Premium House Lights
Incident Response Report

Zehra Nur Ozer

July 2024

Table of Contents

Executive Summary

Premium House Lights Inc. experienced a recent cybersecurity breach, and this report provides an overview, creates a timeline for the incident, and makes some recommendations to mitigate the company's impact.

The breach was initiated on February 19, 2022, when unauthorized access and data filtration occurred to the company’s customer database. The detailed timeline and technical analysis of the events are presented in the following sections.

Additionally, this report outlines the mitigation strategies and post-incident recommendations for immediate and long-term actions by aligning with the NIST guidelines.

Incident Timeline

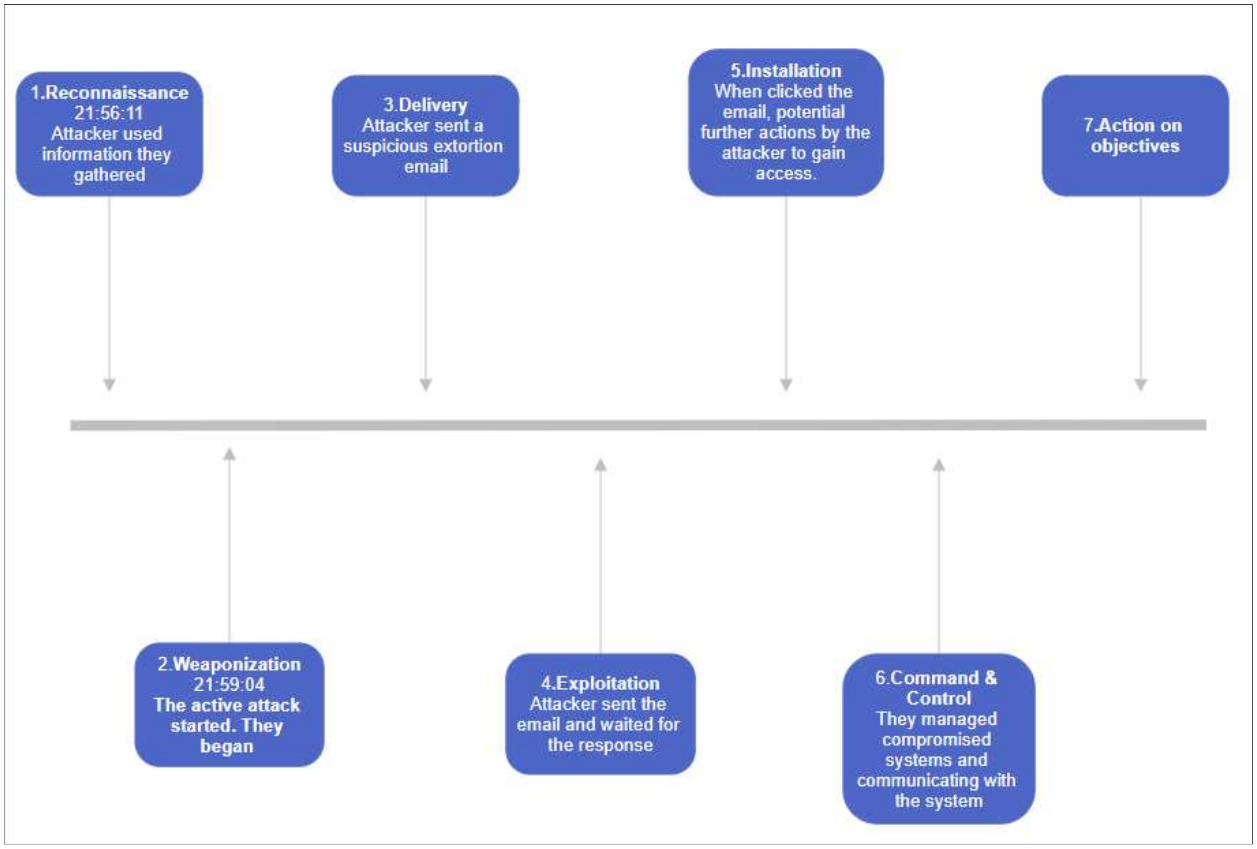

1.Reconnaissance 21:56:11 Attacker used information they gathered
3.Delivery Attacker sent a suspicious extortion email
5.Installation When clicked the email, potential further actions by the attacker to gain access.
7.Action on objectives
2.Weaponization 21:59:04 The active attack started. They began
4.Exploitation Attacker sent the email and waited for the response
6.Command & Control They managed compromised systems and communicating with the system

Figure 1Incident Timeline (by smartdraw)

Technical Analysis

Using the given artifacts listed below, the team investigated whether this was a malicious attack.

