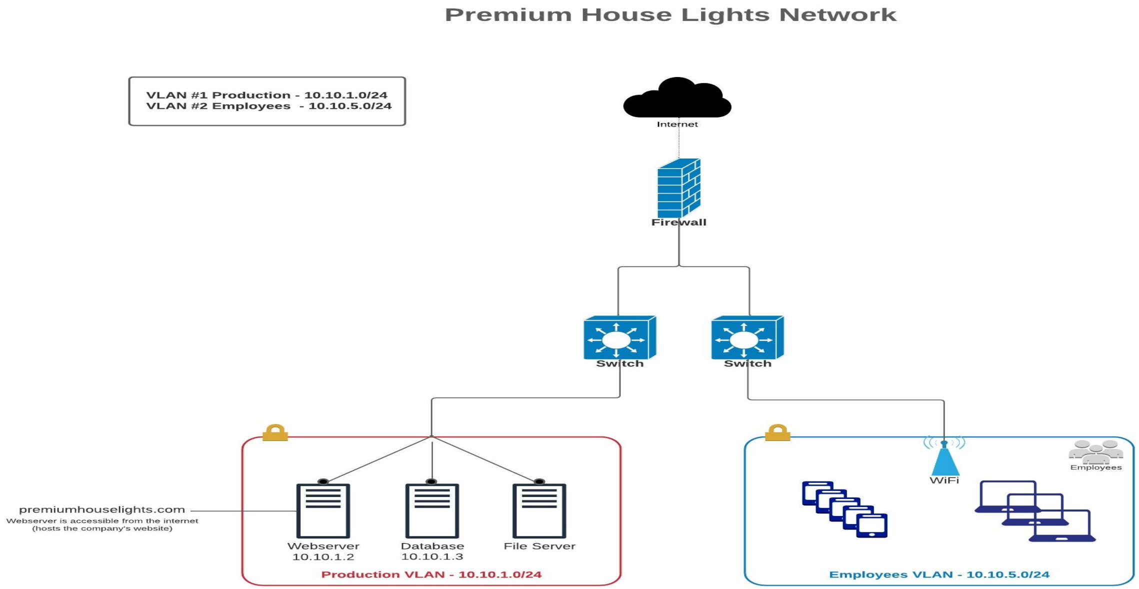
Premium House Lights Inc. Data Breach - Feb 19, 2022

Analysis Presented by: Victor Onukwu
Date: December 05, 2023

Scope of Attack Analysis

- Company Network Topology
- Incident Analysis
- Key Vulnerability Analysis
- Post-Incident Analysis
- Conclusion
- References

Company Network Topology


Premium House Lights Network
VLAN #1 Production - 10.10.1.0/24
VLAN #2 Employees - 10.10.5.0/24
Internet
Firewall
Switch
Switch
premiumhouselights.com
Webserver is accessible from the internet
(hosts the company's website)
Webserver
10.10.1.2
Database
10.10.1.3
File Server
Production VLAN - 10.10.1.0/24
WiFi
Employees
Employees VLAN - 10.10.5.0/24

Incident Analysis

A look at the incident analysis using the following frameworks:

- ➢ Timeline Analysis - Lockheed Martin Kill Cyber Kill Chain

- ➢ Technical Analysis - MITRE ATT&CK Framework.

Timeline Analysis

- **Reconnaissance(Web Server)**
  19/Feb/2022:21:56:13 -0500
  The attacker uses SiteCheckerBotCrawler.

- **Exploitation(Web Server)**
  19/Feb/2022:21:58:40 -0500
  Attacker performs an HTTP request smuggling.

- **Weaponization-Delivery-Exploitation-Installation**
  19/Feb/2022:21:59:04
  Attacker gains initial entry and delivered a malicious python reverse shell script injection.

- **Reconnaissance(Database)**
  19/Feb/2022:21:50 EST
  Attacker performs an NMAP scan.

- **Exploitation(Database)**
  19/Feb/2022:22:00:18 EST
  Attacker successfully gains access into Database(10.10.1.2) from Web server(10.10.1.3)

- **Command and Control**
  19/Feb/2022:00:27- 22:02:38
  Attacker gains administrative privilege and exfiltrates customer Personally Identifiable Information(PII).

- **Action and Objective**
  Attacker sends an extortion email from: 4C484C@qq.com to: support@premuimhouselights.com requesting for a ransom payment.

