

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>

The screenshot shows the VirusTotal analysis interface for a file hash. The main summary indicates a 'Community Score' of 28/62, with a note that 28/62 security vendors flagged the file as malicious. The file name is 2fac802da7057d67fa47ea71fd6f028a1f6a60c0120d087dd6603d82c8fc4779, and it is a VBScript file named metallicka.vbs. The file size is 36.98 KB, and the last analysis date is 4 hours ago. Below the summary, there are tabs for DETECTION, DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY. Under the DETECTION tab, there are sections for 'Crowdsourced YARA rules' and 'Crowdsourced Sigma Rules'. Both sections show a single alert each, both of which are marked as low risk (MEDIUM 1). The first alert is for a Base64EncodedURL signature from InQuest Labs, and the second is for a Suspicious DNS Query from Sigma Integrated Rule Set.

JasonSandBox

- Result: Malicious – Exploiter

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

General Information

Sample name:	metalicka.vbs
Analysis ID:	1761782
Has dependencies:	false
MD5:	e77d78fc7e6b105d...
SHA1:	cc19954eafe31e88f...
SHA256:	2fac802da7057d67fa...
Tags:	AgentTesla, vbs
Infos:	

Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

Signatures

- Found malware configuration
- Malicious sample detected (through community ...)
- Multi-AV Scanner detection for submitted file
- Sonicata IDS alerts for network traffic
- Yara detected AgentTesla
- Yara detected AntiVM3
- Check if machine is in data center or colocation ...
- Contains functionality to check if a debugger is r...
- Contains functionality to log keystrokes (Net So...
- Creates processes via WMI
- Found Tor onion address
- Injects a PE file into a foreign processes
- Joe Sandbox ML detected suspicious sample
- Queries sensitive network adapter information (...)

Classification

Malware Bazaar

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

MALWARE bazaar
from ABUSE.ch | SPAMHAUS

Intelligence 11 **IOCs** **YARA** 2 **File information** **Comments** **Actions** ▾

SHA256 hash:	2fac802da7057d67fa47ea71fd6f028a1f6a60c0120d087dd6603d82c8fc4779
SHA3-384 hash:	0eb0bd81e662e685bd8288a2305c85aaad90b4934db22cdbe11bcc9908e6ed6d562b46f80e14cad93234fad3f4033eb3
SHA1 hash:	cc19954eafe31e88fa43b3862a1cbdec3defa04e
MD5 hash:	e77d78fc7e6b105d31a3b210ae39d63
humanhash:	music-eighteen-salami-alaska
File name:	metalicka.vbs
Download:	download sample
Signature ⓘ	Alert ▾
File size:	37'870 bytes
First seen:	2025-08-21 07:03:51 UTC
Last seen:	Never
File type:	vbs

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.