Recent Egregious Data Breaches: How They Happened

by Sharon D. Nelson and John W. Simek

We should be grateful for other peoples' data breaches – they help us to improve our own security. In our breach-a-day world, we seem to have more data breaches than ever. They come fast and furious – rare is the day when we don't hear of one or more breaches on the evening news or through online media. Attack vectors change constantly – those of us in information security have a deep sense of humility in the face of constant changes in threats as well as technology, policies and training to defend against those threats.

Herewith, a few of the famous data breaches of 2015 (and one from 2014) with lessons to be learned from how they happened.

Office of Personnel Management

This was probably the most controversial breach of 2015. In May, the federal Office of Personnel Management (OPM) reported a breach affecting 4.2 million current and former federal employees. A few days later, it revealed a second breach (lesson here: don't speak too quickly about data breach specifics). The second breach brought the number impacted to 22 million people who had applied for government jobs or security clearances. Data from some applicants' family members was also compromised. The data taken included names, addresses, names of relatives, employment histories and health care histories. There was a lot of talk about the fact that 5.6 million digital fingerprints were compromised, giving rise to concern about the security of biometrics. Members of law enforcement, the intelligence community and the federal court system were all impacted. Some of the data included information on peoples' sex lives, drug and alcohol problems and debts, all of which could be used for blackmail.

The press confirmed through multiple sources that the government had concluded that China was behind the hack. But it declined to overtly accuse China because revealing technical details of how they attributed the breach to China would tip off hackers to the ways that American intelligence agencies track them.

Computer security firm CrowdStrike, which has close ties to U.S. law enforcement, said it had traced the breach to hackers it said were "affiliated with the Chinese government," using forensic information from the hack provided by the government. The Director of OPM resigned.

The breach went undetected for 343 days – it was ultimately discovered when anomalous SSL traffic and a decryption tool were observed within the network.

Though the U.S. has not talked publicly about how the breach happened, U.S. Department of Homeland Security official Andy Ozment testified that the attackers had gained valid user credentials to the systems they were attacking, likely through social engineering.

VTech Holdiings

This Hong Kong digital company was the victim of one of the year's biggest hacks in November when its Learning Lodge database was compromised, permitting hackers to get adults' profile information, e-mail addresses, passwords, chat logs and audio files - and the names, home addresses, first names and birthdates of millions of children and their photographs. Some of the audio recordings were of children's voices from VTech's Kid Connect, a service that allows parents and kids to chat via a mobile phone app and a VTech tablet. The release of the information of children was particularly disturbing and garnered a lot of publicity.

So how did the information of over 6 million people get exposed? According to security researchers, the hacker used a SQL injection to gain root access to VTech's web and database servers. Users' passwords weren't properly scrambled and hashed. The MD5 algorithm that VTech used had been known to be vulnerable for a decade or more. Worse yet, the company stored customers' security questions and answers in plain text, a clear security no-no. The reported hacker said that the entire purpose of the hack was to expose the security flaws and said he would not use or publish the data.

Besides mishandling the data from a security perspective, one wonders why the company needed to store this much data to fulfill its business purposes. It is a common problem – storing data one does not need, which itself creates a potential vulnerability.

Anthem

In February, heath insurer Anthem said that hackers had accessed its servers and downloaded the personal data of employees and those who were insured by Anthem. Even those who were not Anthem customers may have been impacted because Anthem handles paperwork for smaller insurers. Data stolen included names, addresses, birthdates, Social Security numbers, and employment information, including salaries. 79 million records were compromised and dumped online – this was the largest data breach of 2015.

This breach occurred because the hackers had gained access to the login credentials of employees with system access. How? Reportedly, the credentials were obtained through a watering hole attack. A watering hole attack is a security exploit in which the attacker seeks to compromise a specific group of end users by infecting websites that members of the group are known to visit. The goal is to infect a targeted user's computer and gain access to the network at the target's place of employment.

In this case the attackers created a bogus domain name "we11point.com" (based on Wellpoint, the former name of Anthem). In this cases, the hackers set up subdomains which were designed to mimic real services such as human resources, a VPN and Citrix server. By then sending phishing e-mails, users may have been lured to infected websites and entered their log-in credentials. A number of security companies believe the hack came from Deep Panda, a Chinese-based hacking group.

The breach was undetected for nine months and was discovered when a systems administrator noticed that a legitimate account was querying internal databases but without the legitimate user's knowledge.

There are similarities between this attack and the breach of Premera Blue Cross in 2015, impacting 11 million people – are they related? Impossible to say, but another bogus domain name "prennera.com" was discovered in the Anthem investigation.

Pentagon

In July, alleged Russian hackers hacked an unclassified e-mail server of the Pentagon. U.S. officials announced that Russia had launched a "sophisticated cyberattack" against the Pentagon's Joint Staff unclassified e-mail system. The officials added that the cyber-attack compromised data belonging to 4,000 military and civilian personnel who worked for the Joint Chiefs of Staff.

