DeepCytesiOS AntiSpyware Security Report

Generated: 2025-08-23 21:42:39

EXECUTIVE SUMMARY

Risk Assessment: CRITICAL RISK

Total Threats Detected: 8
Critical Severity Threats: 2
High Severity Threats: 1
AI-Enhanced Analysis: 0 findings
Files Affected: 4

DETAILED SECURITY FINDINGS

Finding #1: Lateral_Movement_Patterns

File: lateral.txt
Line: 1
Severity: High
Confidence: Medium
Evidence: ssh connection rapid multiple internal hosts
Context: 2025-08-12 09:21:03 Detected ssh connection rapid multiple internal hosts...

RECOMMENDED ACTION:

Isolate affected systems, audit network access, reset credentials, implement network segmentation

Finding #2: App_Masquerading

File: ps.txt
Line: 4
Severity: Unknown
Confidence: Medium
Evidence: Safari1.app
Context: /private/var/mobile/Containers/Bundle/Safari1.app.app...

RECOMMENDED ACTION:

Investigate app source, check app store legitimacy, verify developer signature

Finding #3: App_Masquerading

File: ps.txt
Line: 4
Severity: Unknown
Confidence: Medium
Evidence: Safari1.app.app

Context: /private/var/mobile/Containers/Bundle/Safari1.app.app...

RECOMMENDED ACTION:

Investigate app source, check app store legitimacy, verify developer signature

Finding #4: App_Masquerading

File: ps.txt
Line: 5
Severity: Unknown
Confidence: Medium
Evidence: Photos.app.app
Context: /Applications/Photos.app.app...

RECOMMENDED ACTION:

Investigate app source, check app store legitimacy, verify developer signature

Finding #5: Zero_Click_Exploit_Detection

File: malicious.txt
Line: 1
Severity: Critical
Confidence: Medium
Evidence: CoreGraphics crash
Context: 2025-08-16 12:34:01 CoreGraphics crash detected - stack trace follows...

RECOMMENDED ACTION:

Review and investigate finding

Finding #6: Zero_Click_Exploit_Detection

File: malicious.txt
Line: 2
Severity: Critical
Confidence: Medium
Evidence: iMessage exploit
Context: 2025-08-16 12:35:01 iMessage exploit CVE-2024-0001 detected...

RECOMMENDED ACTION:

Review and investigate finding

Finding #7: App_Masquerading

File: ps.txt
Line: None

Severity: Medium
Confidence: Medium
Evidence: /private/var/mobile/Containers/Bundle/Safari1.app.app
Context: /private/var/mobile/Containers/Bundle/Safari1.app.app...

RECOMMENDED ACTION:

Investigate app legitimacy, check app store source, verify developer signature

Finding #8: App_Masquerading

File: ps.txt
Line: None
Severity: Medium
Confidence: Medium
Evidence: /Applications/Photos.app.app
Context: /Applications/Photos.app.app...

RECOMMENDED ACTION:

Investigate app legitimacy, check app store source, verify developer signature