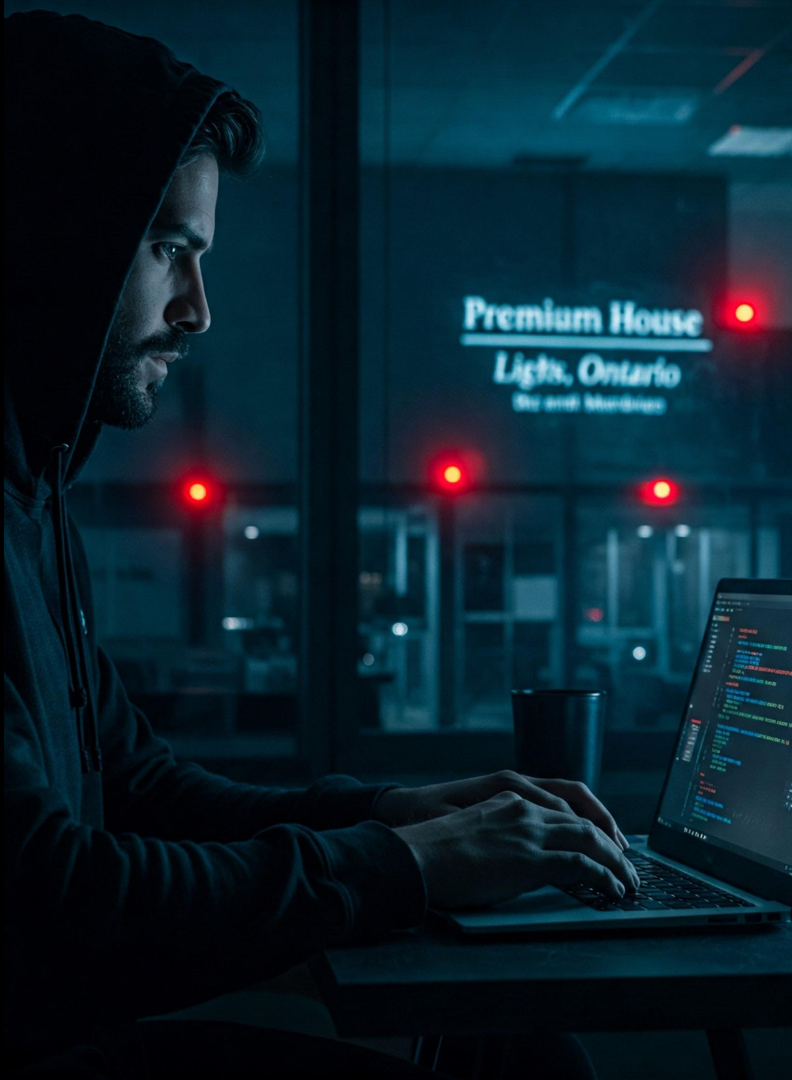
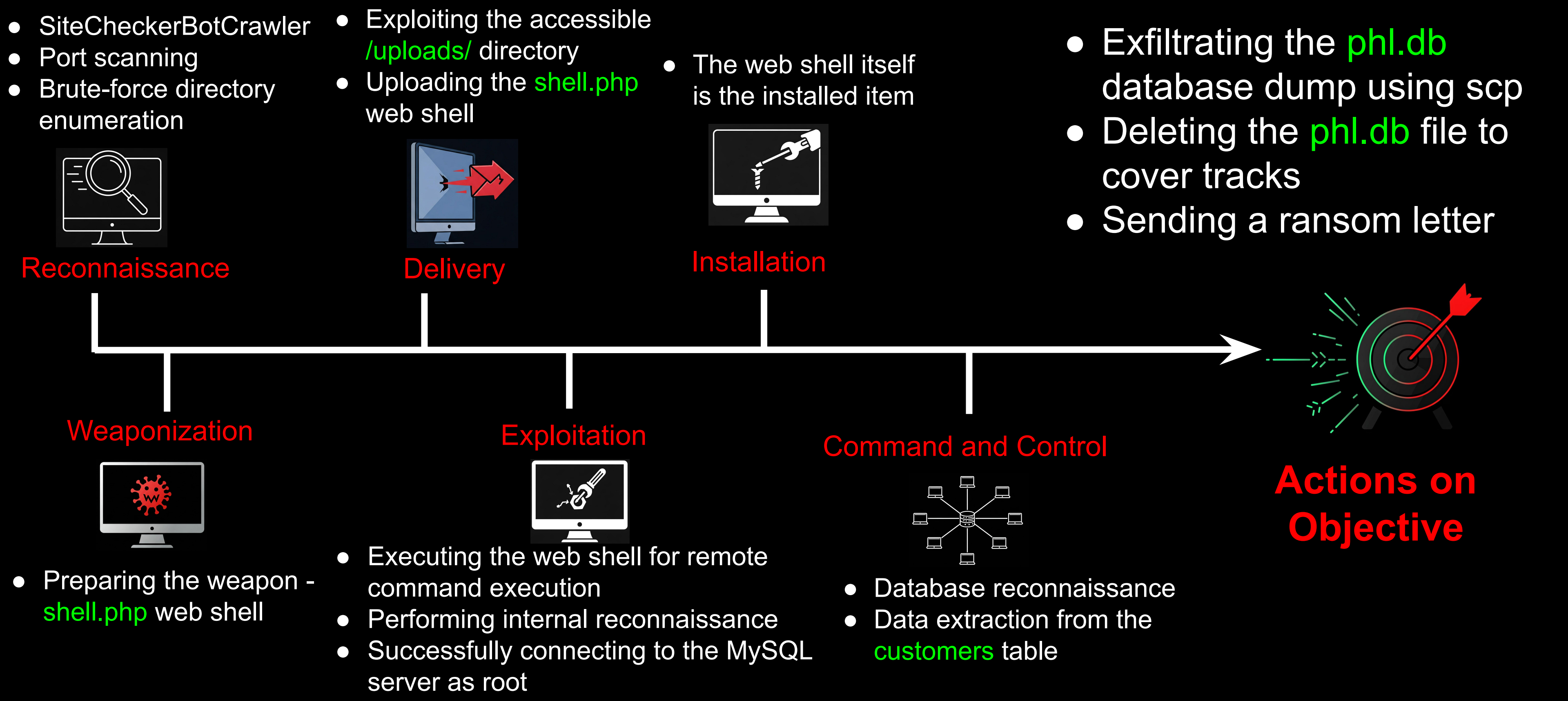
Actions on Objective. Data Exfiltration