As the attack was later described a “spear phishing attack”, it doesn’t on the face of it sound all that sophisticated. However, Department of Defense officials continued to call it the "most sophisticated" cyberbreach in U.S. military history. Officials spent 10 days scrubbing the system and creating mock hacking scenarios before giving military personnel access to it again. The spear phishing attack targeted the personal information of scores of users. What may have made this attack sophisticated is that the hackers used “an automated system rapidly gathered massive amounts of data and within a minutes distributed all the information to thousands of accounts on the Internet.” Encrypted social media accounts were used to coordinate the attack. If true, that might qualify this attack for the adjective “sophisticated.”

Sony

The Sony Pictures Entertainment hack involved the release of confidential data belonging to Sony Pictures Entertainment on November 24, 2014. The data included personal information about Sony Pictures employees and their families, e-mails between employees, information about executive salaries at the company, copies of (previously) unreleased Sony films, and other information. The hackers called themselves the "Guardians of Peace" or "GOP" and demanded the cancellation of the planned release of the film *The Interview*, a comedy about a plot to assassinate North Korean leader Kim Jong-un. United States intelligence officials, evaluating the software, techniques, and network sources used in the hack, allege that the attack was sponsored by North Korea. North Korea denied all responsibility**.**

Sony’s network appeared to have been breached for more than a year.

According to the FBI: *"[A] technical analysis of the data deletion malware used in this attack revealed links to other malware that the FBI knows North Korea previously developed. For example, there were similarities in specific lines of code, encryption algorithms, data deletion methods, and compromised networks.*

The FBI also observed significant overlap between the infrastructure used in this attack and other malicious cyber activity the U.S. government has previously linked directly to North Korea. For example, the FBI discovered that several Internet protocol (IP) addresses associated with known North Korean infrastructure communicated with IP addresses that were hardcoded into the data deletion malware used in this attack. The FBI later clarified that the source IP addresses were associated with a group of North Korean businesses located in Shenyang in northeastern China.

Separately, the tools used in the SPE attack have similarities to a cyber-attack in March of last year against South Korean banks and media outlets, which was carried out by North Korea.”

The FBI later clarified more details of the attacks, attributing them to North Korea by noting that the hackers were "sloppy" with the use of proxy IP addresses that originated from within North Korea. FBI Director James Comey stated that Internet access is tightly controlled within North Korea, and as such, it was unlikely that a third party had hijacked these addresses without allowance from the North Korean government. The National Security Agency assisted the FBI in analyzing the attack, specifically in reviewing the malware and tracing its origins; NSA director Admiral Michael Rogers agreed with the FBI that the attack originated from North Korea. A disclosed NSA report published by *Der Spiegel* stated that the agency had become aware of the origins of the hack due to its own cyber-intrusion on North Korean's network that they had set up in 2010, following concerns of the technology maturation of the country.

That last sentence struck a chord with us: It is possible that we were watching the hack while deeply embedded in North Korea's networks – or at least were able to learn all we needed to know once the data was disclosed. Everything else said above may have been simply "window dressing" to avoid disclosing our own government's surveillance of North Korea.

Ashley Madison

The Ashley Madison dating site breach impacted 37 million people and gave high-value entertainment fodder to pundits everywhere. This was an unusual hack, in that it seemed to be rooted in the moral convictions of the hackers, called The Impact Team. They wanted the site, whose tagline is "Life is short. Have an affair," to take the site down. They also wanted Avid Life Media's "EstablishedMen.com" site taken down. When the site's owner refused to take the sites down, the data was made public in spurts.

The breach was reported in July, and data compromised included e-mails, names, home addresses, sexual fantasies and credit card information. All of the user data released on August 18, 2015. More data (including some of the CEO's emails) was released on August 20, 2015. The release included data from customers who had earlier paid a $19 fee to Ashley Madison to allegedly have their data deleted. It turned out to be a boon to divorce lawyers everywhere. No doubt many members were shocked to find out that most of the women on the site were "bots" – employees who pretended an interest in an affair as part of inducing additional payments to Ashley Madison – and of course users had no clue that they had agreed to the use of bots when they accepted the terms of service.

The data was made vulnerable by a bad MD5 hash implementation. We are not sure how the hack actually happened but The Impact Team itself said this: "Nobody was watching. No security. Only thing was segmented network. You could use Pass1234 from the internet to VPN to root on all servers."

In an interesting side note, as of January 1, 2016 Ashley Madison's membership has supposedly increased by more than 4 million since the breach. Did it really increase or has Ashley Madison perfected its bot logic. Go figure.

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, information security and digital forensics firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com, snelson@senseient.com; jsimek@senseient.com.