

# **South Carolina Department of Revenue**

Public Incident Response Report

November 20, 2012



## **EXECUTIVE SUMMARY**

### **BACKGROUND**

On October 10, 2012, a law enforcement agency contacted the South Carolina Department of Revenue (DoR) with evidence that Personally Identifiable Information (PII) of three individuals had been stolen. The Department of Revenue reviewed the data provided and identified that the data provided would have been stored within databases managed by the Department of Revenue. On October 12, 2012, Mandiant was contracted by the Department of Revenue to perform an incident response.

Mandiant's objectives were to:

- Determine if the attack was ongoing.
- Confirm the initial method of intrusion and its timing.
- Determine the scope of the compromise.
- Determine data loss/exposure.
- Perform immediate remediation activities.
- Develop short and long term remediation plans.

Mandiant performed the following activities to achieve these objectives:

- Met with the South Carolina Department of Revenue and Division of State Information Technology (DSIT) representatives to discuss initial evidence preservation requirements.
- Reviewed log data, created forensic images and performed forensic analysis of the web, application, and database systems that housed the PII data provided in the law enforcement notification.
- Analyzed Department of Revenue computer systems with the Mandiant Intelligent Response (MIR) technology for indicators of compromise (IOCs). MIR is a tool used by experienced investigators to look for evidence of malicious activities across a large number of systems.
- Monitored all network traffic from the Department of Revenue's single Internet egress point for evidence of ongoing malicious activity.
- Reviewed available network and security device logs for indicators of compromise.
- Collected live response data and forensic images from key systems as well as network and system logs.
- Analyzed malware to identify additional indicators of compromise.
- Analyzed evidence to identify attacker activities and additional indicators of compromise.
- Documented findings and remediation recommendations.
- Performed a PCI Forensics Investigation (PFI) as required by the Department of Revenue's acquiring bank, First Data.

Mandiant performed both on-site and off-site incident response activities from October 13, 2012 through November 16, 2012.

### **FINDINGS**

Mandiant's major findings are provided below.

#### **Summary of the Attack**

A high level understanding of the most important aspects of the compromise are detailed below.

1. August 13, 2012: A malicious (phishing) email was sent to multiple Department of Revenue employees. At least one Department of Revenue user clicked on the embedded link, unwittingly executed malware, and became compromised. The malware likely stole the user's username and password. This theory is based on other facts discovered during the investigation; however, Mandiant was unable to conclusively determine if this is how the user's credentials were obtained by the attacker.

2. August 27, 2012: The attacker logged into the remote access service (Citrix) using legitimate Department of Revenue user credentials. The credentials used belonged to one of the users who had received and opened the malicious email on August 13, 2012. The attacker used the Citrix portal to log into the user's workstation and then leveraged the user's access rights to access other Department of Revenue systems and databases with the user's credentials.
3. August 29, 2012: The attacker executed utilities designed to obtain user account passwords on six servers.
4. September 1, 2012: The attacker executed a utility to obtain user account passwords for all Windows user accounts. The attacker also installed malicious software ("backdoor") on one server.
5. September 2, 2012: The attacker interacted with twenty one servers using a compromised account and performed reconnaissance activities. The attacker also authenticated to a web server that handled payment maintenance information for the Department of Revenue, but was not able to accomplish anything malicious.
6. September 3, 2012: The attacker interacted with eight servers using a compromised account and performed reconnaissance activities. The attacker again authenticated to a web server that handled payment maintenance information for the Department of Revenue, but was not able to accomplish anything malicious.
7. September 4, 2012: The attacker interacted with six systems using a compromised account and performed reconnaissance activities.
8. September 5 - 10, 2012: No evidence of attacker activity was identified.
9. September 11, 2012: The attacker interacted with three systems using a compromised account and performed reconnaissance activities.
10. September 12, 2012: The attacker copied database backup files to a staging directory.
11. September 13 and 14, 2012: The attacker compressed the database backup files into fourteen (of the fifteen total) encrypted 7-zip<sup>1</sup> archives. The attacker then moved the 7-zip archives from the database server to another server and sent the data to a system on the Internet. The attacker then deleted the backup files and 7-zip archives.
12. September 15, 2012: The attacker interacted with ten systems using a compromised account and performed reconnaissance activities.
13. September 16, 2012 - October 16, 2012: No evidence of attacker activity was identified.
14. October 17, 2012: The attacker checked connectivity to a server using the backdoor previously installed on September 1, 2012. No evidence of additional activity was discovered.
15. October 19 and 20, 2012: The Department of Revenue executed remediation activities based on short term recommendations provided by Mandiant. The intent of the remediation activities was to remove the attacker's access to the environment and detect a re-compromise.
16. October 21, 2012 - Present: No evidence of related malicious activity post-remediation has been discovered.

## Extent of Compromise

The following points describe the extent of the compromise:

1. The attacker compromised a total of 44 systems:
  - One system had malicious software ("backdoor") installed
  - Three systems had database backups or files stolen
  - One system was used to send data out of the environment to the attacker
  - Thirty nine systems were accessed by the attacker (the attacker performed such activities as reconnaissance and password hash dumping)
2. The attacker used at least 33 unique pieces of malicious software and utilities to perform the attack and data theft activities including:
  - A backdoor
  - Multiple password dumping tools
  - Multiple administrative utilities
  - Multiple Windows batch scripts to perform scripted actions
  - Multiple generic utilities to execute commands against databases

---

<sup>1</sup> A publicly available utility used to compress and decompress files (<http://www.7-zip.org/>)

3. The attacker remotely accessed the Department of Revenue environment using at least four IP addresses.
4. The attacker used at least four valid Department of Revenue user accounts during the attack.

## **Information Exposure**

A high level description of stolen or potentially stolen information is provided below.

1. The attacker created fifteen encrypted 7-zip archives totaling approximately 8.2 GB of compressed data. The data decompressed into approximately 74.7 GB of data. The data was comprised of:
  - Fourteen total 7-zip archives that contained twenty three database backup files
  - One 7-zip archive that contained ~1,200 files related to the sctax.org web site and an encrypted version of the data encryption key
2. The twenty three database backup files contained a combination of encrypted and unencrypted data. According to the Department of Revenue, all instances of encrypted data within the various databases were encrypted using an industry standard two-key method that leveraged the AES 256-bit encryption standard. One key was used to encrypt the data ("encryption key"); the second key was used to protect the encryption key by encrypting it ("key encrypting key" or KEK).
  - The attacker stole the encrypted version of the data encryption key
  - No evidence was discovered to suggest that the attacker stole, or accessed, the key encrypting key

## **REMEDIATION**

Mandiant developed an immediate containment plan to deny the attacker access to the environment using the known methods of access. A containment plan is critical in a compromise involving potential PII and/or cardholder data loss. The Department of Revenue started implementing the containment plan on October 19, 2012 and completed containment activities on October 20, 2012. Mandiant then developed a plan to implement intermediate and longer term recommendations to enhance the Department of Revenue's security against future compromise. Those longer term recommendations are in the process of being implemented. No evidence of ongoing attacker activity post-remediation has been identified.

---

Public Incident Response Report Submitted By:

**Marshall Heilman**

*Director*

**Christopher Glyer**

*Manager*