2018's worst cyber-security breaches

Written by My Office News (http://myofficemagazine.co.za/author/leigh/) on 11th July 2018. Posted in Tech News (http://myofficemagazine.co.za/category/news/tech-news/).

By Lily Hay Newman for Wired (https://www.wired.com/story/2018-worst-hacks-so-far/)

Looking back at the first six months of 2018, there haven't been as many government leaks and global ransomware attacks as there were by this time last year, but that's pretty much where the good news ends. Corporate security isn't getting better fast enough, critical infrastructure security hangs in the balance, and state-backed hackers from around the world are getting bolder and more sophisticated.

Here are the big digital security dramas that have played out so far this year—and it's only half over.

Russian grid hacking

In 2017, security researchers sounded the alarm about Russian hackers infiltrating and probing United States power companies; there was even evidence that the actors had direct access to an American utility's control systems. Combined with other high-profile Russian hacking from 2017, like the NotPetya ransomware attacks, the grid penetrations were a sobering revelation. It wasn't until this year, though, that the US government began publicly acknowledging the Russian state's involvement in these actions. Officials hinted at it for months, before the Trump Administration first publicly attributed the NotPetya malware to Russia in February and then blamed Russia in March for grid hacking. Though these attributions were already widely assumed, the White House's public acknowledgement is a key step as both the government and private sector grapple with how to respond. And while the state-sponsored hacking field is getting scarier by the day, you can use WIRED's grid-hacking guide to gauge when you should really freak out.

US universities
In March, the Department of Justice indicted nine Iranian hackers over an alleged spree of attacks on more than 300 universities in the United States and abroad. The suspects are charged with infiltrating 144 US universities, 176 universities in 21 other countries, 47 private companies, and other targets like the United Nations, the US Federal Energy Regulatory Commission, and the states of Hawaii and Indiana. The DOJ says the hackers stole 31 terabytes of data, estimated to be worth $3 billion in intellectual property. The attacks used carefully crafted spearphishing emails to trick professors and other university affiliates into clicking on malicious links and entering their network login credentials. Of 100,000 accounts hackers targeted, they were able to gain credentials for about 8,000, with 3,768 of those at US institutions. The DOJ says the campaign traces back to a Tehran-based hacker clearinghouse called the Mabna Institute, which was founded around 2013. The organization allegedly managed hackers and had ties to Iran's Islamic Revolutionary Guard Corps. Tension between Iran and the US often spills into the digital sphere, and the situation has been in a particularly delicate phase recently.

Rampant data exposures
Data breaches have continued apace in 2018, but their quiet cousin, data exposure, has been prominent this year as well. A data exposure, as the name suggests, is when data is stored and defended improperly such that it is exposed on the open internet and could be easily accessed by anyone who comes across it. This often occurs when cloud users misconfigure a database or other storage mechanism so it requires minimal or no authentication to access. This was the case with the marketing and data aggregation firm Exactis, which left about 340 million records exposed on a publicly accessible server. The trove didn't include Social Security numbers or credit card numbers, but it did comprise 2 terabytes of very personal information about hundreds of millions of US adults —not something you want hanging out for anyone to find. The problem was discovered by security researcher Vinny Troia and reported by WIRED in June. Exactis has since protected the data, but it is now facing a class action lawsuit over the incident.

Cloud leaks pop up regularly, but data exposures can also occur when software bugs inadvertently store data in a different format or location than intended. For example, Twitter disclosed at the beginning of May that it had been unintentionally storing some user passwords unprotected in plaintext in an internal log. The company fixed the problem as soon as it found it, but wouldn't say how long the passwords were hanging out there.

After the revelation of a data exposure, organizations often offer the classic reassurance that there is no evidence that the data was accessed improperly. And while companies can genuinely come to this conclusion based on reviewing access logs and other indicators, the most sinister thing about data exposures is that there's no way to know for sure what exactly went down while no one was watching.

Under Armour
Hackers breached Under Armour's MyFitnessPal app in late February, compromising usernames, email addresses, and passwords from the app's roughly 150 million users. The company discovered the intrusion on March 25 and disclosed it in under a week—some welcome hustle from a large company. And it seems Under Armour had done a good enough job setting up its data protections that the hackers couldn't access valuable user information like location, credit card numbers, or birth dates, even as they were swimming in login credentials. The company had even protected the passwords it was storing by hashing them, or converting them into unintelligible strings of characters. Pretty great, right? There was one crucial issue, though: Despite doing so many things well, Under Armour admitted that it had only hashed some of the passwords using the robust function called bcrypt; the rest were protected by a weaker hashing scheme called SHA-1, which has known flaws. This means that attackers likely cracked some portion of the stolen passwords without much trouble to sell or use in other online scams. The situation, while not an all-time-worst data breach, was a frustrating reminder of the unreliable state of security on corporate networks.

One to watch: VPNFilter
At the end of May, officials warned about a Russian hacking campaign that has impacted more than 500,000 routers worldwide. The attack spreads a type of malware, known as VPNFilter, which can be used to coordinate the infected devices to create a massive botnet. But it can also directly spy on and manipulate web activity on the compromised routers. These capabilities can be used for

diverse purposes, from launching network manipulation or spam campaigns to stealing data and crafting targeted, localized attacks. VPNFilter can infect dozens of mainstream router models from companies like Netgear, TP-Link, Linksys, ASUS, D-Link, and Huawei. The FBI has been working to neutrallise the botnet, but researchers are still identifying the full scope and range of this attack.

Related

(http://myofficemagazine.co.za/cyberattackers-hit-olympic-opening-ceremony/)
Cyberattackers hit Olympic opening ceremony
(http://myofficemagazine.co.za/cyberattackers-hit-olympic-opening-ceremony/)
14th February 2018
In "Crime Alert"

(http://myofficemagazine.co.za/top-cybersecurity-tips-small-businesses/)
Top cybersecurity tips for small businesses
(http://myofficemagazine.co.za/top-cybersecurity-tips-small-businesses/)
13th September 2017
In "Crime Alert"

(http://myofficemagazine.co.za/hackers-hindered-pen-paper/)
Hackers hindered by pen and paper
(http://myofficemagazine.co.za/hackers-hindered-pen-paper/)
21st March 2017
In "Crime Alert"

Tags: breaches (http://myofficemagazine.co.za/tag/breaches/), cyber security (http://myofficemagazine.co.za/tag/cyber-security/), hackers (http://myofficemagazine.co.za/tag/hackers/), leaks (http://myofficemagazine.co.za/tag/leaks/), technology (http://myofficemagazine.co.za/tag/technology/)

< Previous (http://myofficemagazine.co.za/sas-broadband-speed-ranking/)

Next > (http://myofficemagazine.co.za/absa-now-offers-whatsapp-banking/)