Technical Analysis

Using MITRE ATT&Ck Framework to analyze attacker tactics, techniques, and procedure:

- **Stage 1**-Reconnaissance-TA0043-T1595.002 - Active Scanning: Vulnerability Scanning(MITRE, 2020)|T1590.004 - Gather Victim Network Information: Network Topology(MITRE, 2020)

- **Stage 2**-Initial Access-TA0001-T1190 - Exploit Public-Facing Application(MITRE, 2018)|T1659 - Content Injection(MITRE, 2023)

- **Stage3**-Execution-TA0002-T1059.006- Command and Scripting Interpreter: Python(MITRE, 2020)

- **Stage 4**-Lateral Movement-TA0008-T1021.004 - Remote Services: SSH(MITRE,2020)

- **Stage 5**-Persistence-TA0003-T1133 - External Remote Services(MITRE,2017)

- **Stage 6**-Credential Access-TA0006-T1110.001 - Brute Force-Password Guessing(MITRE,2017)

Technical Analysis

- **Stage 7**- Defense Evasion-TA0005-T1078.002 - Valid Accounts: Domain Accounts(MITRE, 2020)

- **Stage 8**- Discovery-TA0007-T1007 - System Service Discovery(MITRE,2017)

- **Stage 9**- Collection-TA0009-T1005 - Data from Local System(MITRE,2017)

- **Stage 10-** Command and Control-TA0011-T1572 - Protocol Tunneling(MITRE,2020)

- **Stage 11**-Exfiltration-TA0011 T1048.003 - Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol.(MITRE,2020)

- **Stage 12 Impact**-TA0040- T1657 - Financial Theft(MITRE,2023)

Key Vulnerabilities

- The web application exhibited HTTP/1.1 Request Smuggling vulnerability.
- Insufficient Input/output validation vulnerability in the web server.
- Lack of segmentation between the organization's critical assets.
- Unpatched software, weak password policy, and poor monitoring.
- Poor Identity and Access Management(IAM), unnecessary open ports and service.
- The absence of intrusion detection and prevent systems(IDPS).

Post-Incident Recommendation

Future similar Ransomware attacks can be mitigated by implementing the following controls based on MITRE ATT&CK Framework and NIST CSF(NIST SP 800-53 r5)

- M1016- Regularly scan externally facing systems for vulnerabilities.
- M1001-Establish procedures to rapidly patch systems when critical vulnerabilities are discovered
- M1030- Deny direct remote access to internal systems through the use of network proxies, gateways, and firewalls.
- M1042- Disable or block remotely available services that may be unnecessary.
- M1032- Use strong two-factor or multi-factor authentication.
- DS0015- Monitor authentication logs for system and application login failures of Valid Accounts by implementing SIEM and SOAR solution.

Post-Incident Recommendation

Future similar Ransomware attacks can be mitigated by implementing the following controls based on MITRE ATT&CK Framework and NIST CSF(NIST SP 800-53 r5)

- ❖ M1057- Data loss prevention(DLP) can restrict access to sensitive data and detect sensitive data that is unencrypted.
- ❖ M1037- Enforce proxies and use dedicated servers for services such as DNS.
- ❖ AT-2(4) - Literacy Training and Awareness | Suspicious Communication and Anomalous System Behavior.
- ❖ AC-3 - Access Enforcement.
- ❖ AU-1,2,3…16- Implement audit and accountability policies.

Conclusion

The successful ransomware attack on PHL Inc. points to the dynamic and evolving threat landscape of today, characterized by increasingly sophisticated cyber attacks. Adopting a well-established frameworks like MITRE ATT&CK and the NIST CSF is not merely advisable but essential for PHL Inc to protect their infrastructure, secure sensitive information, and build a resilient defense against a future ransomware cyber attack.

References

Joint Task Force. (2020). Security and Privacy Controls for Information Systems and Organizations. NIST Special Publication 800-53, Revision 5. National Institute of Standards and Technology. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf on November 27, 2023

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer security incident handling guide (NIST Special Publication 800-61 Revision 2). National Institute of Standards and Technology. https://csrc.nist.gov/pubs/sp/800/61/r2/final

MITRE. (2023). MITRE ATT&CK®. Retrieved from https://attack.mitre.org/

Lockheed Martin. (n.d.). Cyber Kill Chain®. Retrieved December 4, 2023, from [https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html]

Common Vulnerabilities and Exposures (CVE) - NVD. (2023). National Vulnerability Database. Retrieved December 4, 2023, from https://nvd.nist.gov/vuln