**Capstone Project**

**Lighthouse Labs   
Cybersecurity Flex Program**

**Incident Response Report: Potential Data Breach and Extortion Attempt Affecting Premium House Lights**

**By   
Harpreet Singh Sahi**

Table of Contents

[Executive Summary 3](#_heading=h.5urtaho6oenw)

[Incident Timeline 3](#_heading=h.k5at2fqpo0u9)

[Technical Analysis 3](#_heading=h.52jq7bi23qms)

[Attack Origin and Initial Assessment 3](#_heading=h.o41fo0xihta7)

[Network Traffic Analysis 6](#_heading=h.8cksbgvxsz26)

[Web Server Access Log Analysis 7](#_heading=h.z6pl8t5b5lsw)

[Database Shell Log Analysis 7](#_heading=h.t4175hcu179l)

[Identification of Potential Vulnerabilities 8](#_heading=h.384rds13caf7)

[Incident Response 8](#_heading=h.a2bim2n0qfw5)

[Recommended Containment Steps 8](#_heading=h.qkaio6sg96s1)

[Recommended Remediation Steps 8](#_heading=h.wcmyeacpygli)

[Post-Incident Recommendations 9](#_heading=h.v2g8p21vyzdl)

[Future Protection Measures 9](#_heading=h.b1lub5iqqi7h)

[Recommended Potential Adjustments to Security Policy 9](#_heading=h.r9z5qmwhsec3)

[Conclusion 9](#_heading=h.ni9a2kcr51qi)

[References 10](#_heading=h.sdqdveqez8to)

# Executive Summary

Premium House Lights received a suspicious extortion email alleging possession of its customer database and demanding a ransom of 10 Bitcoin. The email included a snippet of customer data to substantiate the claim. Without confirmation of a breach, the company initiated an investigation. This report analyzes the extortion email and digital artifacts to determine the threat's validity, the nature and scope of the alleged compromise, and recommends incident response measures. The findings suggest a high likelihood of a data breach, necessitating immediate containment, remediation, and implementation of future preventive measures.

# Incident Timeline

The receipt time of the extortion email at support@premiumhouselights.com is key to establishing the start of the incident. Reporting this email initiates the initial assessment and triggers the incident response. Digital artifacts, such as network diagrams, Wireshark captures, access logs, session logs, database logs, and data files, are then collected and analyzed. Each artifact undergoes analysis with specific timelines. Documenting key events, such as suspicious network connections or unauthorized access attempts, based on timestamps, is crucial for understanding the incident's progression, identifying the root cause, and addressing gaps in the response process.

Technical Analysis

## Attack Origin and Initial Assessment

The extortion email, originating from the address 4C484C@qq.com and directed to support@premiumhouselights.com, serves as the initial indicator of a potential security incident. The sender's email address utilizes the qq.com domain, which is associated with Tencent, a major Chinese internet and technology company. Although not inherently malicious, this domain has been associated with various cyberattacks, spam campaigns, and phishing attempts. This association warrants a cautious approach and further scrutiny of the sender's activities. The recipient address, support@premiumhouselights.com, is a logical point of contact for such an extortion attempt, as it is publicly accessible and often monitored for customer-related inquiries.

A screenshot of a computer

AI-generated content may be incorrect.

Fig1: Extortion Email from attackers

The ransom demand of 10 Bitcoin (BTC) is characteristic of ransomware and extortion schemes due to the decentralized and anonymous nature of cryptocurrency transactions. The provided Bitcoin wallet ID, 1JQqFLmAp5DQJbdD3ThgEiJGSmX8eaaBid, requires examination using blockchain explorers and threat intelligence platforms to determine if it has been previously linked to any known malicious activities or threat actors. This analysis could provide valuable context regarding the credibility and sophistication of the threat.

The email includes a snippet of the customer database table, with fields such as contact first name, contact last name, and phone number. The data presented appears genuine and consistent with the type of information Premium House Lights collects from its customers. The inclusion of this data suggests that unauthorized access to at least a portion of the company's customer database may have occurred. This underscores the need for a thorough technical analysis to understand how this data was compromised and whether other sensitive information, like email addresses or payment details, might also be at risk.

