Cybersecurity Threat Analysis

1. HIGHEST THREAT LEVEL REACHED

HIGH

2. ASSESSMENT

Critical threats detected include blacklisted flows, suspicious TLS activities, and DNS anomalies. Immediate containment and investigation are required to prevent further compromise, including data exfiltration and network infiltration.

3. THREATS

Threat Level	Threat Description	Involved IPs
High	Blacklisted Flows	[redacted]
High	TLS Suspicious Extensions	[redacted]
High	Suspicious DGA Domains	[redacted]
Medium	Invalid Client HELLO After Server HELLO	[redacted]
Medium	DNS Large Packets	[redacted]
Medium	Applications on Non-Standard Ports	[redacted]
Low	HTTP Anomalies (Suspicious User-Agent)	[redacted]

4. TIMELINE

- **May 17, 21:46 - 23:38:** SSL/TLS handshake anomalies detected.
- **May 18, 00:37 - 02:30:** HTTP anomalies and blacklisted flows intensify.
- **May 18, 04:52 - 05:54:** Critical blacklisted flows and suspicious TLS extensions detected with DNS anomalies.

5. NEXT STEPS

- **Immediate:** Block all blacklisted IPs (e.g., [redacted]) to prevent malicious communications.
- **Immediate:** Isolate impacted devices (e.g., [redacted]) to limit the spread of possible malware and perform forensic analysis.
- **High Priority:** Investigate suspicious TLS extension activities for potential encryption bypass or advanced persistent threats.
- **High Priority:** Analyze DNS anomalies for potential tunneling or covert communications.
- **Medium Priority:** Audit applications running on non-standard ports to identify unauthorized services or misconfigurations.
- **Medium Priority:** Investigate invalid SSL/TLS handshakes to determine if downgrade or man-in-the-middle attacks are occurring.
- **Low Priority:** Review HTTP anomalies (e.g., suspicious user-agents) for potential misuse or exfiltration attempts.

6. TECHNICAL DISCUSSION

The logs exhibit a combination of high-priority and medium-priority threats, which require immediate attention:

- **Blacklisted Flows:** These indicate communication with known malicious entities, commonly associated with botnets, command-and-control servers, or data exfiltration. Blocking these flows is crucial to prevent further compromise.
- **TLS Suspicious Extensions:** Irregularities in TLS handshakes, such as suspicious extensions, might signify attempts to exploit cryptographic vulnerabilities or evade detection mechanisms. This can be indicative of advanced threats.
- **Suspicious DGA Domains:** The detection of potentially algorithmically generated domains (e.g., webservices.mozgcp.net) suggests malware communication or command-and-control activity.
- **DNS Large Packets:** Oversized DNS packets may indicate DNS tunneling, which is often used for covert data exfiltration or command-and-control communication.

- **Invalid Client HELLO Messages:** These anomalies in SSL/TLS handshakes could result from misconfigured clients, downgrade attacks, or malicious interception attempts.
- **Applications on Non-Standard Ports:** Communication over unexpected ports may indicate unauthorized or misconfigured services, potentially bypassing firewall rules.
- **HTTP Anomalies:** Issues such as suspicious user-agents might indicate malware attempting to disguise its activity as legitimate traffic.

The high-priority threats, including blacklisted flows, TLS anomalies, and suspicious domains, require immediate action to mitigate the risk of data breaches or malware propagation. Medium-priority issues like DNS anomalies and non-standard port usage should be investigated promptly to uncover hidden threats. Low-priority anomalies should be addressed as part of the ongoing security posture improvement efforts.