The Ashley Madison 'hack' - DDSS Case Study #3

José Donato, donato@student.dei.uc.pt, 2016225043

I. Introduction

In this report I will give my point of view about the Ashley Madison hack. I will talk about its source causes, impact, prevention and mitigation. This hack occurred in 2015 and it was a data breach of more than 25 GB of sensitive data. It had a severe impact in lot of people lives because their private and sensitive information became public [1].

II. Source Causes

Avid Life Media is a company that beyond 'Ashley Madison' website has two other websites. All three with a similar goal: dating services. In case of Ashley Madison website, it offers a service where marry people can seek for casual hookups with other marry people. Only knowing this, we already know ALM is diving into a obscure business but it doesn't end here.

Because 95% of the website traffic were men, they introduced fake women profiles to talk to the men in the platform. This situation was portrayed as "bunch of men in cages talking to zombies" [1]. Note that the men in the website could create an account and setup a profile for free but then to talk to people they have to pay, so they were paying to have conversations with fake people. Following this fraud strategy, the company did also include a "full" delete feature where for 19$ the users could supposedly delete their trace in the website. Although, it didn't happen, the company kept the records of the users including sensitive information such as payment details.

All this fraud actions brought the attention of a hacker group called Impact Team. They managed to somehow get access (today the details of this penetration are still unknown but lot of people think it was an inside job) to all Ashley Madison data and threatened to exposed it all unless they shutdown the website. ALM didn't believe the hack was real and kept the website alive. In December 2015, Impact Team dumped 10GB of sensitive data including emails and all types of customer sensitive data from sexual likes and dislikes to addresses. Their motivations were this company fraud actions and they compared the company to drug dealers feeding addicts with more heroin.

This fraudulent actions were the sources of the attack. Highly motivated and experienced people like the Impact Team didn't like these actions and went far to destroy them.

III. Impacts

In the first leak more than 37 million email addresses were dumped. All the data was released on anonymous networks and soon everyone had access to it. It contained more than 15 thousand military (.mil) and government (.gov) US addresses [2]. This data was used to blackmail and the leaked emails could after be used for phishing and malware attacks. Governors, state attorneys and company CEOs admitted that they used the website and immediately resigned.

But there were far more severe consequences. This hack took lives, multiple people suicide when this data turned public and their names were associated to it. More than 30 million families were destroyed [2].

It was revealed that the CEO of ALM at the time had also affairs and resigned right away. Although, this didn't stop the company and they re branded and continued to claim that they were a respectable and "100% discrete" service.

IV. Prevention

It is true that Impact Team illegally obtained sensitive data and ruined a lot of people lives but all this could be prevented if ALM company had the right policies (for example, encrypt all sensitive data). Although the company claimed that they had a great security, they were hacked and lost all their sensitive data to the Impact Team. All this sensitive data should have been encrypted.

The company should also have permanently and irreversibly deleted the data when they said they have deleted it (remember the full delete feature). Lot of data encountered in the breach was supposedly deleted [3]. Also, users shouldn't need to pay for full privacy as we seen with the 19$ to "full" delete their information [4]. This action of trying to rip off more money from the customers was the main reason why Impact Team wanted to take down this website.

V. Mitigation

When signing up for the Ashley Madison website, lot of people used their work email addresses. This puts the work company in a position where they can be blackmailed. If one employer of a company is known to use a infidelity website, it can give leverage to adversaries. To prevent this, after the data breaches companies should always analyse the data and seek if they have vulnerable/exposed employers or not [5].

In the process of registering in the website, lot of users signed up with their personal email addresses. This is also a problem because only knowing the email, it can directly redirect to the real person since normally people use their names in the email address. Because of this, tools like haveibeenpwned (https://haveibeenpwned.com/) or exposed email checkers (https://ashley.cynic.al/) were created. Note that the company behind Ashley Madison didn't inform the users if they had been exposed because of the hack. Accessing this tools or seeing the actual data dump were the only ways to actually know if their data was leaked or not and take measures.

VI. Conclusion

Supporting my opinion on what the Impact Team said, I think the Ashley Madison data breach was a "wake up call for ordinary people that they shouldn't trust companies with their deepest secrets because they may become public" [1]. Of course this hacking group did something illegal and must be punished for it but they weren't the only bad guys in this history. The company behind Ashley Madison was as much or more guilty and should also bear the consequences.

References

[1] Cyberwar. The Ashley Madison Hack. https://www.youtube.com/watch?v=slW2yGiRTi0.

[2] Steve Mansfield-Devine. The Ashley Madison affair. https://www.researchgate.net/publication/283172894_The_Ashley_Madison_affair.

[3] Panda Security. A dating site and corporate cyber-security lessons to be learned. https://www.pandasecurity.com/mediacenter/security/lessons-ashley-madison-data-breach/.

[4] Mathew J. Schwartz. Ashley Madison Breach: 6 Lessons. https://www.bankinfosecurity.com/6-lessons-ashley-madison-breach-a-8419.

[5] Mathew J. Schwartz. Mitigating Organizational Risks After the Ashley Madison Leaks. https://www.bankinfosecurity.com/interviews/extortion-alert-ashley-madison-emails-i-2854.