## Suricata Analysis with MITRE ATT&CK Mapping

FILE: eve-2025-11-02-2252.json

Event 1

- Classification: Suspicious outbound traffic (Potentially Bad Traffic)

- Severity: Medium

- Verdict: True Positive (low risk)

- What happened: Single outbound connection from an internal host to an external address flagged as suspicious HTTP traffic, with no follow-on exploit, payload, or C2 observed.

- MITRE Mapping: T1071.001 (Web Protocols - attempted), T1046 (Network Service Discovery - weak indicators)

- Remediation: Monitor this host for recurrence, enforce outbound web filtering, and retain NetFlow for short-term historical analysis.

FILE: eve-2025-11-03-0013.json

Event 1

- Classification: Protocol anomaly

- Severity: Medium

- Verdict: Likely Noise / True Negative

- What happened: One-off protocol anomaly with no accompanying malware, exploit, or repeated behavior from the same asset.

- MITRE Mapping: T1046 (Network Service Discovery - low confidence)

- Remediation: Tune the specific Suricata signature if it causes frequent noise, verify host posture, but no isolation is required at this time.

FILE: eve-2025-11-03-0022.json

Events: 3 (same host, same timeframe)

- Observed:

  - Suspicious User-Agent string

  - Hostile traffic pattern

  - Network Trojan classification (severity 1)

- Assessment: Severity High, Verdict True Positive

- What happened: The host first presents a suspicious User-Agent, then generates traffic classified as hostile, followed by a Trojan detection; this forms a clear escalation from anomaly to confirmed malware behavior.

- MITRE Mapping:

  - T1059 (Command and Scripting Interpreter - malware execution behavior)

  - T1105 (Ingress Tool Transfer - malicious payload download)

  - T1071.001 (Application Layer C2 over HTTP)

- Remediation: Isolate the host, acquire memory and disk images, block associated domains/IPs from this sequence, and search SIEM/EDR data for prior or subsequent activity using the same User-Agent or external IPs.

FILE: eve-2025-11-03-0044.json

Events: 2 (same flow)

- Assessment: Malware payload behavior followed by suspicious traffic.

- Severity: High

- Verdict: True Positive

- What happened: Initial packets match a known malware delivery/payload signature, followed closely by further suspicious HTTP traffic between the same internal host and external IP, indicating payload staging and early execution.

- MITRE Mapping:

  - T1105 (Ingress Tool Transfer - malicious binary or component delivery)

  - T1203 (Exploitation for Client Execution - exploit-initiated code execution on client)

  - T1059 (Command and Scripting Interpreter - malware execution)

- Remediation: Patch or update the client application that was exploited, terminate malicious processes associated with the connection, quarantine or delete downloaded binaries, and review browser/plugin configurations on the affected host.

FILE: eve-2025-11-03-0052.json

Events: 3

- Assessment: Trojan behavior, memory-based execution, and malformed HTTP patterns are present.

- Severity: Critical

- Verdict: True Positive

- What happened: A sequence of alerts indicates a network Trojan, abnormal HTTP structures, and follow-on activity suggestive of in-memory execution and possible process injection.

- MITRE Mapping:

  - T1106 (Native API - direct use of OS APIs by malware)

  - T1055 (Process Injection - code execution inside other processes)

  - T1622 (Debugger/Evasion - anti-analysis behavior)

  - T1059 (Execution via interpreter or shell)

- Remediation: Immediately isolate the host, perform memory forensics and EDR deep-dive, plan for full OS rebuild, and reset credentials used on the machine, especially privileged or domain accounts.

FILE: eve-2025-11-03-0112.json

Event: 1

- Assessment: Low-signal anomaly with no supporting malicious activity.

- Severity: Low

- Verdict: Informational / Monitor

- What happened: Single alert that does not escalate into malware, C2, or exploitation.

- MITRE Mapping:

  - T1595 (Active Scanning - low-confidence)

- Remediation: Monitor for recurrence or additional related alerts; no immediate containment needed unless more corroborating evidence appears.

FILE: eve-2025-11-03-0114.json

Events: 2

- Assessment: Recon or scanning behavior, plus a related anomaly.

- Severity: Medium

- Verdict: True Positive (Reconnaissance)

- What happened: Short-window correlated alerts from the same host indicating scanning or probing of services, but no confirmed exploitation in this file.