First, the team verified that this was an actual attack. Second, they collected all the potential artifacts to investigate. The team also discovered the findings using the tools listed below.

Artifacts

Company Network Diagram: Understand the network architecture to identify potential points of entry or compromise.

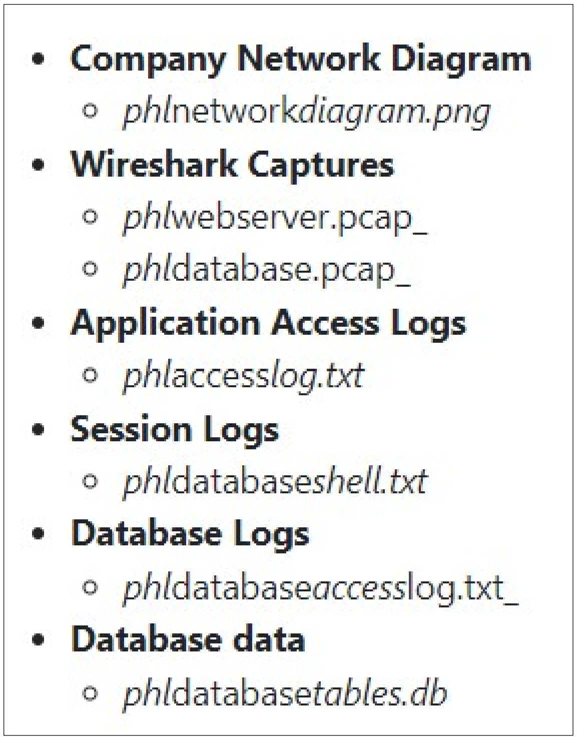
Wireshark Captures (phlwebserver.pcap_ and phldatabase.pcap_): Analyze network traffic to detect any suspicious activities or unauthorized access.

Application Access Logs (phlaccesslog.txt): Review logs for unusual access patterns or unauthorized login attempts.

Session Logs (phldatabaseshell.txt): Examine shell session logs for any unauthorized commands or activities.

Database Logs (phldatabaseaccesslog.txt_): Investigate database access logs for anomalies or unusual queries.

Database Data (phldatabasetables.db): Assess if sensitive data has been accessed or exfiltrated.



- **Company Network Diagram**
  - *phlnetworkdiagram.png*
- **Wireshark Captures**
  - *phlwebserver.pcap_*
  - *phldatabase.pcap_*
- **Application Access Logs**
  - *phlaccesslog.txt*
- **Session Logs**
  - *phldatabaseshell.txt*
- **Database Logs**
  - *phldatabaseaccesslog.txt_*
- **Database data**
  - *phldatabasetables.db*

