**Investigation and Research Report**

**Subject**

**Mariott Data breach (2014-2018)**

**Max Daguste**

**Lighthouse Labs Assignment W8D5**

**Table of Contents**

1. Introduction
   * Overview of Marriott and its reputation
   * Scope of the investigation: Data breach from 2014 to 2018
   * Nature of the breach
2. Victims of the Attack
   * Impact on the organization
   * Compromised information
3. Tools, Techniques, and Technologies used
   * Advanced Persistent Threat (APT)
   * Definition and characteristics of APT attacks
   * Insights from cybersecurity expert on the attack
   * Definitions of Phishing and Spear-phishing attacks
4. APT Stage 1: Infiltration
   * Social engineering techniques used in APT attacks
   * Spear-phishing targeting high-level individuals
   * Targeted emails from compromised team members
5. APT Stage 2: Escalation and Lateral Movement
   * Malware insertion and lateral movement
   * Establishing a "backdoor" for stealth operations
6. APT Stage 3: Exfiltration
   * Storing and exfiltrating stolen information
   * Use of distraction tactics during data exfiltration
7. Characteristics of an APT Attack
   * Persistence, Advanced techniques, Targeted approach, Evasive tactics
8. Targeted Systems
   * Speculation about targeted systems and attackers' goals
9. Motivation of the Attackers
   * Complex motives behind the breach
   * Likelihood of state-sponsored intelligence-gathering
10. Outcome of the Attack
    * Extent of breach and tactics employed by hackers
    * Successful exfiltration of sensitive data
11. Financial and Reputational Impact
    * Financial penalty and insurance coverage
    * Tarnished reputation and lasting implications
12. Mitigation Techniques and Security Controls
    * Strategies to enhance defenses against APTs
    * Network segmentation, Regular patching, Staff training
    * Incident response plan, User access controls, Multi-Factor Authentication
    * Data encryption, Continuous monitoring
13. References
    * List of all references used in the report
14. **Introduction:**

Marriott is a renowned hospitality company with a reputation for hosting a middle to higher class clientele. Managing an expansive network of hotels and resorts worldwide, Marriott also collects and stores personal payment information from customers during the reservation and check-in process. This investigation delves into a massive data breach that spanned from 2014 to 2018, impacting both the company and its guests. The breach exposed a wide range of sensitive information, including clients' addresses, phone numbers, passport numbers, and credit card details.

[Reference: <https://www.csoonline.com/article/567795/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html>]

1. **Victims of the Attack:**

Approximately 300 million of guests who had reservations at Marriott's establishments hotels, resorts, and other properties were adversely affected by the breach. This compromise led to the exposure of various critical details, including but not limited to addresses, names, phone numbers, payment information, and passport numbers. This breach puts the victims at risk of data/identity theft, financial losses and more.

1. **Tools, Techniques and Technologies used:**

Not a whole lot is disclosed about the attack on the Mariott, but due to the nature of the attack and the dwelling time that spanned of 4 years (from 2014 to 2018), we could safely assume that it is an Advance Persistent Threat (APT).

**Advance Persistent Treat:**

*An advanced persistent threat (APT) is a sophisticated, sustained*[*cyberattack*](https://www.crowdstrike.com/cybersecurity-101/cyberattacks/)*in which an intruder establishes an undetected presence in a network in order to steal sensitive data over a prolonged period of time. An APT attack is carefully planned and designed to infiltrate a specific organization, evade existing security measures and fly under the radar.* (more on that threat later in the report).

