Example of a Incident Response Report of a infected system with reverse shell or command and control system. The compromised system became infected through a web server in the same network.

Example made by Fernando.

I. Incident Summary

Date: November 10th, 2020
Incident Type: Reverse Shell/Command and Control System Infection

II. Incident Details

Victim: My Website
Threat Actor: Unknown
Intrusion Kill Chain:

• Reconnaissance: Unknown
• Initial Access: Unknown
• Execution: Unknown
• Persistence: Unknown
• Command and Control: A reverse shell was identified
• Actions on Objectives: Unknown

III. Campaign Correlation

• Malicious activity was identified on the web server of My Website.
• The malicious activity appears to be a reverse shell or command and control system.
• This activity may be related to other malicious activity identified in the recent past.

IV. Courses of Action

• Isolate affected systems
• Identify and remove malicious files
• Restore systems from backups
• Monitor for suspicious activity
• Update security measures

V. Diamond Model

• Attacker: Unknown
• Capabilities: Unknown
• Infrastructure: Unknown
• Motivations: Unknown

VI. Timeline

• November 10th, 2020 – Malicious activity was identified on the web server of My Website.
• November 10th, 2020 – A reverse shell or command and control system was identified.

VII. Conclusion

It appears that My Website has been infected with a reverse shell or command and control system. The source of this infection is unknown, however, the infected system has been isolated and remediation steps are being taken to identify and remove the malicious files. Additionally, security measures have been updated to prevent