Lewis Joseph Feik
Security Awarness
Week 3,LAB DAY 1

Lab 3 Report – Malware Case Analysis

Source: *Ciampa, Security Awareness, 6e, Chapter 3, Hands-On Project (File Infector Malware Simulation)*

Malware Type

The malware demonstrated in this lab was a ***file infector virus****. A file infector attaches malicious code to executable files (.exe or .com). When the infected program runs, the virus executes, spreading by corrupting additional files on the system. Unlike Trojans that rely on disguise or worms that self-replicate through networks, file infectors specifically target executable files, degrading system performance and damaging critical software.*

Infection Method & Symptoms

In the simulation, the file infector virus spread when a user opened an infected program downloaded from an untrusted source. Once executed, the malware inserted malicious code into multiple executable files across the system. Symptoms observed included:

- *Slower performance when opening applications.*
- *Corrupted or crashing programs that previously worked correctly.*
- *Unusual file size increases in executable files.*
- *Antivirus alerts indicating multiple file infections.*

This type of malware is particularly dangerous because it can render software unusable and cause widespread system instability.

Evidence Collected

During the guided lab, several artifacts were identified:

- ***Antivirus Logs:*** *Listed dozens of infected executables across the C:\Program Files directory.*
- ***File Properties:*** *Screenshots showed infected files had abnormal size increases compared to clean versions.*
- ***Event Viewer Logs:*** *Recorded repeated application faults tied to corrupted executables.*

Lewis Joseph Feik
Security Awarness
Week 3,LAB DAY 1

Defenses & Mitigations

To protect against file infector viruses, several defenses should be applied:

1. ***Antivirus and Endpoint Protection:*** *Ensure updated signature-based and behavior-based antivirus solutions are in place to detect and block file modifications.*

2. ***File Integrity Monitoring:*** *Use hashing and monitoring tools to detect unauthorized changes to critical system files.*

3. ***Least Privilege Controls:*** *Limit user permissions so that malware cannot easily write to system directories.*

4. ***Regular Backups:*** *Maintain secure, offline backups to restore clean copies of files in case widespread infection occurs.*

Connection to NetAcad Modules 2.1–2.2

This lab directly ties into ***NetAcad Modules 2.1 and 2.2****. Module 2.1 covers social engineering and risky user behavior, which were central to this infection since the user executed an untrusted file. Module 2.2 classifies malware and describes file infectors specifically, noting their ability to corrupt executables and propagate by embedding malicious code. Seeing this behavior in the lab reinforced how theory maps to practice, emphasizing the need for layered defenses and safe computing practices.*

Conclusion

The file infector virus simulation demonstrated how quickly and silently malware can compromise a system once an infected file is executed. Key evidence included corrupted files, antivirus alerts, and degraded system performance. This exercise underscored the importance of technical safeguards like antivirus and file integrity monitoring, combined with user awareness and strong security practices. With these defenses, organizations can minimize the risks posed by file infector malware.