[Reference <https://www.crowdstrike.com/cybersecurity-101/advanced-persistent-threat-apt/> ]

*CrowdStrike cybersecurity expert Ryan Cornateanu told Hotel Tech Report, “The attack on Marriott was hapless and a popular entry point for adversaries is through email spoofing. This tactic is used in phishing to get malware onto a target network to then move laterally across all systems. From there, hackers can leverage account numbers, driver's license numbers, and other sensitive information from loyalty programs and reservations systems. The general data protection regulation has gone a long way to protect consumers, but there's only so much that can be done when a hacker is able to secure login credentials or access servers directly.”* [Reference: <https://hoteltechreport.com/news/marriott-data-breach> ]

**Definitions**

*Phishing email:*

***Phishing****is a scam that impersonates a reputable person or organization with the intent to steal credentials or sensitive information. Although email is the most common type of phishing attack, depending on the type of phishing scam, the attack may use a text message or even a voice message.*

[Reference: <https://www.crowdstrike.com/cybersecurity-101/phishing/>]

*Spear-phishing attack:*

*Spear-phishing is a type of phishing attack that targets specific individuals or organizations typically through malicious emails. The goal of spear phishing is to steal sensitive information such as login credentials or infect the targets’ device with malware. Spear phishers carefully research their targets, so the attack appears to be from trusted senders in the targets’ life. A spear phishing email uses social engineering techniques to urge the victim to click on a malicious link or attachment. Once the victim completes the intended action, the attacker can steal the credentials of a targeted legitimate user and enter a network undetected.*

[Reference: <https://www.crowdstrike.com/cybersecurity-101/phishing/spear-phishing/> ]

**APT Stage 1: Infiltration**

In the first phase, **advanced persistent threats often gain access through social engineering techniques**. One indication of an APT is a[phishing email](https://www.crowdstrike.com/cybersecurity-101/phishing/) that selectively targets high-level individuals like senior executives or technology leaders, often using information obtained from other team members that have already been compromised. Email attacks that target specific individuals are called “spear-phishing.”

The email may seem to come from a team member and include references to an ongoing project. If several executives report being duped by a [spear-phishing attack](https://www.crowdstrike.com/cybersecurity-101/phishing/spear-phishing/), start looking for other signs of an APT.

Not much information has not been revealed about the Mariott breach. However, it is certain that the target has been studied by the attacker through an extended period and social engineering through the above-mentioned means have been executed.

**APT Stage 2: Escalation and Lateral Movement**

*Once initial access has been gained, attackers insert*[*malware*](https://www.crowdstrike.com/cybersecurity-101/malware/)*into an organization’s network to move to the second phase, expansion. They****move laterally to map the network and gather credentials****such as account names and passwords to access critical business information.*

*They may also establish a “backdoor” — a scheme that allows them to sneak into the network later to conduct stealth operations. Additional entry points are often established to ensure that the attack can continue if a compromised point is discovered and closed*.

[Reference: <https://www.crowdstrike.com/cybersecurity-101/advanced-persistent-threat-apt/> ]

As mentioned above, the attacker can extend his scope of “work” once he has established a presence in the network. He can move laterally and also vertically (upper management) provided that he has acquired access to their credentials as well.

**APT Stage 3: Exfiltration**

*To prepare for the third phase, cybercriminals typically****store stolen information in a secure location****within the network until enough data has been collected. They****then extract, or “exfiltrate” it without detection****. They may use tactics like a denial-of-service (DoS) attack to distract the security team and tie up network personnel while the data is being exfiltrated. The network can remain compromised, waiting for the thieves to return at any time.*

[Reference: <https://www.crowdstrike.com/cybersecurity-101/advanced-persistent-threat-apt/> ]

It is unclear what amount of data has been exfiltrated from the Mariott’s network. However, it is certain that the exfiltration did occur. If the incident was a harmless one, the company would likely not have been so “secretive” about the incident.

It is worth mentioning that APT is often represented in more stages that shown in the report. For the sake of brevity it has been segmented in the above-mentioned phases. For a more exhaustive breakdown of the phases you can click on this link <https://www.splunk.com/en_us/blog/learn/apts-advanced-persistent-threats.html> and go on **Phases in APTs: A step-by-step approach section.**

**Characteristics of an APT Attack:**

Une image contenant texte, cercle, capture d’écran, internet

Description générée automatiquement

* **Persistence**: *Attackers are persistent and may remain undetected within a target network for months or years, continuously working towards their objective.*
* **Advanced**: *APTs are usually orchestrated by highly skilled individuals or groups with significant financial and technical resources, such as:*
* *Nation-states*
* *Organized crime groups*
* *State-sponsored hacking groups*

Malicious actors employ advanced methods to infiltrate and compromise their targets, like zero-day exploits, social engineering, spear-phishing, etc.

