A-Ryan Security Report

Generated on: 2025-09-24 18:12:27 ADT

Executive Summary

The security scan revealed a high risk level due to the detection of several processes lacking digital signatures and an unusual location of `explorer.exe`. While no vulnerabilities were identified based on the scan data, the presence of unsigned processes and the atypical execution of a system process warrant immediate investigation. Further proactive monitoring and security hygiene practices are recommended.

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': '2025-09-24T18:12:27.009396', 'total_processes': 267, 'suspicious_processes': 6, 'high_resource_processes': 0, 'network_processes': 35, 'processes': [{'pid': 272, 'name': 'Registry', 'exe_path': 'Registry', 'cmdline': '', 'cpu_percent': 0.0, 'memory_percent': 0.06788283195131865, 'create_time': '2025-09-24T13:29:03.567301', 'username': None, 'status': 'running', 'num_threads': 4, 'network_connections': 0, 'listening_ports': []}, {'pid': 848, 'name': 'svchost.exe', 'exe_path': 'C:\\Windows\\System32\\svchost.exe', 'cmdline': '', 'cpu_percent': 0.0, 'memory_percent': 0.021056226709859367, 'create_time': '2025-09-24T13:29:12.324593', 'username': None, 'status': 'running', 'num_threads': 9, 'network_connections': 2, 'listening_ports': [49666, 49666], 'file_size': 88232, 'file_modified': '2025-09-10T14:48:48.612114', 'file_created': '2025-09-10T14:48:48.593875', 'file_hash_partial': '09d6bb18abb809eee33c5961a1c92b62', 'digitally_signed': True}, {'pid': 864, 'name': 'smss.exe',... [truncated]

Vulnerability Scan Results

[OK] No vulnerabilities detected in the scanned directories.

OSV Scanner Details

Network Traffic Analysis

Analyzed 13 network connections

Process Security Analysis

Scanned 267 processes, found 6 suspicious processes. Process security risk level: HIGH

Key Process Findings:

Found 6 potentially suspicious processes

Susp

AI Security Recommendations

Detailed Analysis & Recommendations

1. **Investigate Unsigned Processes Immediately:** Prioritize immediate investigation of all processes lacking digital signatures (notepad++.exe, LibreViewMASMonitor.exe). Analyze their activity, purpose, and source to determine if they are legitimate or malicious. 2. **Verify `explorer.exe` Location:** Confirm the legitimacy of `explorer.exe` running from c:\windows\explorer.exe. This is a critical system process, and any deviation from its standard location could indicate a compromise. Review the process's activity and resource usage closely. 3. **Run Full Antivirus Scan:** Execute a full, deep-scan antivirus scan across the entire system to identify and remove any malware or suspicious files associated with the detected processes. 4. **Implement Process Monitoring and Alerting:** Configure robust process monitoring tools to track all running processes in real-time. Set up alerts for any process exhibiting unusual behavior, such as unexpected network connections, high CPU usage, or access to sensitive files. 5. **Strengthen System Security Hygiene:** Ensure all software is up-to-date with the latest security patches. Implement and maintain a strong firewall to control network traffic and prevent unauthorized access. Consider using software restriction policies to limit the execution of unsigned or potentially harmful applications.

Risk Assessment

Overall Risk Level: LOW - System appears secure