

Incident Analysis Report

1. Alarm Information

- **Alarm ID / Case No:** 009
- **Alarm Source:** SIEM / IDS
- **Alarm Description:** File Download Detected – Hash IOC:
44d88612fea8a8f36de82e1278abb02f
- **Timestamp:** [e.g., 2025-08-24 13:20 CET]

2. IOC Information

- **IOC Type:** 44d88612fea8a8f36de82e1278abb02f
- **IOC Value:** 44d88612fea8a8f36de82e1278abb02f
- **IOC Location:** [Unknown]

3. OSINT Investigation

VirusTotal

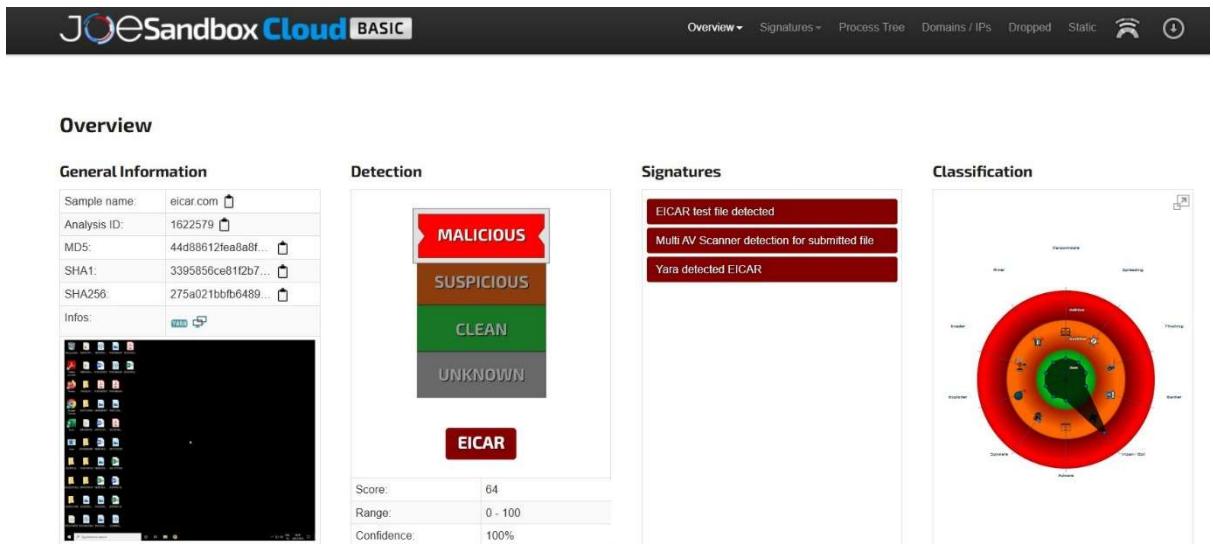
- Result: Detected by 1 AV engine (High confidence).
- <https://www.virustotal.com/gui/file/275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f/detection>

The screenshot shows the VirusTotal analysis interface for a file with MD5 hash 44d88612fea8a8f36de82e1278abb02f. The file was distributed by Offensive Security and has a community score of 65/69. It was analyzed 3684 times. The file size is 68 B and it was last analyzed 5 minutes ago. The file is identified as EICAR virus test files (100% match). The analysis details section shows the file type as Powershell and its source as EICAR virus test files. The file is also associated with PowerShell, ps, and ps1 file types. The file size is 68 B (68 bytes).

JasonSandBox

- Result: Malicious - Trojan

- <https://www.joesandbox.com/analysis/1622579/0/html>



4. Analysis & Assessment

- VirusTotal result High Risk evidence.
- JasonSandBox Malicious - Trojan

5. Conclusion / Decision

- **Decision:** True Positive
- **Category:** Trojan
- **Risk Level:** High (based on organization's classification)

6. Recommended Actions

1. Block the IP address on firewall / IPS.
2. Review SIEM logs for additional login attempts from the same source.
3. Correlate failed logins with user accounts for potential compromise attempts.
4. Consider implementing automated blocking rules for IPs with high abuse scores.