SOC Investigation #4 — Brute Force & Malicious Domain Correlation

Executive Summary

This report analyzes authentication failures and outbound network activity found in log file 'big.log'. Multiple indicators reveal a coordinated brute-force attack accompanied by communication with a malicious external domain. The primary threat actor demonstrates persistence across prior SOC investigations. **Findings**

- 190 total authentication errors detected.
- IP **203.0.113.10** generated 100 consecutive failed login attempts (brute-force attack).
- Same IP appeared in SOC Investigations #1, #2, and #3, indicating persistent malicious activity.
- 30 outbound connections to **malware-check.evil-domain.com**, a confirmed malicious domain.
- IP 198.51.100.50 generated 50 failed attempts — suspicious but not correlated with malware.
- IP 192.168.1.5 generated 40 failed attempts — internal traffic, low severity.

Correlation Analysis

The combination of high-volume brute-force activity, repeated appearance in earlier investigations, and outbound communication to a malicious domain indicates an active and coordinated attack attempt. This behavior aligns with known malware patterns involving credential attacks followed by Command & Control (C2) communication. **Threat Severity**

- **High Severity:** 203.0.113.10 + malicious domain
- **Medium Severity:** 198.51.100.50
- **Low Severity:** 192.168.1.5 (internal)

Conclusion

The evidence strongly supports that 203.0.113.10 is the primary attacker, engaging in both brute-force authentication attempts and malicious outbound communication. This represents a multi-stage attack requiring immediate attention, blocking, and further investigation.