- MITRE Mapping:

  - T1595 (Active Scanning)

  - T1046 (Network Service Discovery)

- Remediation: Review firewall and internal access control logs to confirm scope of scanning, verify segmentation is effective, and monitor for transition from recon to exploitation.

PRIMARY FILE: eve.json (134 events – core of incident)

Host: 192.168.3.35

- Behavior: Tibs/Harnig downloader activity, malware-like User-Agent, invalid HTTP/MSIE headers.

- Severity: High / Critical

- Verdict: Confirmed Compromise (Downloader)

- What happened: This host is repeatedly detected performing downloader-style activity and using suspicious UA and malformed headers, characteristic of malware retrieving secondary payloads.

- MITRE Mapping:

  - T1105 (Ingress Tool Transfer)

  - T1071.001 (Web-based C2)

  - T1059 (Execution)

  - T1547 (Boot or Logon Autostart Execution – likely persistence vector)

- Remediation: Isolate the asset, collect memory and disk images, remove any malicious autoruns or services, and plan to rebuild or reimage the system. Search for similar traffic patterns enterprise-wide.

Host: 192.168.3.65

- Behavior: Confirmed C2 traffic to 188.72.243.72, EXE downloads, packed executable indicators, and likely in-memory execution.

- Severity: Critical

- Verdict: Confirmed Infection with Active C2

- What happened: Traffic clearly shows command-and-control sessions, executable payload delivery from 188.72.243.72, and behavior associated with packed binaries and runtime execution.

- MITRE Mapping:

  - T1071.001 (Web C2 over HTTP)

  - T1105 (Payload delivery)

  - T1055 (Process Injection)

  - T1027 (Obfuscated/Packed Executables)

  - T1497 (Virtualization/Sandbox Evasion – inferred from anti-VM-style patterns)

  - T1106 (Native API execution)

- Remediation: Immediately block communications with 188.72.243.72 and any related infrastructure, isolate and forensically image the machine, perform credential hygiene (password resets, especially for privileged users), and hunt for lateral movement originating from this host.

Hosts: 192.168.10.124–192.168.10.128

- Behavior: Repeated scanning behavior tied to CVE-2020-12695 and Unicode-based SMB share access attempts.

- Severity: High

- Verdict: True Positive (Recon and Lateral Movement)

- What happened: These hosts are involved in systematic scanning and SMB-based access attempts, consistent with internal discovery and lateral movement activity following initial compromise elsewhere.

- MITRE Mapping:

  - T1595 (Active Scanning)

  - T1021.002 (SMB/Windows Admin Shares for lateral movement)

  - T1087 (Account Discovery – inferred by SMB enumeration patterns)

- Remediation: Patch systems to address CVE-2020-12695, disable or constrain SMBv1 and legacy protocols, enforce least-privilege for lateral movement, and monitor for abnormal use of admin shares or brute-force/authentication anomalies.

Global Summary and MITRE-Aligned Incident View

- Overall Severity: Critical

- Overall Verdict: True Positive Incident

- Observed ATT&CK Stages:

  - Initial Access / Delivery: T1105, T1203

  - Execution: T1059, T1106

  - Persistence: T1547 (likely)

  - Discovery/Recon: T1595, T1046

  - Lateral Movement: T1021.002

  - Command & Control: T1071.001

  - Defense Evasion / Anti-Analysis: T1622, T1027, T1497

High-Level Remediation Plan (MITRE-Aligned)

- Immediate (Containment):

  - Isolate compromised hosts (192.168.3.35, 192.168.3.65, 192.168.10.124–128).

  - Block known malicious IPs (e.g., 188.72.243.72, 188.124.9.56, and related ranges such as 195.2.253.0/24).
  - Initiate memory and disk acquisition on key systems for full incident response.

- Short-Term (24–72 Hours):
  - Patch externally exploitable vulnerabilities such as CVE-2020-12695.
  - Enforce stricter egress filtering aligned to T1071.001 and T1105 controls.
  - Perform a hunt for the same malware families, User-Agents, and C2 endpoints across the environment.

- Medium-Term (Ongoing):
  - Implement MITRE ATT&CK–aligned detection rules in SIEM/EDR for the observed techniques.
  - Tighten lateral movement defenses (credential hygiene, SMB hardening, segmentation).
  - Conduct a post-incident review, update playbooks for T1105, T1071.001, T1021.002, and T1595.