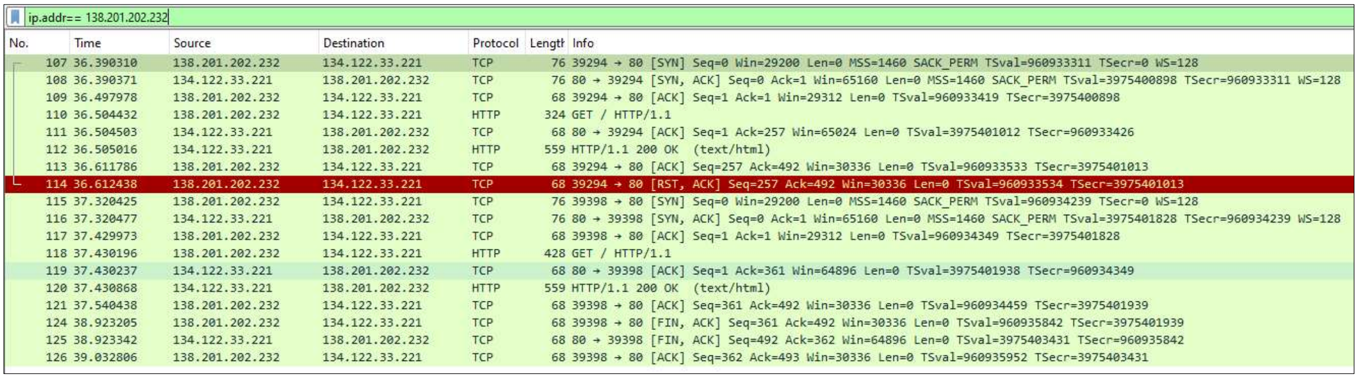
Figure 2 Artifacts for the investigation

Tools

- Wireshark v4.2.5
- Visual Studio Code
- VirusTotal.com
- Nmap
- Linux Ubuntu

Outline of Weaknesses

As the team traced the attack's origin, Virustotal.com flagged some IP addresses (136.243.111.17 and 138.201.202.232). These IP addresses made multiple requests to the web server within fractions of a second of each other. When the team analyzed the captures with Wireshark, they identified that these IP addresses were able to connect to the web server with "POST" requests and manage the unauthorized access to the server.



ip.addr== 138.201.202.232

No.	Time	Source	Destination	Protocol	Length	Info
107	36.390310	138.201.202.232	134.122.33.221	TCP	76	39294 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM TSval=960933311 TSecr=0 WS=128
108	36.390371	134.122.33.221	138.201.202.232	TCP	76	80 → 39294 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=3975400898 TSecr=960933311 WS=128
109	36.497978	138.201.202.232	134.122.33.221	TCP	68	39294 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=960933419 TSecr=3975400898
110	36.504432	138.201.202.232	134.122.33.221	HTTP	324	GET / HTTP/1.1
111	36.504503	134.122.33.221	138.201.202.232	TCP	68	80 → 39294 [ACK] Seq=1 Ack=257 Win=65024 Len=0 TSval=3975401012 TSecr=960933426
112	36.505016	134.122.33.221	138.201.202.232	HTTP	559	HTTP/1.1 200 OK (text/html)
113	36.611786	138.201.202.232	134.122.33.221	TCP	68	39294 → 80 [ACK] Seq=257 Ack=492 Win=30336 Len=0 TSval=960933533 TSecr=3975401013
114	36.612438	138.201.202.232	134.122.33.221	TCP	68	39294 → 80 [RST, ACK] Seq=257 Ack=492 Win=30336 Len=0 TSval=960933534 TSecr=3975401013
115	37.320425	138.201.202.232	134.122.33.221	TCP	76	39398 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM TSval=960934239 TSecr=0 WS=128
116	37.320477	134.122.33.221	138.201.202.232	TCP	76	80 → 39398 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=3975401828 TSecr=960934239 WS=128
117	37.429973	138.201.202.232	134.122.33.221	TCP	68	39398 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=960934349 TSecr=3975401828
118	37.430196	138.201.202.232	134.122.33.221	HTTP	428	GET / HTTP/1.1
119	37.430237	134.122.33.221	138.201.202.232	TCP	68	80 → 39398 [ACK] Seq=1 Ack=361 Win=64896 Len=0 TSval=3975401938 TSecr=960934349
120	37.430868	134.122.33.221	138.201.202.232	HTTP	559	HTTP/1.1 200 OK (text/html)
121	37.540438	138.201.202.232	134.122.33.221	TCP	68	39398 → 80 [ACK] Seq=361 Ack=492 Win=30336 Len=0 TSval=960934459 TSecr=3975401939
124	38.923205	138.201.202.232	134.122.33.221	TCP	68	39398 → 80 [FIN, ACK] Seq=361 Ack=492 Win=30336 Len=0 TSval=960935842 TSecr=3975401939
125	38.923342	134.122.33.221	138.201.202.232	TCP	68	80 → 39398 [FIN, ACK] Seq=492 Ack=362 Win=64896 Len=0 TSval=3975403431 TSecr=960935842
126	39.032806	138.201.202.232	134.122.33.221	TCP	68	39398 → 80 [ACK] Seq=362 Ack=493 Win=30336 Len=0 TSval=960935952 TSecr=3975403431

