The Reverse Shell Upload

Ransomware Case at Premium House Lights Inc

—

By Sumit Giri
Cybersecurity Analyst
Premium House Lights Inc.

The Discovery Process

- **Introduction:** We'll explore how the reverse shell (shell.php) was uploaded by the attacker using the tactic 'TA0001', known as initial access (MITRE ATT&CK).

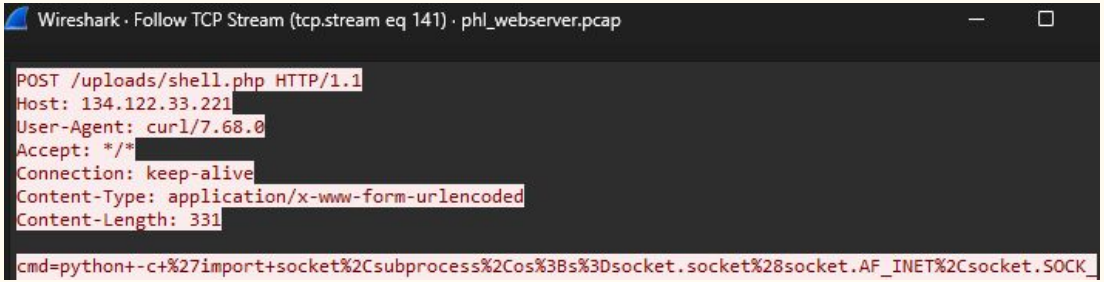
- **Focus:** Specifically, we'll delve into sub-technique 'T1105', which is called the ingress tool transfer.

- **Discovery:** We found the evidence of reverse shell upload through the HTTP POST request by analysing the web server access log.

```
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"
```

Understanding ‘TA0001’ : Initial Access

- **What is TA0001?** TA0001(Initial Access) involves adversaries using various entry vectors to gain their initial foothold within a network.
- **Our Case Study:** Analyzed Web server and packet capture (PCAP) files to uncover the attacker explored the file uploading facility on the server. Then the attacker uploaded a payload (shell.php) which initiated a reverse shell connection back to the attacker.
- **Key Takeaway:** understanding these tactics helps us identify and prevent such threats in the future.



Understanding ‘T1105’: Ingress Tool Transfer

- **What is Ingress Tool Transfer?** Ingress tool transfer helps Adversaries move tools/files into a compromised system to execute malicious activities. This includes:

    - ➢ Setting Up Backdoors: Adversaries transfer tools to compromised systems to maintain access.
    - ➢ Uploading Malicious Payloads: Utilities like curl, wget, and scp are used for stealthy uploads.
- **Our Case Study:** The attacker uploaded a malicious reverse shell script (shell.php) to the /uploads directory using curl and executed the script to establish persistent access to the server. It fits the criteria of T1105.

Vulnerabilities and Impact

Key Vulnerabilities:

- Lack of Input Validation
- Executable Permission
- Publicly Accessible Directory
- Lack of Monitoring

Impact:

- Backdoor Access
- Privilege escalation
- Lateral Movement
- Data Exfiltration

Conclusion and Next steps:

Summary:

- Analyzed adversarial tactics (TA0001) to gain insights into the cyber attack targeting Premium House Lights.
- Identified the attacker's method of delivering and executing a reverse shell (shell.php), establishing a backdoor for unauthorized access.

Next Steps:

- Analyze web server packet captures to uncover any additional malicious activities, including possible privilege escalation.
- Review database logs and shell activity for indications of lateral movement or privilege escalation efforts.

THANK YOU

I appreciate Your time and attention today.
Feel free to connect over LinkedIn

https://www.linkedin.com/in/sumit-giri-0111/