* **Targeted**: APTs are highly targeted attacks aimed at specific organizations, industries or governments with valuable information or assets. Attackers carefully select their targets based on the potential strategic value.
* **Evasive/Stealthy:** *A key characteristic of APTs is their focus on remaining undetected within the target’s network. Attackers employ various tactics to maintain a low profile, such as:*
* *Using legitimate credentials.*
* *Blending in with regular network traffic.*
* *Erasing traces of their activities.*

*[Reference:* <https://www.splunk.com/en_us/blog/learn/apts-advanced-persistent-threats.html>]

1. **Targeted Systems**

No information has been provided about the systems that were targeted for the Marriott’s breach. It is safe to assume that the attackers played the long game and had the intention of staying there for a long time (and they did) to increase the scope of their attacks over time. Identifying a specific system might be impossible without knowing the Mariott’s system. However, a fair assumption would be to say that the clients credit card information may have been part of the attackers goals.

1. **Motivation of the Attackers**

The complexity of identifying the culprits behind the Marriott breach is compounded by the multifaceted motives driving their actions. According to reports from reputable sources such as The New York Times and The Washington Post, this attack was likely orchestrated as part of a state-sponsored intelligence-gathering endeavor. The techniques employed during the breach and the absence of guest records on the dark web usually a hotspot for data sales hint that this breach was not primarily driven by financial gain. Instead, the evidence points towards espionage, as a nation-state's strategic objectives align more closely with the observed attack patterns.

*[Reference:* [*https://hoteltechreport.com/news/marriott-data-breach*](https://hoteltechreport.com/news/marriott-data-breach)*]*

1. **Outcome of the Attack**

Marriott's internal investigation uncovered the extent of the breach and shed light on the tactics employed by the hackers. Beyond gaining unauthorized access to the system, the attackers employed encryption techniques to obscure their actions. In the process, they successfully exfiltrated a substantial amount of data. This trove included sensitive information extracted from a significant number of guest records, estimated to be around 500 million. While the breach affected a considerable volume of guest records, it's noteworthy that a portion of these records were duplicates. This incident showcased the intricacy of the attack and the comprehensive measures the hackers took to circumvent detection and exfiltrate data.

The impact of the breach was exacerbated by vulnerabilities in the reservation system and organizational practices. An incident in 2015, during which security was compromised and remained undetected for an extended period, revealed pronounced weaknesses in the system's defenses. Additionally, changes following a 2016 acquisition, including workforce reductions, hindered the smooth integration of new properties into the company's reservation infrastructure. Consequently, the compromised reservation system continued to operate with vulnerabilities, lacking effective oversight and inadvertently creating a pathway for the breach.

Marriott's financial challenges extended beyond the immediate aftermath of the breach. The hotel company was dealt a major setback, being fined around $23.8 million due to the 2014 data breach. Although insurance did offer some financial relief, the incident severely tarnished Marriott's reputation, with lasting implications. The breach, which exposed sensitive information like credit card details, passport numbers, and birthdates of over 300 million guests stored in the company's worldwide guest reservation system, ranked among the most substantial data breaches on record.

*[Reference:* [*https://hoteltechreport.com/news/marriott-data-breach*](https://hoteltechreport.com/news/marriott-data-breach)*]*

1. **Mitigation Techniques Recommended and Security Controls to Implement**

Mitigating the risk of Advanced Persistent Threats (APTs) requires a multifaceted approach to strengthen the organization's network system. Implementing the following strategies and security controls can significantly enhance defenses against APTs:

**Network Segmentation:**

Isolating critical systems from potential compromise through network segmentation helps contain an attack's impact. By dividing the network into distinct segments, unauthorized lateral movement can be restricted, preventing attackers from easily traversing the network and accessing sensitive data.