**3.2. Analysis of Threat Actor Indicators**

Researching the email address 4C484C@qq.com through open-source intelligence and threat intelligence databases might reveal if this address has been implicated in past security incidents or is associated with known threat actors. While a lack of immediate attribution does not negate the threat, any prior history of malicious activity linked to this address would serve as a significant indicator.

Investigating the Bitcoin wallet ID 1JQqFLmAp5DQJbdD3ThgEiJGSmX8eaaBid using blockchain explorers like Blockchain.com and threat intelligence platforms like Chainalysis can reveal its transaction history and any associations with previous security incidents or known threat groups.

A diagram of a cloud network

AI-generated content may be incorrect.

Fig2: Premium House Lights Network

Network Traffic Analysis

Analyzing the phl\_webserver.pcap\_ file with Wireshark is essential for detecting any malicious activity targeting the web server. Filter traffic by Premium House Lights' web server IP addresses to focus on relevant data. Look for unusual spikes in traffic, connections to suspicious IPs or domains, and significant outbound data transfers, which may indicate data exfiltration. Examine for exploits like SQL injection or directory traversal attempts. Investigate common e-commerce vulnerabilities and identify any command and control (C2) traffic between compromised systems and attacker servers.

A screenshot of a computer

AI-generated content may be incorrect.

Fig3: Wireshark capture of Network traffic

The phl\_database.pcap\_ file should be analyzed similarly, focusing on network traffic directed to and from the database server. This analysis should aim to identify any unauthorized connection attempts, suspicious SQL queries executed against the database, or any network communication that might indicate data being transmitted from the database server to an external, unauthorized destination.

A screenshot of a computer

AI-generated content may be incorrect.

Fig4: Wireshark capture network on database server

Web Server Access Log Analysis

The phl\_access\_log.txt file provides a record of all requests made to the web server. Analyzing these logs using various log analysis tools can reveal suspicious patterns. This includes identifying requests originating from unusual or unexpected IP addresses, attempts to access sensitive files or directories on the server, or an abnormally high number of requests from a single IP address within a short timeframe, which could indicate a brute-force attack.

A screen shot of a computer screen

AI-generated content may be incorrect.   
Fig5: Analyzing requests made to the web server

Database Shell Log Analysis

The phl\_databaseshell.txt file records commands executed on the database server's command-line interface. Reviewing this log is crucial for identifying any actions at the operating system level. This includes searching for commands related to data transfers, such as the use of ftp or scp, or tools like wget or curl to send data to external servers. Any attempts to create or modify user accounts with elevated privileges, or actions aimed at altering security features or audit logs, should also be recorded.

A screenshot of a computer

AI-generated content may be incorrect.

Fig6: Analyzing commands executed on the database server

Identification of Potential Vulnerabilities

To understand the alleged data breach at Premium House Lights, it's essential to identify potential system weaknesses. These may include outdated software, misconfigured security settings, weak authentication, or vulnerabilities like SQL injection, cross-site scripting, or directory traversal attacks. Recognizing these issues is critical for improving security and preventing future breaches.

Incident Response

Recommended Containment Steps

When a data breach is confirmed, take immediate steps to contain it and prevent further damage. Isolate affected systems, such as web and database servers, from the network to prevent lateral movement or data exfiltration. Reset passwords for all potentially compromised accounts and deactivate any that are directly affected. Review and update firewall rules to block suspicious traffic. Verify the integrity and security of recent backups, storing them offline and off-site.

Recommended Remediation Steps

After containment, remediation involves identifying and patching the attack vector, removing malware, and updating vulnerable software. If necessary, restore systems from clean backups. Engage cybersecurity experts for comprehensive forensic analysis. Review and harden security configurations based on best practices and lessons learned.

# Post-Incident Recommendations

Future Protection Measures

To improve security at Premium House Lights, implement these measures: enforce multi-factor authentication for admin access, establish strong password policies, conduct regular security audits and scans, deploy a Web Application Firewall, monitor systems with logging and alerts, provide employee security training, apply Data Loss Prevention, use network segmentation, and maintain timely patch management.

