# The Marriott Hotel and the RAT

Can you inherit data breaches in IT security? The answer is a resounding yes. It happened to the Marriott Hotel chains in 2018 and has become part of the lore of the digital security world, one of the most infamous data breaches in its history, and finding a home in most top ten lists for computer and network security breaches, and it was because of a RAT.

A RAT is a Remote Access Trojan (RAT), malware that can gain remote control over a computer or network. It takes its name from the classical story from antiquity, the Trojan Horse. The reason for this is RATs are disguised as something that might belong on your system, a file, or an application. This is part of the deception. The attackers are hoping you click on it.

A RAT gets into its target system by stealth. It disguises itself as a software update or an attachment on an email or something else innocuous and not suspicious or raising alarms.

The reason for RATs is the same as any data breach: theft, access to classified or restricted material, personal data records, financial data, credit card numbers, and just about anything else that cyber criminals are after in a breach of a network or a computer. It turns out that a digital RAT is as bad for reputation as literal rats in the hotel business.

Once inside it stays hidden, just like real rats, sensitive to everything around them, motion, smell, vibration, and only breaking cover when everything is quiet and calm. RATs are designed to survive the sweeps of antivirus software and other security measures. They come in different sizes, just like real rats, but in the digital analogy size is potency — the level and degree of remote access and control. A well-formed RAT can gain access to your computer, your microphone, and all of your files and programs. It can do whatever the user of the computer can do and see whatever the user of the computer can see.

Sometimes a RAT is put into place just for surveillance. Once the RAT is firmly ensconced in the computer or the network they can monitor everything that happens including keystrokes. This information can be used at a future date to access other networks. A well designed RAT will have the ability to avoid detection, but, hands down, the most daunting aspect of a RAT is its ability to open a communication channel with a command and control server run by whoever created and deployed the RAT. The control server gives the attacker the ability to receive data from the compromised system and perhaps even completely take it over remotely. Once the RAT is established on the network or computer the compromised system is open until the RAT is discovered. It allows backdoor access to the system anytime that the remote operators want to enter and control or view what’s going on.

So how did this happen? It’s all detailed in the testimony of Arne Sorenson, President & CEO, Marriott International, as given to the *Senate Committee on Homeland Security & Governmental Affairs Permanent Subcommittee on Investigations*. It began with a corporate merger on November 15, 2015. The Marriott Corporation merged with Starwood, another hotel chain. The transaction closed on September 23, 2016.

It was in that ten-month window that the Marriott looked at all of Starwood's technology and network in an attempt to assess an integration plan. The evaluation was limited by the fact that until the merger formally closed, Starwood was still a competitor. The decision was made to maintain the Marriott’s system as the primary system for reservations. It took another two years to migrate all of Starwood’s 1,270 hotels onto the Marriott reservation system. This all had to be done without disrupting the existing reservation process at the Marriott. After the close of the merger, Marriott continued to operate the Starwood reservation system. Additional security investments were made in the system which was evaluated as coming up short when compared to the existing security on the Marriott reservation system. In September 2018, a company that managed the Starwood guest reservation database contacted the Marriott IT team with information about an alert generated. An IBM security product used on the Starwood system that helped secure the databases was triggered by a query from an administrator’s account to return the count of rows from a table in a database, and the query would not return the content of the rows, rather, only the total number of rows in the table. This set off red flags and commenced an investigation by the Marriott IT team. It was discovered that the individual whose credentials were used had not made the query. Containment protocols were invoked. The Marriott engaged legal counsel and industry experts to investigate the scale and scope of the incident. They subsequently brought in third-party investigators for a full forensic investigation to understand what led to the alert and to assist with the containment. The outside investigators found the RAT. Once it was determined that a RAT was involved a fuller investigation was undertaken to mitigate risk. The Marriott had to know what had been accessed and what had been stolen from their database. By the end of October 2018, the FBI was contacted.

In November of that same year, the investigation discovered two compressed, encrypted files had been deleted from a device that was being examined. Given that the files had been encrypted, the actual content was not known. There was also evidence that two files had been removed from the Starwood network. It was decrypted in November of 2018. One contained an export of a table from the Starwood guest reservation database with guest data, and the other contained an export of a table holding passport information. It was at this point that the Marriott realized it had to make the information public. It was the realization that guest information in the form of passports had been accessed. They had a legal obligation.

It gives new meaning to the idea that nobody wants to stay in a hotel with rats,

and it was a terrible loss of reputation and marketing capital for the esteemed hotel chain. Here is the size and scope of the breach as given by the testimony of Sorenson

“According to our most recent investigative findings, the incident involved approximately 18.5 million encrypted passport numbers and approximately 5.25 million unencrypted passport numbers (approximately 663,000 of which have been associated with the United States). Concerning payment cards, the incident involved approximately 9.1 million encrypted payment card numbers, of which approximately 385,000 were unexpired as of September 2018. Based on our current information, we believe that the information accessed by an unauthorized third party could include several thousand unencrypted payment card numbers. To date, we have not found evidence that the master encryption keys needed to decrypt encrypted payment card and passport numbers were accessed, but we cannot rule out that possibility.”

The cost of repairing the reputation was enormous. The Marriott had to set up a system to notify guests and update them on all information. This manifested as a dedicated website for guests and a call center to answer questions. They also offered two free monitoring solutions for potentially affected guests, services that monitor known sites where personal information might be shared and, if the data of a registered Marriott guest was discovered, an alert to the guest, the security service of the guest’s financial institution, or another designated party. The Marriott also included fraud loss reimbursement coverage and unlimited fraud consultation services for one year. A quarter million of Marriott’s guests availed themselves of the service by the end of February, 2019.

The Marriott Hotel case illustrates how security is everybody’s concern. We live in a time where digital security is mandatory and should be a serious consideration in any acquisition or merger in which the purchaser is inheriting network systems with sensitive data. The Marriott Hotel case highlights how liability can be inherited by the merger of another computer system with inferior security or improper security auditing. There are a couple of ways to deal with this. The first is to make sure that you have the very best security to recognize human interaction on your system. In this domain, hCaptcha™ is the best in class. It employs the latest in machine learning (ML) and human verification technologies.

The other remedy is legal. It may be necessary to write acquisition contracts in which a post-purchase security breach in the inherited system is the liability of the seller. Security standards among organizations should be mandatory, but they’re not, and there is only so much that can be done through due diligence in the area of system security, especially if a RAT is already nested in the system. It’s a matter for the courts and lawyers. The lesson for the entire IT industry is that the very best in human verification technology should be employed in all systems, but especially in systems that preserve sensitive financial and personal data like passport numbers.