HBO breach accomplished with hard work by hacker, poor security practices by victim

scmagazine.com/home/security-news/cybercrime/hbo-breach-accomplished-with-hard-work-by-hacker-poor-security-practices-by-victim/

August 9, 2017

Doug OlenickAugust 9, 2017

Cybersecurity executives are speculating the HBO hack by “Mr. Smith” was the result of the intruder putting in a tremendous amount of effort to infiltrate the entertainment giant that included many separate attacks, while said giant most likely was slayed by ignoring basic security hygiene.

On August 7 a small treasure trove of HBO content was posted publicly to the web by a hacker who is now demanding a $6 million payment to stop any further release of data. The hacker who goes by Mr. Smith posted five scripts for Game of Thrones and a month's worth of email from HBO Vice President for Film Programming Leslie Cohen along with some other corporate information, according to the Associated Press.

The general consensus among cybersecurity insiders is the hacker was able to procure this information through a series of small attacks conducted over an extended period of time tied to poor security practices by either by HBO or perhaps a third-party vendor. Mr. Smith seemed to confirm the timeline saying the $6 million ransom amount is tied to the length of time his crew spent on the hack, about six months.

“Through a persistent effort of phishing, malware attacks and plain old social engineering, the attackers likely compromised many individual identities. Once these identities are compromised, the attackers can inject malware onto systems that over time learn more passwords and allow them lateral access into other systems on the network,” Corey Williams, Centrify's senior director of products and Marketing, told SC Media.

Another strong possibility is HBO is simply another victim of partnering with a third-party vendor that either made an error or did not have its cybersecurity ducks lined up in a row. If this turns out to be true HBO will join a long list of companies, to include Verizon, Trump Hotels, Hard Rock and Scottrade, which suffered a data breach due to one of these ancillary companies proving to be a weak link.

“They have to treat intellectual property (IP) with the same level of protection that banks treat regulated customer information – that is it should be given the highest level of IT security controls and data privacy protection. Then in those instances where a studio has outsourced to a vendor (e.g. Larson Studios and the Netflix hack), they must insure that their vendors employ equally strong security,” Brad Keller, director 3rd Party Strategy for Prevalent, said in an email interview with SC Media.

HBO launched an investigation into the initial attack that took place on August 1 when its CEO and Chairman Richard Plepler confirmed the cable company had been victimized. So far the company has not released any information.

Whatever the company discovers during its investigation, along with its decision on whether or not is should pay the $6 million ransom will prove quite educational for other media firms who may find themselves victimized in a similar manner.

As with most ransomware situations, the consensus on whether or not the victim should pay up was split. If the data is deemed more valuable than the ransom and it cannot be replicated than breaking out the corporate check book might be in order, but otherwise, if at all possible, the bad guys should not be paid off.

“It's a business decision, plain and simple. If an attacker was threatening to release the new Star Wars movie early, I'd want to understand the business impact of that. If it meant that there would be a decrease in people attending movies or buying merchandise in dollar amounts that exceeded the amount of the ransom, I'd at least consider coming to the table and negotiating,” said James Carder, CISO of LogRhythm.

However, everyone did agree that snatching IP was a smart move as it forces the company to quickly make a decision over what is essentially a product with an expiration date. And they did not rule out that despite asking for money the hacker could have an ulterior motive, one similar to the Sony hack that was focused on damaging the studio for the release of the anti-North Korea movie “The Interview.”

“"Intellectual property is particularly well suited to ransomware attacks because there is little way to repair the damage after it has been released. In the case of movies and/or episodes, there is an immediate diminution in market value,” Keller said.

Williams agreed, adding the negative consequences of pre-releasing brand defining IP can be tremendous with the possibility of subscriptions being impacted in HBO's case.

Carder did add that if a company manages to save a few dollars in negotiating to pay a lower ransom it would be smart to take that money and invest in boosting its cybersecurity. And he had a few suggestions on where to invest with the most important point made being the amount the company invests should be near the equivalent to the value of what it is trying to protect.

“Unfortunately, there isn't a silver bullet or one thing these studios can do. It's a combination of things that must happen. Studios must practice good IT and security hygiene (patching systems and applications, updating and modernizing systems/applications/infrastructure, controlling access to only those that need access, validating identities, encrypting or applying other safeguards to critical business systems and data). They also must implement stringent monitoring and alerting mechanisms as compensating controls for when or if an attacker breaks through their defenses,” Carder said.

Williams noted that even improving some basic security protocols would be a huge help. The first change he suggested is to stop relying on passwords as a line of defense to protect intellectual property. Next is to implement multifactor authentication and utilize machine learning to halts attacks as they happen.

While there are many things companies must do to increase security, the one thing they cannot do is underestimate their enemies, said Matthew Pascucci, Cybersecurity Practice Manager at CCSI.

"The HBO hack should be taken seriously. Anytime a malicious actor has your sensitive data and is releasing it to the public they've earned the right to be taken serious. How HBO responds to their demands and moves forward with the isolation of the incident will determine what needs to be done moving forward from a hardening and process perspective,” he said.

In the end it may be hard to discern what will be the final result of this attack. HBO may determine how it was done, but unless it publicly states that it paid, or the hacker makes such a disclosure, the world may not know. Unlike the NotPetya attack, which has negatively impacted the financials of FedEx and Maersk, HBO may pass through this incident unscathed. Especially if it enters into a negotiation with Mr. Smith.

“Just like with any business deal, there could be some level of negotiation and potentially some agreements made if HBO thinks that the stolen data has considerable value from a business perspective. By comparison, if you look at the effects of Sony's breach, there was

really no material impact on Sony's fiscal results the year it was breached. Most of the cost incurred was associated with the investigation and the remediation necessary to bolster their cybersecurity program, which could be seen as an investment in the long run," Carder said.

Doug Olenick

Related