Recommended Potential Adjustments to Security Policy

Premium House Lights should revise its security policies in light of recent incidents and enhance overall security. An updated Incident Response Plan (IRP) is necessary, outlining procedures for various security incidents, including ransomware and extortion. Implement a Data Handling Policy to manage the classification, storage, access, and disposal of sensitive data. Review and update the Access Control Policy to maintain the principle of least privilege. Establish a Third-Party Risk Management Policy if vendors access systems, and set up a BYOD Policy if employees use personal devices for work. Develop a Data Breach Notification Policy to comply with Ontario and Canadian regulations.

# Conclusion

The extortion email and genuine customer database snippet indicate a data breach at Premium House Lights. A technical analysis is necessary to confirm the extent, identify the attack vector, and verify any other accessed data. Immediate containment measures are crucial to prevent further damage. Remediation steps should be followed to fix vulnerabilities and remove the attacker's presence. Implementing post-incident security measures and revising policies will improve resilience against future threats. Consult legal counsel about potential data breach notification obligations in Ontario.

References :

* *A-Packets: Online PCAP Analysis and Network Traffic Insights*. (n.d.). Retrieved April 6, 2025, from <https://apackets.com/>
* Acunetix. (n.d.). *Directory Traversal Attack: Path traversal explained*. Retrieved April 6, 2025, from [https://www.acunetix.com/blog/articles/directory-traversal-path-traversal-explained/](https://www.google.com/search?q=https://www.acunetix.com/blog/articles/directory-traversal-path-traversal-explained/)
* Akamai. (n.d.). *The 8 Most Common Causes of Data Breaches*. Retrieved April 6, 2025, from <https://www.akamai.com/blog/security/8-most-common-causes-of-data-breaches>
* Amirootyet.com. (n.d.). *PCAP Analysis with Wireshark and Tshark | Digital Forensics and Incident Response*. Retrieved April 6, 2025, from [https://amirootyet.com/pcap-analysis-wireshark-tshark/](https://www.google.com/search?q=https://amirootyet.com/pcap-analysis-wireshark-tshark/)
* Bitcoin.org. (n.d.). *Choose your wallet - Bitcoin*. Retrieved April 6, 2025, from <https://bitcoin.org/en/choose-your-wallet>
* *Bitcoin Wallet* [Mobile app]. (n.d.). Google Play Store. Retrieved April 6, 2025, from [https://play.google.com/store/apps/details?id=de.schildbach.wallet&hl=en\_CA&gl=US](https://www.google.com/search?q=https://play.google.com/store/apps/details%3Fid%3Dde.schildbach.wallet%26hl%3Den_CA%26gl%3DUS)
* BitLaunch. (n.d.). *How to check your server for suspicious activity in Linux*. Retrieved April 6, 2025, from [https://www.bitlaunch.io/blog/check-server-for-suspicious-activity/](https://www.google.com/search?q=https://www.bitlaunch.io/blog/check-server-for-suspicious-activity/)
* Blockchain.com. (n.d.). *Blockchain Explorer - Bitcoin Tracker & More*. Retrieved April 6, 2025, from <https://www.blockchain.com/explorer>
* Blockstream.info. (n.d.). *Blockstream.info: Bitcoin Explorer*. Retrieved April 6, 2025, from <https://blockstream.info/>
* Bluevoyant. (n.d.). *Top 8 Incident Response Plan Templates*. Retrieved April 6, 2025, from [https://www.bluevoyant.com/resources/blog/top-8-incident-response-plan-templates](https://www.google.com/search?q=https://www.bluevoyant.com/resources/blog/top-8-incident-response-plan-templates)
* Bright Security. (n.d.). *Directory Traversal: Examples, Testing, and Prevention*. Retrieved April 6, 2025, from <https://brightsec.com/blog/directory-traversal/>
* Bright Security. (n.d.). *SQL Injection Attack: How It Works, Examples and Prevention*. Retrieved April 6, 2025, from <https://brightsec.com/blog/sql-injection-attack/>