CSC429: Computer Security
Homework 1

Group Member:

Abdulrahman Alateeq [redacted]

Mohammed Aljalajil [redacted]

Abdlrahman Almyman [redacted]

Question 1: Identifying Malware Type and Name Hash 1:

44d88612fea8a8f36de82e1278abb02f

- **Type: Virus, trajon**
- **Name:** EICAR Test File

Hash 2: 7e5e1f83718Ge5127aa86e0a834fe8f1e55c57c7

- **Type:** Trojan
- **Name:** Emotet

Hash 3: dccfb0G2faG7Gfb51c8c8ca64368a6f4334Ge41d

- **Type:** Worm, trojan, virus
- **Name:** LoveLetter

Question 2: Detailed Analysis for Each Malware Sample

Hash 1: EICAR Test File

- **Detection Ratio:** (65/69) Almost all antivirus programs detect this file. A high ratio shows this file is well-known and safe. It’s used to test antivirus programs. If your antivirus doesn’t catch it, something might be wrong with its setup.
- **Aliases:** EICAR_Test_File, Misc.Eicar-Test-File, EICAR-Test-Not-a-Virus.
- **Behavior:** It doesn’t do anything harmful. It’s just a harmless file for testing antivirus software.
- **Mitigation:** No action is needed since it’s safe.

Hash 2: Emotet

- **Detection Ratio:** (62/72) Many antivirus programs recognize it as malicious. This high detection ratio shows the threat is widely recognized as dangerous, confirming it’s a serious risk that requires immediate action to prevent harm.
- **Aliases:** Trojan/Win32.Agent.R220515, Trojan:Win/EmotetC.2F588DD7, Trojan/Win32.TSGeneric.

- **Behavior:**

  1. It can download harmful files onto the infected system.
  2. It may connect to unknown servers without permission.

- **Mitigation:**

  1. Keep antivirus software up-to-date.
  2. Avoid downloading files or software from suspicious or untrusted websites.

Hash 3: LoveLetter

- **Detection Ratio:** (49/62) Most antivirus programs identify this as a worm. This moderate detection ratio shows the worm is a known threat but may evade some antivirus programs, requiring strong protection.

- **Aliases:** Worm/Script.Agent.SC190953, Generic.ScriptWorm.6B95AC28

  , BV:LoveLetter-AN

- **Behavior:**

  1. It spreads through removable drives like USB sticks.
  2. It changes system settings to start running automatically.

- **Mitigation:**

  1. Turn off the AutoRun feature on your computer.
  2. Scan all external devices before using them.

Why do antivirus engines use multiple names for the same malware?

1. **Different Detection Mechanisms**: Each antivirus vendor uses its own detection methods, leading to unique naming conventions.
2. **Shared Behaviors**: Malware may share behaviors with other threats, so engines use generic names to classify them.
3. **Evolving Malware**: Variants of the same malware can appear, prompting engines to assign slightly modified names.

Question 3: Differences Between Malware Categories

1. **Virus:**
   - What It Does: A virus attaches itself to legitimate files and spreads when those files are used.
   - How to Protect: Keep antivirus programs updated and don’t open unknown files.

2. **Trojan:**
   - What It Does: A Trojan looks like a helpful program but does harmful things in the background.
   - How to Protect: Be cautious about downloading programs and only get software from trusted sources.

3. **Worm:**
   - What It Does: Worms spread by themselves across networks or devices, without needing a person to activate them.
   - How to Protect: Install system updates, watch for unusual network activity, and separate your network to prevent worms from spreading.