BE CAREFUL WHERE YOU CLICK

Timothy L. Baker
University of South Carolina

In 2012, the South Carolina Department of Revenue (SCDOR) experienced one of the largest known breaches of taxpayer data known to date. Subsequent investigation revealed the SCDOR breach utilized a common social engineering scheme.

The extent of the breach affected millions of taxpayers, their dependents, and over 700,000 businesses. The full impact of the breach from potential identity theft is still unknown. The State of South Carolina paid for credit monitoring services for affected taxpayers until late 2018. The investigation by various Federal and State law enforcement agencies is still ongoing.

The State of South Carolina implemented a task force to make decisions concerning the breach. The task force must solve the issues surrounding the breach by answering three questions, 1) What happened, 2) What steps to take immediately, and 3) What steps to take long term.

INTRODUCTION

On a brisk evening in late October 2012, South Carolina Governor Nikki Haley stepped up to a microphone at a press conference and grimly stated *"this is not a good day for South Carolina. South Carolina has come under attack by an international hacker."* Haley said she knew where the attack originated, but would not disclose the location so not to jeopardize the investigation. She further added, *"I want this person slammed against the wall. I want that man just brutalized."*

BACKGROUND

August 13, 2012, started like any other Monday. Employees were reporting for work at the South Carolina Department of Revenue (SCDOR). Many individuals routinely began the day by checking e-mails that arrived over the weekend. One executive opened an attachment to an unusual email, and then deleted the e-mail and continued with the day.

That fall, the United States Secret Service detected identity theft on three South Carolina taxpayers. The Secret Service informed South Carolina State officials on October 10. On October 12, the State of South Carolina hired cybersecurity firm

Mandiant to investigate the possibility of a data breach, and offer short and long-term recommendations.

INVESTIGATION

Mandiant used forensic tools and log analysis to determine that a malicious e-mail was sent to several employees of SCDOR. The e-mail used a link that allowed the hackers to access the username and password of those clicking on the link to access the attachment.

The analysis provided by Mandiant showed that the hackers logged into the compromised employee's computer using remote access service beginning on August 27. Software deployed by the attackers allowed them to obtain passwords for other users' accounts on the network. The intruders also installed software on one server to allow for backdoor access to the systems of SCDOR.

Starting in early September of 2012, the hackers began accessing and investigating the contents of various servers using the stolen credentials. On September 12, the attackers created a staging directory on a server and began copying database backup files to that location. Over the following two days, the hackers used compression utilities to encrypt the files into 14 archives. The attackers uploaded the files to an off-site location, and next deleted them on the SCDOR servers. An additional archive was uploaded that contained files from the SCDOR website and an encrypted version of the encryption key.

The hackers gained additional network access to investigate the network, but Mandiant did not detect further by the attackers. Between October 19 and 20, SCDOR executed recommendations by Mandiant to remove the ability of the attackers to access the network environment and detect any subsequent attempts to access those resources.

PUBLIC DISCLOSURE

Governor Nikki Haley first informed the public during a press conference held on October 26, 2012, that a breach had occurred at SCDOR affecting 3.8 million taxpayers, their 1.9 million dependents, and 700,000 businesses. Additionally, the breach exposed 3.3 million bank accounts and 5,000 credit cards. The Governor stated, *"There wasn't anything where anyone in state government could have done anything to avoid it."* She further explained that the State of South Carolina was using compliant with recommendations made by the Internal Revenue Service (which did not require encryption of sensitive data, including taxpayer social security number). She vowed to the citizens of South Carolina that the perpetrator(s) of the breach would be found and prosecuted.

Exhibit 1: Timeline of Events

ADDITIONAL DISCOVERY AND DISCLOSURE

State Legislature hearings regarding the security breach revealed details of dynamics within the state agencies that cast a different light on the matter. The hearings exposed a conflict between the previous Chief Information Officer (CIO) and Chief Information Security Officer (CISO) at SCDOR. The former CISO stated that the CIO had ignored his specific recommendations and repeated requests for data encryption of sensitive information including taxpayer social security numbers and the need for multi-factor authentication.