Figure 3 Wireshark capture with malicious IP

The team also identified the weaknesses that allowed the incident to occur. These incidents are

- **Insufficient Network Segmentation**: Limited segmentation between production and employee VLANs, increasing risk exposure.
- **Inadequate Firewall Rules**: Potential gaps in firewall rules allowing unauthorized external access.
- **Weak Access Controls**: Inadequate access control mechanisms for critical systems.
- **Outdated Software**: Potential vulnerabilities in outdated software versions on the webserver and database server.

Incident Response

Recommended Incident Response Playbook with Customized Workflow

Detection and Analysis:

- Immediate review of the extortion email and identification of the claimed breach.
- Collection of relevant artifacts (network diagrams, logs, Wireshark captures).

Containment:

- Isolate affected systems (webserver and database server) from the network.
- Implement temporary firewall rules to block suspicious IP addresses.

Eradication:

- Remove any identified malware or unauthorized software.
- Patch vulnerabilities in software and update systems.

Recovery:

- Restore affected systems from clean backups.
- Verify the integrity of restored data and systems.

Lessons Learned:

- Conduct a post-incident review to identify areas for improvement.
- Update incident response plans based on findings.

Steps to contain and remediate the incident

Immediate Isolation:

- Disconnect the compromised web server and database server from the network.
- Block external IP addresses identified in the Wireshark captures.

Malware Removal and System Patching:

- Scan affected systems for malware and remove any identified threats.
- Apply security patches to all systems and update software to the latest versions.

Data Integrity Verification:

- Verify the integrity of critical data and restore from backups if necessary.
- Conduct a thorough review of access logs to identify any unauthorized changes.

Post-Incident Recommendations

To safeguard against future attacks, the company should improve network segmentation by implementing more stringent controls between production and employee VLANs. It is crucial to enforce strengthened firewall rules to limit external access to critical systems and ensure robust access control mechanisms, such as multi-factor authentication, are in place.

Regular updates to all systems and software are imperative to maintain their security. Furthermore, the security policy should be updated by incorporating lessons learned from the current incident into the incident response plan.

Equally important is providing regular security training for employees to help them identify and report suspicious activities. Implementing continuous monitoring solutions will enable the company to detect and respond to security incidents in real time.

Lastly, conducting regular security audits and vulnerability assessments is essential to identify and address potential weaknesses.

References

Barker, E., Dang, Q., Frankel, S., Scarfone, K., & Wouters, P. (2020). *Guide to IPSEC VPNs*. https://doi.org/10.6028/nist.sp.800-77r1

Chatgpt. (2024, July 1). chatgpt. (2024, July 8). Chatgpt.

Cyber Kill chain. (n.d.). Lockheed Martin. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Cybersecurity Framework | NIST. (2024a, April 25). NIST. https://www.nist.gov/cyberframework

Cybersecurity Framework | NIST. (2024b, April 25). NIST. https://www.nist.gov/cyberframework

Irwin, L. (2023, March 16). *What Is the Cyber Kill Chain? Definition & Explanation - IT Governance USA Blog*. IT Governance USA Blog. https://www.itgovernanceusa.com/blog/what-is-the-cyber-kill-chain-definition-explanation

Scribbr. (2024, July 15). Scribbr.

