Case Study

Point of Sale Attack

Marriott Data Breach 2018

Attack Category:
Point of Sale

A point-of-sale (POS) attack is a cyberattack targeting POS applications and systems that store or process customers' credit card details or transactions. POS malware enters through compromised or weakly secured systems and scrapes the RAM to find payment card data, which is then sent unencrypted to the hacker. The malware is used by cybercriminals to target point of sale (POS) and payment terminals with the intent to obtain credit card and debit card information, a card's track 1 or track 2 data and even the CVV code, by various man-in-the-middle attacks.

Ponemon and IBM Security's 2022 global case study report revealed that $2.94 million was the average total cost of a data breach in the hospitality industry from 2021 to 2022. The associated costs from a breach come from several sources including lost business, reputational damage, legal costs, forensic activities, crisis management, regulatory response and customer notification — to name a few.
Additionally, according to IBM Security's report, 83% of global organizations suffer more than one data breach.

Source: Cost of a Data Breach Report 2022 IBM Corporation, Jul 2022

Company Description and Breach Summary

Marriott International is an American hospitality company founded in 1927, headquartered in Bethesda, Maryland, US. It is the largest hotel chain in the world with a total of 30 brands in 131 countries. With 21 years in the Fortune 500 list, Marriott international holds 151 rank in the list as of 2019. Marriott International is known widely for its luxurious hotels and rich customers.
From a root beer stand to the world's largest hotel chain, Marriott International's story is a true inspiration for many entrepreneurs.

In 2014—two years before Marriott even acquired Starwood—the latter company's guest reservation system was infiltrated by cybercriminals via remote access trojan (RAT). Despite this intrusion within the guest reservation system, Starwood was unable to detect the cybercriminals' activity—allowing them to remain unnoticed.

In 2016, Marriott officially acquired Starwood. During the acquisition process, Marriott failed to complete a detailed cybersecurity audit of Starwood's networks and technology. Marriott then also began migrating information from several databases housed within Starwood's guest reservation system. While the information in these databases was encrypted, the cybercriminals were eventually able to locate their associated decryption keys and subsequently unlock the information. From there, the cybercriminals began exfiltrating the information. After transporting this information, the cybercriminals then re-encrypted it in an effort to remain undetected within the system.

A full two years after the acquisition—Marriott finally identified the breach due to a system security alert. Marriott confirmed to the public that the personal information of nearly 500 million customers around the world—including the United States, Canada and the United Kingdom—had been compromised.

Timeline

1. Nov 2014: Chinese State Sponsored Attacker's install a malware to steal debit and credit card data, PII at PoS cash registers of Starwood Hotels
2. Nov 2015: Starwood Hotels report the breach with a total of 50+ hotels impacted by the breach
3. Sep 2016: Marriott International acquires Starwood Hotels for 13 billion dollars and maintains the same IT system. But the staff responsible were laid off
4. September 2018: internal security tool flagged as suspicious an attempt to access the internal guest reservation database for Marriott's Starwood brands. Marriott launches an internal investigation.
5. Nov 2018: Marriott reports the breach with a total loss of 500 million guest records including Ph numbers, Credit Card data, names, etc
6. Jul 2019: Marriott was fined with 123 million dollars GDPR fine and potentially much more is expected to be paid.

Vulnerabilities

Marriott International reported that it was breached in November 2018. The breach was believed to have begun in 2014 when the hacked system was a part of Starwood Hotel's. Following the merger, Marriott did not integrate the system to a central security system and rather maintained the same systems as before. The attackers used RAT, and MimiKatzto obtain the guest list along with their travel details and credit card details. The keys to credit card encryptions were also believed to be breached.

Exposed RDP ports

Although RDP ports are useful workplace tools that permit employees to connect remotely to other servers or devices, leaving these ports open can allow cybercriminals to leverage them as a vector for deploying malicious software or other harmful programs (including RATs). That being said, RDP ports should never be unnecessarily left open to the internet.

M&A Due Diligence

Marriott neglecting to prioritize cybersecurity amid its acquisition of Starwood proved detrimental in this breach. Primarily, Marriott should have diligently assessed Starwood's IT vulnerabilities throughout the M&A process. Further, Marriott should have ensured an effective cybersecurity infrastructure between the combined companies once the acquisition took place. Especially as cyber incidents continue to surge in both cost and frequency, cybersecurity should be top of mind during any M&A activity. In particular, each company involved in the M&A process should be carefully evaluated for potential cybersecurity gaps. A proper plan for rectifying or—at the very least—mitigating these exposures should be developed prior to the finalization of the M&A event. In many cases, it can also be advantageous for merged companies to adopt shared digital processes and security policies in order to maintain uniform defense strategies against cybercriminals.

Poor data and network security

The compromised data included 5.25 million unencrypted passport numbers and, potentially, unencrypted credit card data for several thousand users. The sensitivity of these data means that it should have been stored only in an encrypted format. Network segmentation is required for compliance with PCI-DSS, the standard that governs organizations collecting and storing payment card information. Marriott did not consider beforehand the importance of compliance with such standards.

Poor management support for cybersecurity

Marriott does not appear to have the necessary level of support and focus on cybersecurity. None of their thirteen board members has a strong cybersecurity or technology background, and the organization does not have a dedicated cyber-risk committee. As a result, Marriott needed to rely on third parties to manage all investigation and analysis of the breach. A more cyber-focused culture at Marriott may have been able to manage the breach in-house and detected and responded to it more rapidly, minimizing the damage.

Costs and Prevention

Costs

- **March 2019 — the company had incurred $28 million in expenses related to breach but Cyberinsurance had cut its losses to a mere $1 million.**
- **July of 2019 — The UK's Information Commissioner's Office (ICO) levied a fine of more than $120 million — for violating British citizens' privacy rights under the GDPR.**
- **Marriott's stocks dropped by 5% almost immediately after it announced the details of the breach**
- **The company is estimated to have suffered over $1 billion in lost revenue due to diminished customer loyalty**

Prevention

- Maintaining and securing the PoS cash registers.
- Auditing the Starwood IT system after acquisition
- Integrating the Starwood IT system with a centralized security system.
- Better Log analysis and detection principles automated by Artificial intelligence.
- Regular audits of all the systems involved with industry specific requirements.
- Virtual private networks (VPNs) and multi-factor authentication protocols can also be utilized to help keep RDP ports from being exploited by cybercriminals.
- Implement IP whitelisting for the affected database and is implementing network segmentation to protect sensitive data.
- The organization should have a dedicated cyber-risk committee who has a strong cybersecurity or technology background.