Premium House Lights Data Breach

Prepared by Anastasiya Gruneva



Incident Breakdown



Reconnaissance

- SiteCheckerBotCrawler
- Port scanning
- Brute-force directory enumeration

Weaponization

- Preparing the weapon - shell.php web shell

Delivery

- Exploiting the accessible /uploads/ directory
- Uploading the shell.php web shell

Exploitation

- Executing the web shell for remote command execution
- Performing internal reconnaissance
- Successfully connecting to the MySQL server as root

Installation

- The web shell itself is the installed item

Command and Control

- Database reconnaissance
- Data extraction from the customers table

Actions on Objective

- Exfiltrating the phl.db database dump using scp
- Deleting the phl.db file to cover tracks
- Sending a ransom letter

Actions on Objective & Data Exfiltration

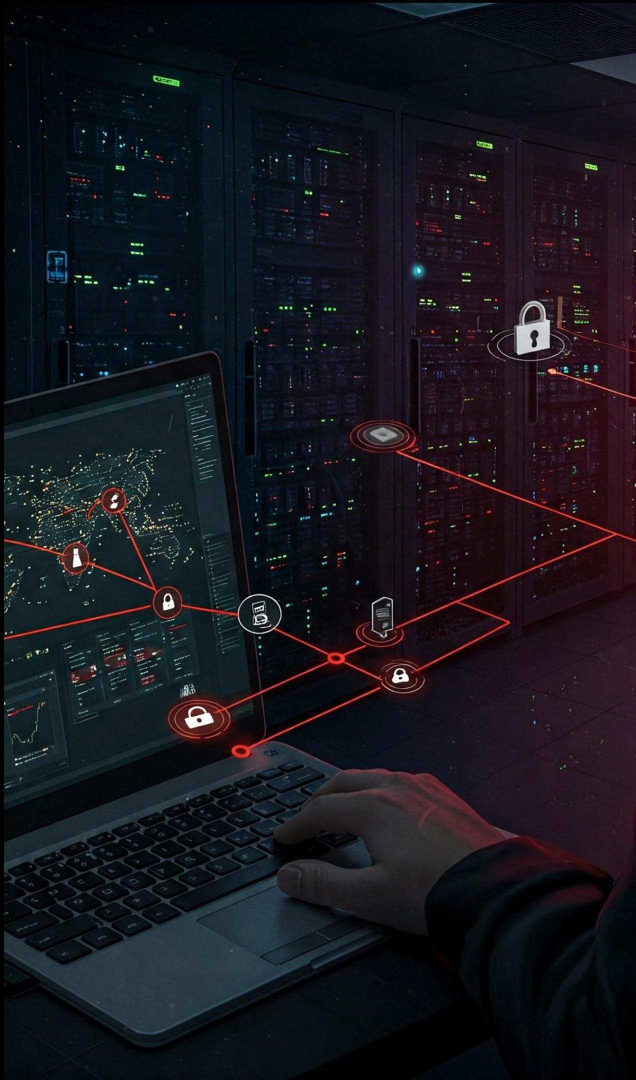
Actions on Objective - the final stage of the Cyber Kill Chain, where attackers achieve their goals (data theft, ransomware, etc.).

MITRE ATT&CK: TA0010 - Exfiltration

- The adversary attempts to steal data and move it outside the network.

Exfiltration Methods:

- **Command & Control (C2) Channels** – Hidden communication with attacker servers
- **Alternative Protocols (DNS Tunneling, HTTP, HTTPS)** – Masking data transfers
- **Cloud Services (Google Drive, Dropbox, OneDrive)** – Uploading stolen files
- **Physical Media (USB Drives, External Hard Drives)** – Removing data manually
- … and more techniques used by attackers



How Data Exfiltration Happened in This Attack?

Database Extraction

🕒 10:01:21 - 10:01:45 PM: Attacker used mysqldump to steal customer data.

🕒 10:01:46 PM: Attacker locked the customer table and ran SQL queries to avoid detection.

Data Transfer

🕒 10:02:26 PM: Attacker used scp to send stolen data to external server (178.62.228.28)

- 🔹 MITRE ATT&CK Reference: T1041 - Exfiltration Over C2 Channel

Covering Tracks

🕒 10:02:36 PM: Attacker deleted the stolen database file.

Ransom

💰 Ransom note sent demanding payment for the stolen data.

Key Recommendations

🛡️ **Data Loss Prevention (DLP):**

Deploy DLP solutions to monitor and block unauthorized data transfers, especially those involving sensitive information like customer data.

🚨 **Network Intrusion Detection/Prevention Systems (IDS/IPS):**

Configure IDS/IPS to detect and block suspicious network traffic, including large data transfers to unknown IP addresses.

📡 **Monitoring Outbound Traffic:**

Monitor outbound network traffic for unusual spikes in data transfer, especially to external servers.

🔧 **Disable Unnecessary Protocols:**

If SCP is not needed, disable it. If it is needed, restrict it to only needed IP addresses.

Thank you!