Incident Analysis Report

1. Alarm Information

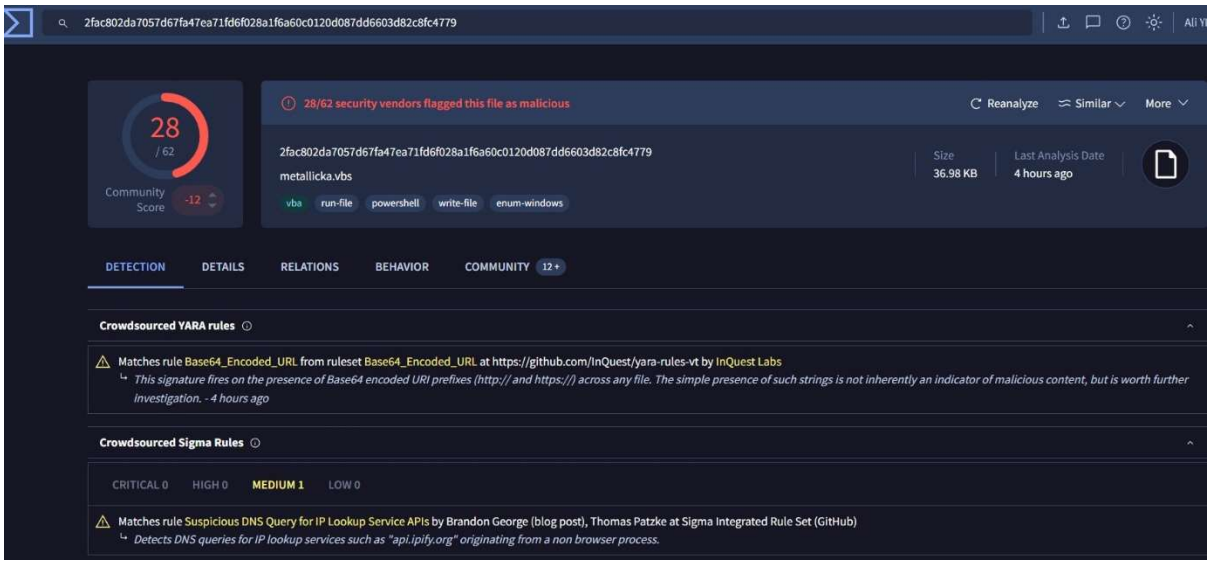
- **Alarm ID / Case No:** 010
- **Alarm Source:** SIEM / IDS
- **Alarm Description:** Download Detected – Hash IOC: e77d78fcb7e6b105d31a3b210ae39d63
- **Timestamp:** [e.g., 2025-08-24 13:20 CET]

2. IOC Information

- **IOC Type:** e77d78fcb7e6b105d31a3b210ae39d63
- **IOC Value:** e77d78fcb7e6b105d31a3b210ae39d63
- **IOC Location:** [Sweden]

