ESL Pro Security Report

Generated on: 2025-09-13 23:49:36 ADT

Executive Summary

This security analysis reveals a HIGH risk level due to multiple instances of processes exhibiting high network activity, particularly `svchost.exe` and `firefox.exe`. The presence of suspicious network behavior coupled with high resource usage warrants immediate investigation. Proactive monitoring and security measures are crucial to mitigate potential threats.

Antivirus Status

{'C:\\Windows\\Temp': '', 'C:\\Users\\leaw0\\Downloads': ''}

Firewall Status

Domain Profile Settings: ---------- State ON Firewall Policy BlockInbound,AllowOutbound LocalFirewallRules N/A (GPO-store only) LocalConSecRules N/A (GPO-store only) InboundUserNotification Enable RemoteManagement Disable UnicastResponseToMulticast Enable Logging: LogAllowedConnections Disable LogDroppedConnections Disable FileName %systemroot%\system32\LogFiles\Firewall\pfirewall.log MaxFileSize 4096 Private Profile Settings: ---------- State ON Firewall Policy BlockInbound,AllowOutbound LocalFirewallRules N/A (GPO-store only) LocalConSecRules N/... [truncated]

Network Status

{'nmap': {'command_line': 'nmap -oX - -sV 127.0.0.1', 'scaninfo': {'tcp': {'method': 'syn', 'services': '1,3-4,6-7,9,13,17,19-26,30,32-33,37,42-43,49,53,70,79-85,88-90,99-100,106,109-1

11,113,119,125,135,139,143-144,146,161,163,179,199,211-212,222,254-256,259,264,2

80,301,306,311,340,366,389,406-407,416-417,425,427,443-445,458,464-465,481,497,5

00,512-515,524,541,543-545,548,554-555,563,587,593,616-617,625,631,636,646,648,6
66-668,683,687,691,700,705,711,714,720,722,726,749,765,777,783,787,800-801,808,8
43,873,880,888,898,900-903,911-912,981,987,990,992-993,995,999-1002,1007,1009-10
11,1021-1100,1102,1104-1108,1110-1114,1117,1119,1121-1124,1126,1130-1132,1137-11
38,1141,1145,1147-1149,1151-1152,1154,1163-1166,1169,1174-1175,1183,1185-1187,11
92,1198-1199,1201,1213,1216-1218,1233-1234,1236,1244,1247-1248,1259,1271-1272,12
77,1287,1296,1300-1301,1309-1311,1322,1328,1334,1352,1417,1433-1434,1443,1455,14
61,1494,1500-1501,1503,1521,1524,1533,1556,1580,1583,1594,1600,1641,1658,1666,16
87-1688,1700,171... [truncated]

Process Security

{'scan_time': '2025-09-13T23:49:35.950331', 'total_processes': 282, 'suspicious_processes': 8, 'high_resource_processes': 0, 'network_processes': 43, 'processes': [{'pid': 272, 'name': 'Registry', 'exe_path': 'Registry', 'cmdline': '', 'cpu_percent': 0.0, 'memory_percent': 0.08969771264868485, 'create_time': '2025-09-13T22:22:19.566424', 'username': None, 'status': 'running', 'num_threads': 4, 'network_connections': 0, 'listening_ports': []}, {'pid': 760, 'name': 'steamwebhelper.exe', 'exe_path': 'C:\\Program Files (x86)\\Steam\\bin\\cef\\cef.win7x64\\steamwebhelper.exe', 'cmdline': 'C:\\Program Files (x86)\\Steam\\bin\\cef\\cef.win7x64\\steamwebhelper.exe --type=renderer --user-agent-product=Valve Steam Client --user-data-dir=C:\\Users\\leaw0\\AppData\\Local\\Steam\\htmlcache --buildid=1757452101 --steamid=0 --valve-initial-threadpool-size=4 --lang=en-GB --device-scale-factor=1 --num-raster-threads=4 --enable-main-frame-before-activation --renderer-client-id=5 --time-ticks-at-unix-epo... [truncated]

Vulnerability Scan Results

[OK] No vulnerabilities detected in the scanned directories.

OSV Scanner Details

OSV Results: No output from scanner

Network Traffic Analysis

Analyzed 30 network connections

Process Security Analysis

Scanned 282 processes, found 8 suspicious processes. Process security risk level: HIGH

Key Process Findings:

Found 8 potentially suspicious processes

Susp

AI Security Recommendations

Detailed Analysis & Recommendations

1. **Investigate `svchost.exe` (PID: 2900) and `firefox.exe` (PID: 3780) Immediately:** Use process monitoring tools to further investigate the network connections originating from these processes. Determine the legitimate purpose of these connections and verify they are not involved in malicious activity. Examine the processes' code and network traffic for suspicious patterns. 2. **Run Full Antivirus Scan:** Initiate a full system scan using a reputable antivirus software. Specifically target the directories associated with the identified suspicious processes (e.g., `C:\\Users\\leaw0\\AppData\\Local\\Programs\\Microsoft VS Code\\Code.exe` and the firefox profile directory). 3. **Enhance Process Monitoring:** Implement more granular process monitoring, including real-time alerts for processes exceeding normal network activity thresholds. This will enable faster detection and response to anomalous behavior. 5. **Regular Security Audits & Process Reviews:** Schedule regular security audits and process reviews to identify and mitigate potential vulnerabilities and ensure that security policies are being effectively enforced. Focus on identifying and understanding anomalous process behavior.

Risk Assessment

Overall Risk Level: LOW - System appears secure