CYFLARE

Case Study: Fog Ransomware Contained Despite EDR Gaps

A missed endpoint agent gave attackers a foothold. But CyFlare's SOC coordinated a rapid response to stop the spread, confirm the presence of ransomware, and guide remediation efforts across affected systems.

In December 2024, CyFlare's SentinelOne-powered detection capabilities flagged lateral movement using privileged credentials. Due to gaps in EDR coverage, threat actors moved between unmanaged internal systems and initiated ransomware activity, which was ultimately confirmed to be Fog Ransomware.

CyFlare's SOC manually escalated alerts, coordinated with internal teams, and isolated infected machines. While full containment required client-side coordination with forensics and insurance, CyFlare's IOCs and response protocols helped prevent further spread.

INCIDENT HIGHLIGHTS

- Multiple lateral movement alerts over 7 days
- 900+ suspicious files and process events logged
- Ransomware behavior observed: .flocked extension applied
- Affected assets lacked EDR agent visibility
- Manual containment required via IR calls and SOC coordination

TIMELINE SNAPSHOT

DECEMBER 4 4:11 AM	First alert: admin lateral movement detected by SentinelOne
DECEMBER 4 5:03 AM	Manual escalation due to automation failure
DECEMBER 4 7:31 AM	Second alert; indicators of ransomware behavior (.flocked)
DECEMBER 4 9:03 AM	Endpoint isolation begins; client IR collaboration initiated
DECEMBER 4 1:17 PM	Client confirms FOG ransomware infection (.flocked extension found)
DECEMBER 6 3:04 PM	New alert—recurring lateral movement from same compromised account
DECEMBER 6 5:20 PM	Manual escalation again; client agrees to shut down impacted machine
DECEMBER 11 2:40 PM	Servers reinstalled, remediation complete, ticket officially closed

CYFLARE SOC SUMMARY AND RECOMMENDATIONS

The FOG ransomware attack unfolded over seven days, initially bypassing detection due to automation failures and unmanaged endpoint gaps. CyFlare's SOC team responded with hands-on escalation, isolating compromised assets and providing direct support to client-side IR and insurance teams. Even after initial containment, recurring activity required additional intervention, ultimately leading to full threat neutralization and environment recovery.

The incident underscored the need for 100% EDR agent coverage, backup validation, least-privilege access policies, and proactive monitoring for ransomware-like behavior.

Schedule a demo of Cyflare's Managed EDR Services

www.cyflare.com |sales@cyflare.com

REV02_0926