http://www.darkreading.com/cloud/the-growing-danger-of-ip-theft-and-cyber-extortion/a/d-id/1329247?

The Growing Danger of IP Theft and Cyber Extortion

7/6/2017

10:30 AM

Robert McFarlane

Commentar

The Growing Danger of IP Theft and Cyber Extortion

The recent hacks of Disney and Netflix show the jeopardy that intellectual property and company secrets are in, fueled by cheap hacking tools and cryptocurrencies.

Shortly after the latest Verizon Data Breach Incident Report warned of a rise in cyber-espionage attacks aimed at stealing intellectual property (IP) and company secrets, a real-life example hit the news. Entertainment juggernaut Disney was hacked, with attackers gaining access to *Pirates of the Caribbean: Dead Man Tell No Tales,* and threatening to release the movie in five-minute increments until a ransom of an undisclosed amount was paid. Disney has refused.

This follows on the heels of another high-profile entertainment theft; a hacker stole 10 unreleased episodes of Netflix's series *Orange Is the New Black* and threatened to dump them online unless the company paid a hefty ransom in Bitcoin. Netflix refused, and the episodes were posted on the Internet.

Yes, Your Company Should Worry About IP Theft

The Verizon report notes that cyber espionage is of particular concern in the manufacturing industry, where it accounts for 90% of cyber attacks.

Most of these cyberspy operations are perpetrated by state actors who are stealing cutting-edge technology for use in their home countries.

However, as the Disney hack illustrates, companies don't have to be developing pest-resistant supercrops or gene therapy to become targets. Some businesses scoff at the notion of cyber extortion, thinking that they're too unimportant to attract the attention of hackers. As the Verizon report shows, industry and size don't matter: "if you have — or may be perceived to have — useful information, then you are a potential target" for IP theft.

These days, that applies to pretty much everyone: proprietary financial technology solutions, casino gaming software, secret recipes, mobile apps, even company secrets such as data on marketing strategy, employee recruitment, or research into new products. And, of course things such as unreleased books, movies, and television series are targets.

Furthermore, you no longer have to be a well-funded foreign spy — or even particularly technically inclined — to break into enterprise systems.

Cryptocurrencies and "Malware for Dummies" Lower the Bar for Hackers

Computer hacking used to require a high level of technical prowess. A would-be hacker had to have strong coding skills and understand operating systems, network architectures, and hardware. However, the Darknet has evolved to the point where *Mr. Robot*-level technical expertise isn't necessary. Inexpensive, easy-to-use, cloud-based "malware for dummies" can be purchased. At least one group of enterprising hackers even offers customer support in case you run into problems.

The rise of cryptocurrencies such as Bitcoin has also helped cyber extortion grow. Before Bitcoin, sending and receiving very large sums of money while maintaining secrecy and anonymity wasn't something just anyone could do. Now, anyone can sign up for a Bitcoin account and send, receive, and spend as much money as they want, without anyone knowing who or where they are.

Third-Party Vendors Can Put Large Enterprises at Risk

The Netflix hack shone a light on another problem with IP security: large companies are only as secure as their third-party business associates.

Generally, hackers used to target the payment systems or databases of large corporations in search of card data or sensitive personal data, such as Social Security numbers. Targeting a very small company wasn’t worth the effort. Now, with easy-to-use hacking tools, untraceable payment methods, and the fact that companies (including many third-party vendors) store millions of dollars' worth of intellectual property on their networks, cybercriminals are getting creative.

The intruders didn't have to penetrate Netflix itself; they hacked Netflix's third-party post-production vendor, Larson Studios. In a similar vein, criminals could hack into a clothing brand's textile vendor and steal all of their patterns for next season or hack into reality TV contestants' phones and reveal the winner of the current season before the finale airs.

In some cases, breaking into one small vendor can be more lucrative than breaching a multinational. Because Larson Studios sells post-production services to many television networks, it is likely that more extortion attempts are coming.

Combatting IP Cybertheft

Cyber insurers have noticed third-party vendor vulnerabilities for some time; some policies require that organizations ensure the security of their business associates' systems. That's easier said than done. While large companies like Disney can afford to implement Fort Knox-level security on their systems, such measures may break smaller firms' budgets. However, Disney and Netflix show that a large budget alone doesn't guarantee safety from intrusion.

One client-side solution is network segmentation, in which companies create an isolated system for the vendor to work on tasks with a standalone setup, minimal connection to the company's main system, and as small a digital footprint as possible. However, there are costs involved, and in some cases (likely in the Netflix case) the vendor may need highly specialized software and hardware to do its work, which makes creating such an isolated system impossible.

Another, less-expensive solution is for vendors to work entirely in the cloud, isolated from the larger company's system. Vendors shouldn't be able to download data onto their own networks, and the cloud solution should be secured with two-factor authentication with a key fob or app to

avoid the usual security concerns concerning login credentials. This setup isn't foolproof, and it may require vendors to invest in faster connections or deal with slower speeds, but it would ease some of their financial burden.

Finally, organizations of all sizes should consider partnering with a managed security services provider (MSSP). (Note: Mosaic451 is an MSSP, but many other companies offer these services.) Using an MSSP is less expensive than performing cybersecurity functions in-house, especially since the organization doesn't have to make additional investments in security personnel, software, and hardware.

With so much intellectual property being stored digitally, IP theft and cyberextortion are likely to become as big a problem as ransomware. It's imperative for companies of all sizes to get out ahead of this threat, understand the risks, and implement proactive measures to prevent it.

http://www.darkreading.com/author-bio.asp?author_id=3777

Profile of Robert McFarlane

Chief Revenue Officer

Member Since: 6/28/2017

Author

News & Commentary Posts: 1

Comments: 1

Robert McFarlane is the Chief Revenue Officer of Mosaic451, a managed security services provider (MMSP) and consultancy. He has 20-plus years of business development in telecom, data networking, and cybersecurity. He has contributed to the growth, establishment, and expansion of companies ultimately acquired by EarthLink and Comcast.

McFarlane is a Chief Petty Officer in the United States Navy Reserves, Information Warfare Community, with tours in Iraq and Afghanistan. He also serves on the CompTIA Partner Advisory Board & Cyber Security Advisory Council.