Stine, K., Kissel, R., Barker, W. C., Lee, A., Fahlsing, J., & National Institute of Standards and Technology. (2008). NIST Special Publication 800-60 Volume II. In *Guide for Mapping Types of Information and Information Systems to Security Categories* (p. 304) [Report]. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-60v2r1.pdf (Original work published 2008)

Appendix

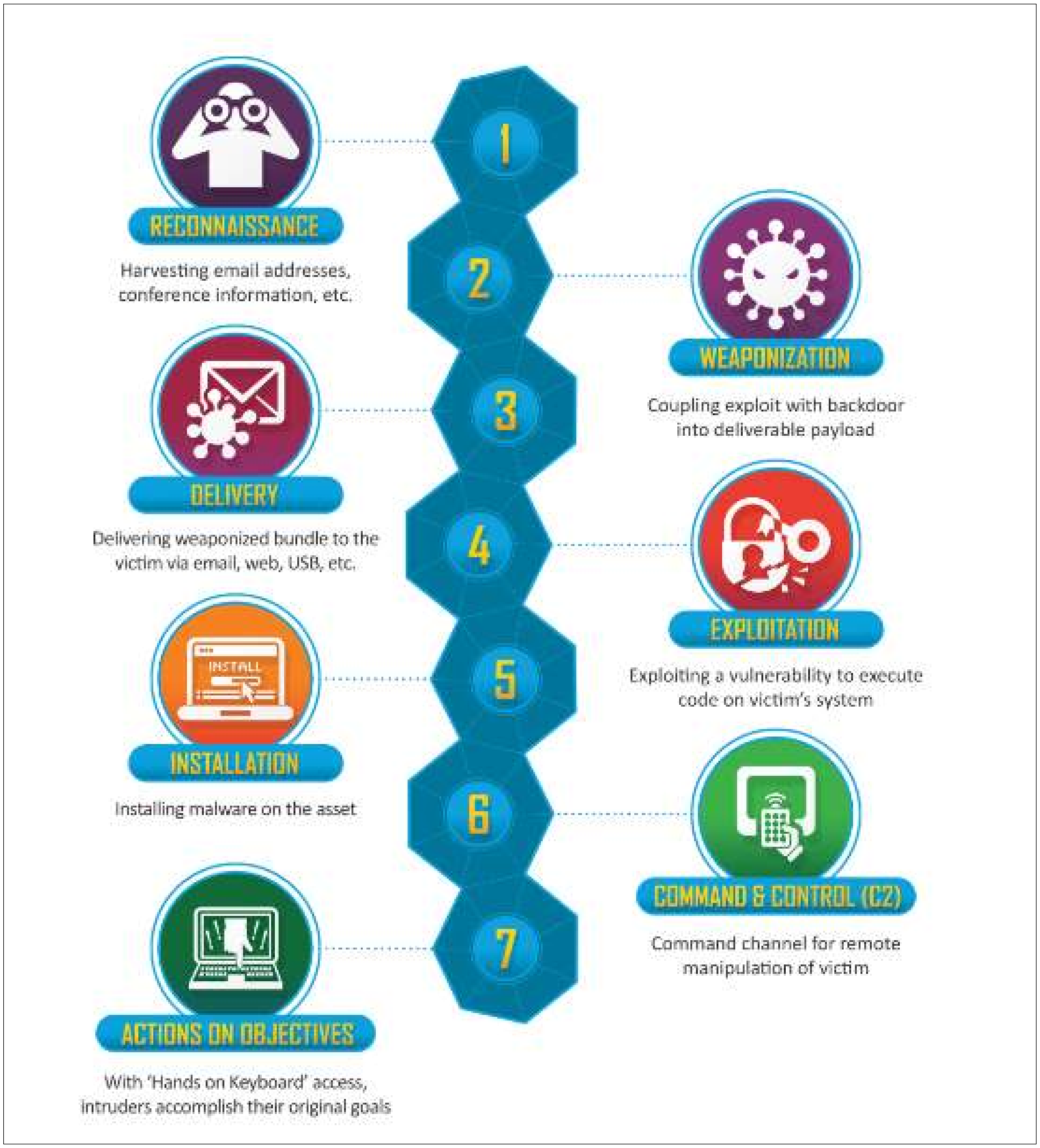
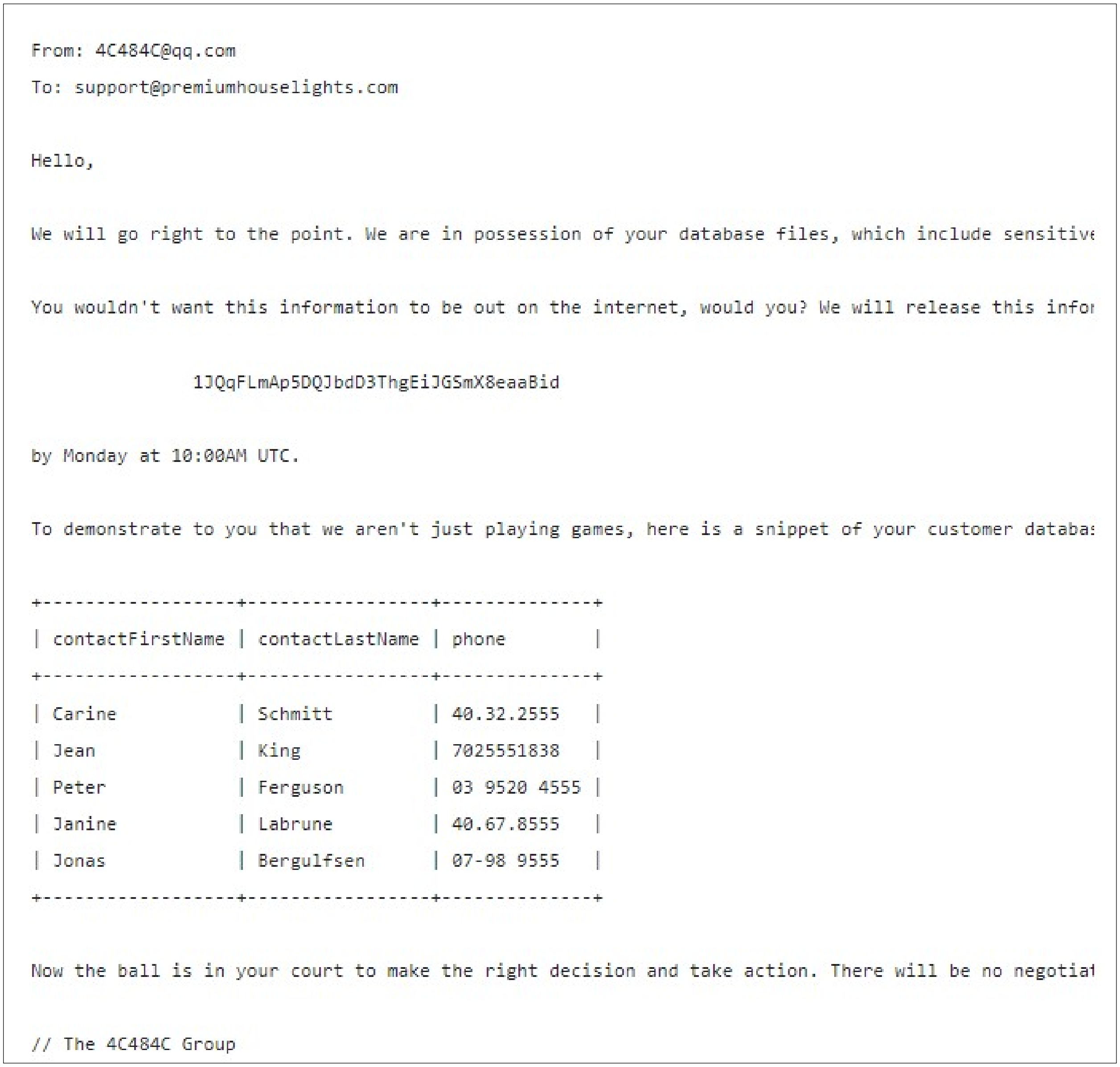

1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALL
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

Figure 4 Cyber security Kill Chain



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

You wouldn't want this information to be out on the internet, would you? We will release this infor

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 databas

```
+------------------+-----------------+--------------+
| 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 negotiat

// The 4C484C Group

Figure 5 Email that the company received