[Reference: <https://www.cisco.com/c/en/us/products/security/what-is-network-segmentation.html>]

**Regular Patching:**

Frequent software updates and patches are crucial to prevent the exploitation of known vulnerabilities by attackers. Prompt patching of operating systems, applications, and third-party software minimizes the attack surface and reduces the risk of successful APT infiltration.

**Staff Training:**

Educating employees about phishing and social engineering tactics is paramount. Regular training sessions raise awareness about the risks associated with suspicious emails, links, and attachments. By empowering employees to recognize and report phishing attempts, organizations can prevent initial attack vectors used by hackers.

**Incident Response Plan:**

Developing a comprehensive incident response plan specifically tailored to APT scenarios is essential. The plan should outline procedures for identifying, containing, eradicating, and recovering from APT incidents. Regularly testing and refining the plan ensures a swift and effective response when an attack occurs.

[Reference: <https://www.securitymetrics.com/blog/6-phases-incident-response-plan>]

**Zero Trust/User Access Controls:**

Implement strict access controls and least privilege principles to limit user access to sensitive data and critical systems. This reduces the potential exposure of sensitive information in the event of a breach.

**Multi-Factor Authentication (MFA):**

Enforce the use of multi-factor authentication across all systems and accounts. MFA adds an extra layer of security by requiring users to provide multiple forms of verification before granting access.

[Reference: <https://www.onelogin.com/learn/what-is-mfa#:~:text=The%20main%20benefit%20of%20MFA,be%20stolen%20by%20third%20parties>.]

**Data Encryption:**

Encrypting sensitive data at rest and in transit safeguards information even if it falls into unauthorized hands. Strong encryption ensures that compromised data remains unintelligible to attackers.

[Reference: <https://www.cisa.gov/safecom/encryption>]

**Continuous Monitoring:**

Implement continuous monitoring of network traffic and system behavior to promptly identify suspicious activities. Real-time analysis enables rapid detection and response to APT activities.

[Reference: <https://www.clearnetwork.com/cybersecurity-monitoring-why-you-need/>]

incorporating these mitigation techniques and security controls, organizations can significantly enhance their ability to prevent, detect, and respond effectively to Advanced Persistent Threats, bolstering their overall cybersecurity posture.

**References**

CSO Online. (n.d.). Marriott data breach FAQ: How did it happen and what was the impact? [https://www.csoonline.com/article/567795/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html]

CrowdStrike. (n.d.). Advanced Persistent Threat (APT). [https://www.crowdstrike.com/cybersecurity-101/advanced-persistent-threat-apt/]

Hotel Tech Report. (n.d.). Marriott Data Breach. [https://hoteltechreport.com/news/marriott-data-breach]

CrowdStrike. (n.d.). Phishing. [https://www.crowdstrike.com/cybersecurity-101/phishing/]

CrowdStrike. (n.d.). Spear Phishing. [https://www.crowdstrike.com/cybersecurity-101/phishing/spear-phishing/]

Splunk. (n.d.). APTs (Advanced Persistent Threats). [https://www.splunk.com/en\_us/blog/learn/apts-advanced-persistent-threats.html]

Cisco. (n.d.). What Is Network Segmentation? [https://www.cisco.com/c/en/us/products/security/what-is-network-segmentation.html]

SecurityMetrics. (n.d.). The 6 Phases of an Incident Response Plan. [https://www.securitymetrics.com/blog/6-phases-incident-response-plan]

OneLogin. (n.d.). What is Multi-Factor Authentication (MFA)? [https://www.onelogin.com/learn/what-is-mfa#:~:text=The%20main%20benefit%20of%20MFA,be%20stolen%20by%20third%20parties.]

CISA. (n.d.). Encryption. [https://www.cisa.gov/safecom/encryption]

ClearNetwork. (n.d.). Why You Need Cybersecurity Monitoring. [https://www.clearnetwork.com/cybersecurity-monitoring-why-you-need/]