Lab 3 Report – Malware Case Study

Student Name: Amber Radune

Date: 2025-09-03

Course: CYBR-1100 Security Awareness

Week 3 Assignment

Malware Type

Response:

The malware in this case study is a **zero-day exploit**. Zero-day malware targets previously unknown vulnerabilities in software before developers have a chance to release a patch. Because the flaw is unknown, traditional antivirus and signature-based defenses often cannot detect or block it. Zero-day exploits are often delivered through phishing emails, malicious websites, or infected file downloads.

Infection Method & Symptoms

Response:

Zero-day malware typically spreads through socially engineered emails that trick users into clicking links or downloading attachments. Once the exploit is triggered, it executes malicious code to gain unauthorized access. Symptoms may include unusual system slowdowns, unexplained network traffic, disabled security tools, or files being encrypted in the case of

ransomware. The stealthy nature of zero-day attacks means symptoms are often subtle until major damage occurs.

Evidence

Response:

During the guided lab, I observed how the malware was able to bypass normal antivirus detection. The system logs showed suspicious activity linked to an unrecognized executable. Screenshots captured network traffic spiking after the file was executed, suggesting data exfiltration. (Insert your screenshots or notes here to show the specific activity from your lab environment.)

Defenses & Mitigations

Response:

1. **Patch Management:** Keep software and operating systems up to date to reduce exposure once a patch is available.

2. **Intrusion Detection/Prevention Systems (IDS/IPS):** These can spot unusual traffic patterns even if the malware signature is unknown.

3. **User Security Awareness Training:** Teach employees how to recognize phishing emails and avoid clicking suspicious links.

4. **Application Whitelisting:** Only allow approved applications to run, blocking unauthorized executables.

NetAcad Linkage

Response:

This case study connects directly to NetAcad Modules **2.1–2.2**. In Module 2.1 (*Analyzing a Cyber Attack*), we learn that attacks often begin with social engineering or malicious attachments, which is how zero-day malware is commonly delivered. Module 2.2 (*Methods of Infiltration*) explains the different ways attackers bypass defenses—such as exploiting unpatched vulnerabilities and leveraging phishing tactics. This directly aligns with the behavior of zero-day malware and reinforces the need for layered security and strong user awareness.

Works Cited

Ciampa, M. (2022). *Security Awareness: Applying Practical Security in Your World* (7th ed.). Cengage Learning.

Cisco Networking Academy. (n.d.). *Introduction to Cybersecurity*. Modules 2.1–2.2. Retrieved from https://www.netacad.com

Trend Micro. (2023, June 15). *What is a Zero-Day Vulnerability?* Retrieved from https://www.trendmicro.com/vinfo/us/security/definition/zero-day