ESL Pro Security Report

Generated on: 2025-09-11 22:55:32 ADT

Executive Summary

The system exhibits a HIGH risk level due to the presence of multiple processes lacking digital signatures and significant network activity from processes like Chrome. The detection of suspicious activity within Chrome, combined with unsigned processes, represents a serious threat requiring immediate investigation and remediation. Further, the overall number of processes running poses a heightened risk of exploitation.

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': '2025-09-11T22:55:32.948463', 'total_processes': 278, 'suspicious_processes': 13, 'high_resource_processes': 0, 'network_processes': 39, 'processes': [{'pid': 272, 'name': 'Registry', 'exe_path': 'Registry', 'cmdline': '', 'cpu_percent': 0.0, 'memory_percent': 0.0706741060562966, 'create_time': '2025-09-10T16:43:08.567507', 'username': None, 'status': 'running', 'num_threads': 4, 'network_connections': 0, 'listening_ports': []}, {'pid': 848, 'name': 'smss.exe', 'exe_path': 'C:\\Windows\\System32\\smss.exe', 'cmdline': '', 'cpu_percent': 0.0, 'memory_percent': 0.0020373915261975863, 'create_time': '2025-09-10T16:43:11.156373', 'username': None, 'status': 'running', 'num_threads': 2, 'network_connections': 0, 'listening_ports': [], 'file_size': 228768, 'file_modified': '2025-09-10T14:48:49.654519', 'file_created': '2025-09-10T14:48:49.633183', 'file_hash_partial': 'e63a0ddb7bd59f22fb5c2ad66e65d61b', 'digitally_signed': True}, {'pid': 936, 'name': 'svchost.exe', 'exe_path': ... [truncated]

Vulnerability Scan Results

[OK] No vulnerabilities detected in the scanned directories.

OSV Scanner Details

[DATA] Total 6 packages affected by 27 known vulnerabilities (2 Critical, 10 High, 11 Medium, 2 Low, 2 Unknown) from 1 ecosystem.

[SCA
Mediu

Network Traffic Analysis

Analyzed 27 network connections

Process Security Analysis

Scanned 278 processes, found 13 suspicious processes. Process security risk level: HIGH

Key Process Findings:

Found 13 potentially suspicious processes

Susp
from
music

AI Security Recommendations

Detailed Analysis & Recommendations

1. **Immediate Investigation of Suspicious Processes:** Prioritize investigating the processes identified as potentially suspicious, particularly YouTube Music.exe (PID: 3116), which is running from a temporary directory and lacks a digital signature. Use process monitoring tools to track network activity and system calls associated with these processes. 2. **Full Antivirus Scan & Malware Removal:** Perform a comprehensive full antivirus scan of the system, targeting areas where suspicious processes were detected. Utilize a reputable anti-malware scanner to remove any identified malware. 3. **Digital Signature Verification & Software Updates:** Verify the digital signatures of all executables on the system. Ensure that all software, including operating system, applications, and drivers, are running the latest versions to patch known vulnerabilities. 4. **Network Activity Monitoring & Firewall Rules:** Enhance network monitoring to closely observe all network connections. Implement or strengthen firewall rules to restrict outbound connections and block suspicious domains. Specifically, investigate Chrome's excessive network activity. 5. **Implement Process Monitoring & Alerting:** Deploy a robust process monitoring solution that provides real-time alerts for unexpected process behavior, high resource consumption, and connections to suspicious domains. This should be integrated with an alerting system to proactively detect and respond to potential threats.

Risk Assessment

Overall Risk Level: LOW - System appears secure