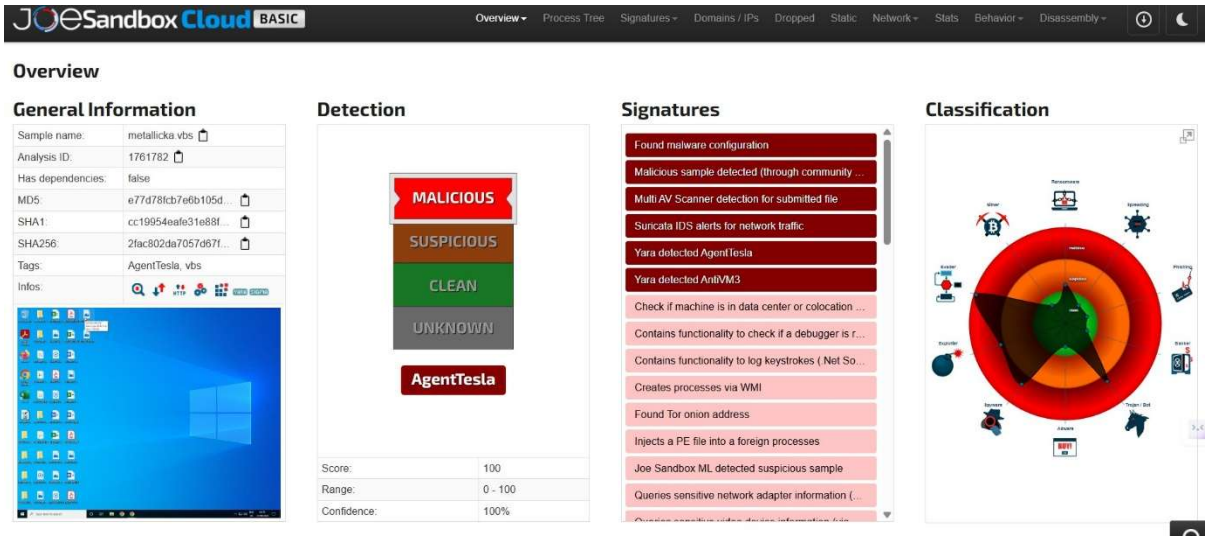
3. OSINT Investigation

VirusTotal

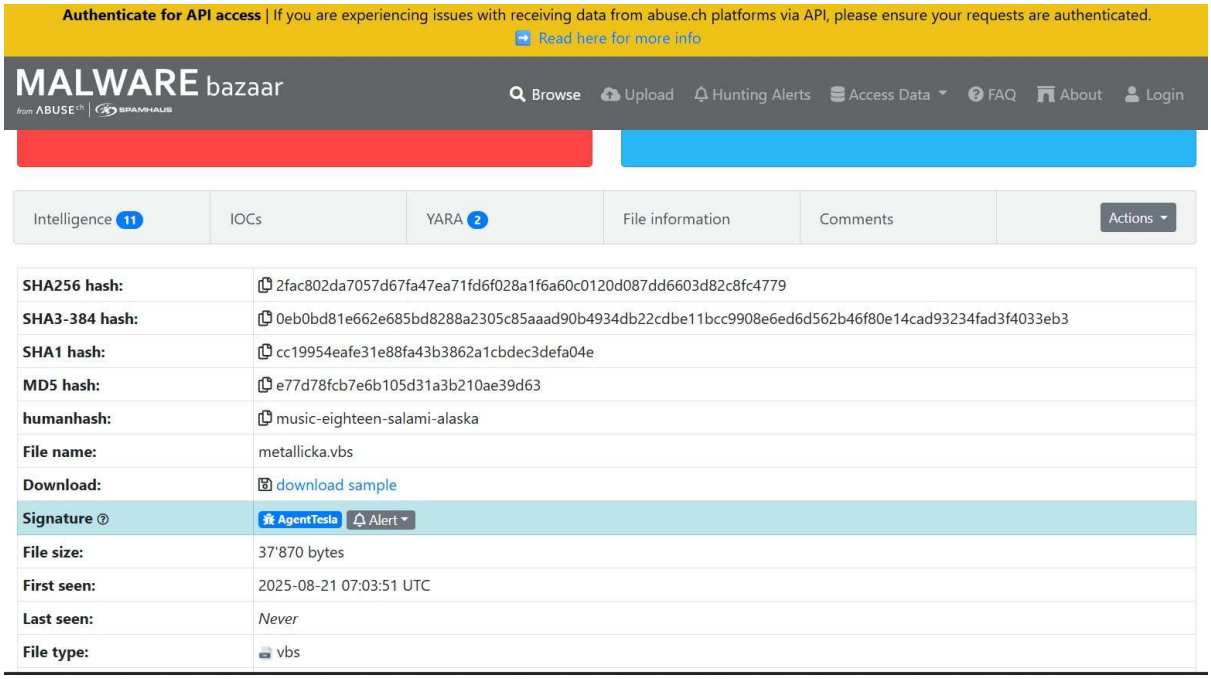
- Result: Detected by 1 AV engine (High confidence).
- https://www.virustotal.com/gui/file/2fac802da7057d67fa47ea71fd6f028a1f6a60c0120d087dd6603d82c8fc4779/detection
- 

JasonSandBox

- Result: Malicious – Exploiter

- https://www.joesandbox.com/analysis/1761782/0/html
- 

Malware Bazaar

- Result: Malicious – Exploiter
- https://bazaar.abuse.ch/sample/2fac802da7057d67fa47ea71fd6f028a1f6a60c0120d087dd6603d82c8fc4779/
- 

4. Analysis & Assessment

- VirusTotal result High Risk evidence.
- JasonSandBox Malicious – Exploiter

- Malware Bazaar Malicious – Exploiter

5. Conclusion / Decision

- **Decision:** ✅ **True Positive**
- **Category:** Exploiter Malware
- **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.