Subject: Workstation Win-USER01 (10.0.2.107) **Date**: February 28th, 2025
Tools Used: Wireshark [capture-win7.pcap] **Prepared By:** Jordan C. Lanning
Capture Date: January 4th, 2014

EXECUTIVE SUMMARY

On January 4th, our SOC Analyst received an alert on his SIEM dashboard. The alert indicated a botnet infection which was flagged and forwarded to the CIST within minutes of the alert. Win-USER01 (10.0.2.107) was affected on January 1st after visiting a spoofed CNN website. The user interacted with a website which was the likely trigger for the botnet persisted until January 4th. The organizational impact was HIGH.

KEY FINDINGS

1. Malicious CNAME Resolution
    a. DNS resolution of [www.edition.cnn.com] revealed a suspicious CNAME: cnnintl-56m.gslb.vgtf.net → 157.166.249.13
2. Suspicious HTTP Request Patterns
    a. Anomalous HTTP GET traffic followed the DNS request, including red flags such as:
        i. Suspicious Accept-Charset values
        ii. Faked User-Agent headers (impersonating Firefox on Windows NT)
3. High Volume of Unsuccessful TCP SYN Traffic
    a. Repeated outbound SYN packets from WIN-User01 with minimal or no SYN-ACK responses
    b. Observed Port Reuse and Packet Retransmission, consistent with denial of service symptoms or botnet beaconing.
4. Persistence of Botnet Activity
    a. The botnet was present on January 1st and continued beaconing until January 4th.
    b. C2 traffic continued at regular intervals until it was isolated.

ACTIONS PERFORMED

1. Isolated and scanned user, Win-USER01; system cleared of malicious processes and persistence mechanisms
2. Blocked outbound traffic to the Command and Control IP
3. Malicious IP address was reported to external intelligence feeds
4. Conducted targeted user awareness training to reinforce acceptable use policies (AUP)

IMPACT

- Risk Level: HIGH
- Operational Impact: Unknown at this time.
- Potential User Impact: Denial of Service was successful

CONCLUSION

The organization is currently investigating total financial impact of the DoS. Cyber insurance companies have been contacted.. While investigation efforts continue, the incident occurred due to improper use of company computers. Users should conduct AUP training on what sites they can and cannot use. We recommend whitelisting all unnecessary websites on company servers to avoid this issue. Additionally, architects should look to tune SIEMs to detect anomalous activities sooner than a few days to prevent damages.

There is **no on-going threat** to organizational systems at this time.

If there are any additional questions or concerns, please refer them Jordan C. Lanning, at 555-555-5555 or jordan.c.lanning@gmail.com. I will assist where I can.

Jordan C. Lanning, MPA, CySA+
Cybersecurity Analyst
555-555-5555