Following the Mandiant recommendations and legislative hearings, Governor Haley backtracked on her initial statement-denying fault for the breach by saying *"All the information that was compromised…is plugged, is secure, and is, um safe and…so there are no more holes and anything that can be penetrated."* Referencing the findings and recommendations by Mandiant Haley stated further *"The main question that I asked Mandiant yesterday was, 'Did we have a chance to do a better job'….And we did."* After initially faulting the IRS for failing to make clear that their rules do not require encryption, she nevertheless acknowledged it was her responsibility saying, *"I ultimately am saying that South Carolina is at fault for not doing this. I should have asked the extra question. I should have said, 'Does this include encryption?'"* Haley further explained the breach by saying *"When you combine the fact that we had 1970 equipment…with the fact that we were IRS-compliant was a cocktail for attack. And the reason I say this is the IRS, which we were compliant with does not believe you have to encrypt Social Security numbers."*

In December of 2012, the State of SC began mailing letters to those compromised in the attack. The letter offered tips for identity theft detection and prevention. The State of South Carolina contracted with an identity theft monitoring service for taxpayers that wished to enroll. The State of South Carolina paid for the monitoring service until late 2018.

The State of South Carolina experienced the largest breach of State taxpayer data in history. They knew they needed to make improvements to protect the information assets of the State and its stakeholders. Governor Haley pledged, *"We are going to have a very strong approach to make sure every South Carolina taxpayer is protected. No taxpayer should be a victim to this. We will take care of them."*

FAST FORWARD

In 2013, the court dismissed a case brought by former state senator John Hawkins against Governor Haley, the judge stating the lawsuit had failed to prove that Gov. Nikki Haley and other government officials had harmed the public by conspiring to keep news of the hacking secret.

News regarding the progress of the investigation of the massive data breach dried up promptly. The most recent article appeared in The State newspaper in 2013.

As of early 2019, almost seven years later, the mystery surrounding the largest data breach of state taxpayer data in US history remains, at least in the public domain. Initially, speculation that members of an Eastern European crime syndicate – one with alleged ties to the Russian government – were responsible for the hack, but has not been confirmed. No formal investigative report was issued to the public. There have been no indictments in the crime. The State of SC experienced a great loss of data concerning its taxpayers. They learned that better data protection should be in place. What should they do to improve the future?

References

Associated Press (2019, January 2). SC cybersecurity 6 years after 6 million tax records stolen. Retrieved from https://apnews.com/81314667903042e587dd155292bef11d

Dark Reading (2012). How South Carolina Failed to Spot Hack Attack. Dark Reading. Retrieved from https://www.darkreading.com/attacks-and-breaches/how-south-carolina-failed-to-spot-hack-attack/d/d-id/1107515?print=yes

Deloitte (2013). State of South Carolina Information Security and Privacy Final Report. Deloitte. Retrieved from https://www.admin.sc.gov/files/InfoSec%20-%20Public%20Final%20Report%20-%201Dec2014.pdf

MANDIANT (2012). South Carolina Department of Revenue Public Incident Report. MANDIANT. Retrieved from https://oag.ca.gov/system/files/Mandiant%20Report_0.pdf

SC Media (2012). S.C. tax breach began when employee fell for spear phish. SC Media. Retrieved from https://www.scmagazine.com/home/security-news/s-c-tax-breach-began-when-employee-fell-for-spear-phish/

The Greenville News (2013, February 27). Security gaps still exist 4 months after S.C. data breach. The Greenville News, Greenville, SC. Retrieved from https://www.usatoday.com/story/news/nation/2013/02/27/hacker-south-carolina/1951719/

The Tax Advisor (2013). South Carolina Taxpayer Information Stolen. AICPA, Durham, NC. January 2013 44(1) 6.

Tripwire (2012). South Carolina Department of Revenue Breach: What Went Wrong? Tripwire. Retrieved from https://www.tripwire.com/state-of-security/security-data-protection/south-carolina-department-of-revenue-data-breach-what-went-wrong/