Kairos A.I. — Incident Report

Generated: 2025-09-26 06:36:03

P2 INC-COMPOSITE-1758886525

Summary

15 recent suspicious file(s) in monitored paths

Artifacts

- file: C:\Users\jas06\Downloads\OculusSetup (1).exe (.exe, 4774136 bytes, sha256=f4d758549c5b5873c9e4ab8592c667e05fce0156aa64d8c6bbe28e6382873c2c)
- file: C:\Users\jas06\Downloads\OculusSetup (2).exe (.exe, 4774136 bytes, sha256=f4d758549c5b5873c9e4ab8592c667e05fce0156aa64d8c6bbe28e6382873c2c)
- file: C:\Users\jas06\Downloads\OculusSetup (3).exe (.exe, 4774136 bytes, sha256=f4d758549c5b5873c9e4ab8592c667e05fce0156aa64d8c6bbe28e6382873c2c)
- file: C:\Users\jas06\Downloads\OculusSetup.exe (.exe, 4774136 bytes, sha256=f4d758549c5b5873c9e4ab8592c667e05fce0156aa64d8c6bbe28e6382873c2c)
- file: C:\Users\jas06\Downloads\urgent_invoice.exe (.exe, 6 bytes, sha256=837ccb607e312b170fac7383d7ccfd61fa5072793f19a25e75fbacb56539b86b)
- file: C:\Users\jas06\Downloads\VirtualDesktop.Streamer.Setup.exe (.exe, 103585944 bytes, sha256=n/a)
- file: C:\Users\jas06\Downloads\XboxInstaller.exe (.exe, 14050752 bytes, sha256=n/a)
- file: C:\Users\jas06\Downloads\VRMark-v1-3-2020\vrmark-setup.exe (.exe, 14793800 bytes, sha256=n/a)
- file: C:\Users\jas06\Downloads\VRMark-v1-3-2020\redist\dotNetFx45_Full_x86_x64.exe (.exe, 50352408 bytes, sha256=n/a)
- file: C:\Users\jas06\AppData\Local\Temp\.tmpccclKV\applypatch.bat (.bat, 137 bytes, sha256=18a5048e30a52521b4f1e7b87ae341847fbd6a37998d46137b0e9a1862a9d260)
- file: C:\Users\jas06\AppData\Local\Temp\.tmpccclKV\apply_patch.bat (.bat, 137 bytes, sha256=18a5048e30a52521b4f1e7b87ae341847fbd6a37998d46137b0e9a1862a9d260)
- file: C:\Users\jas06\AppData\Local\Temp\.tmpHK2kDw\applypatch.bat (.bat, 137 bytes, sha256=18a5048e30a52521b4f1e7b87ae341847fbd6a37998d46137b0e9a1862a9d260)
- file: C:\Users\jas06\AppData\Local\Temp\.tmpHK2kDw\apply_patch.bat (.bat, 137 bytes, sha256=18a5048e30a52521b4f1e7b87ae341847fbd6a37998d46137b0e9a1862a9d260)
- file: C:\Users\jas06\AppData\Local\Temp\.tmpVBmQQ1\applypatch.bat (.bat, 137 bytes, sha256=18a5048e30a52521b4f1e7b87ae341847fbd6a37998d46137b0e9a1862a9d260)
- file: C:\Users\jas06\AppData\Local\Temp\.tmpVBmQQ1\apply_patch.bat (.bat, 137 bytes, sha256=18a5048e30a52521b4f1e7b87ae341847fbd6a37998d46137b0e9a1862a9d260)

Recommendations

- Validate legitimacy with user/context.
- If malicious: terminate processes and quarantine files.
- Block associated domains/IPs at egress and host firewall.
- Preserve evidence (hashes, paths, netconns, cmdlines) prior to remediation.