes action against Marriott and Starwood over multiple data breaches. Federal Trade Commission. https://www.ftc.gov/news-events/news/press-releases/2024/10/ftc-takes-action-against-marriott-starwood-over-multiple-data-breaches

Mitre ATT&CK®. MITRE ATT&CK®. (n.d.). https://attack.mitre.org/

Ross, R., Pillitteri, V., Dempsey, K., Riddle, M., & Guissanie, G. (2021, January 28). Protecting controlled unclassified information in nonfederal systems and organizations. CSRC. https://csrc.nist.gov/pubs/sp/800/171/r2/upd1/final

Welcome to CSF tools - CSF tools. CSF Tools - The Cybersecurity Framework for Humans. (2022, March 20). https://csf.tools/