Ashley Madison: a new darker stage of cyber hacking

By Gary Newe

11 Sep 2015

According to Gary Newe, Technical Director at F5 Networks, cybercriminals are increasingly hacking for ransom, raising concerns around data security and privacy.

JavadR via pixabay.com

In late July, Avid Life Media (ALM) - owners of online dating site Ashley Madison - confirmed it had been the victim of a massive data breach, potentially exposing the personal details and identities of millions of Ashley Madison users.

A month on and the firm's fears (not to mention the fears of its users) were confirmed when the hackers supposedly responsible, known as the Impact Team, published the names, addresses, phone numbers and credit card transaction details of around 32 million customers. The information was published via the 'Dark Web' - a semi-anonymised corner of the internet only accessible using a special Tor browser and Onion router.

Naturally, instructions on how to access the data appeared, followed by a flood of stories in the tabloids of partners who had found their other halves' details. Further coverage has included accusations that the leak was an inside job and deeper social reflection as to how or why many people actually use the site.

The dark side

From a cyber security perspective, however, Ashley Madison represents the most high-profile example yet of a new darker phase of cyber attacks. Rather than simply attempting to cause disruption and embarrassment, or to generate a bit of self-publicity, cybercriminals are increasingly hacking for ransom.

In early July, the movie streaming service Plex was hacked, with the attacker attempting to extract money from the service. A month previously, both the Bank of China and Bank of East Asia were victims of DDoS attacks, with hackers threatening these institutions with extending the attack if they didn't pay a hefty sum in Bitcoins.

The Impact Team have claimed the attack was an almost moral crusade against the firm behind Ashley Madison. According to the hackers, ALM made $1.7 million in revenue in 2014 from the full delete service, which allows users to remove site use history and personally identifiable information for a one-off cost of $19. The Impact Team claim this is not the case, with users' payment details remaining accessible.

A $3.2 billion question?

However, a more likely reason for the hack is the highly sensitive nature of the information stolen and how much money it could be worth. Imagine if the 32 million individuals whose data has been leaked to the dark web would be willing to pay $100 for it to be removed? You do the math (or if you don't fancy it - bribe revenue could be a whopping $3.2 billion) and it's clear to see how powerful a breach like the Ashley Madison hack represents.

So, what does this mean for businesses? Quite simply, the need to get serious about cybersecurity - and fast. Regardless of your views on Ashley Madison and the services it offers, the hack remains an example of the pervasive challenges businesses face in protecting the data of paying customers, with assumed implications for future revenue as well.

Many companies are simply not shifting their policies and protection quickly enough to deal with the fast-evolving security threats. If you haven't been targeted yet, you've been lucky. If organisations don't act now, hackers will continue to find new ways to compromise their systems and steal data.

Getting ahead of the hackers

Unfortunately, there is no silver bullet to protect against hackers. However, organisations should start by looking at what they're trying to protect and what it is hackers might be looking to compromise. Increasingly, the vectors of these attacks are multi-threaded. For example, while a DDoS attack might be ongoing, it is often designed to distract the security and IT team whilst hackers attack your applications surgically elsewhere to gain access to your data. The usual focus areas for these attacks are the applications, where a hacker may exploit the application logic or the people using these applications.

Putting aside any moral debate around Ashley Madison, the focus should be on how hackers are increasingly getting the better of firms, and infringing on personal freedom or the right to anonymity in the process. To prevent these attacks becoming a weekly or even daily story, the security industry and businesses across all sectors need to work together to get ahead of the hackers.

ABOUT THE AUTHOR

Gary Newe, technical director at F5 Networks