CYFLARE
The threat stops here.

Case Study: How CyFlare Stopped a Privilege Escalation Attack via SMBexec

A compromised endpoint allowed an attacker to escalate privileges using NTLM token abuse and deploy remote shell access. Thanks to CyFlare's 24/7 SOC and detection of SMBexec activity, the threat was quickly traced, contained, and investigated across multiple hosts, despite early telemetry gaps.

In September 2024, CyFlare's Stellar-powered EDR identified suspicious NTLM-based privilege escalation attempts tied to RottenPotato behavior. Within hours, Microsoft Defender had been disabled across multiple hosts, and Impacket's smbexec.py was used to install remote services via SMB.

Due to cold storage limitations and telemetry gaps, full log analysis required extended coordination. Still, CyFlare's SOC worked alongside the client and third-party IR teams to correlate activity, trace the attacker's movement, and contain the threat before deeper lateral compromise could occur. Ultimately, remote shell access was neutralized, password resets reviewed, and no critical systems were permanently impacted.

INCIDENT HIGHLIGHTS

- 183MB outbound data transfer to a known malicious IP
- SMBexec activity linked to Impacket tools
- Defender disabled on multiple endpoints
- Privilege escalation via RottenPotato-like NTLM abuse
- 90-day logs required cold storage extraction

TIMELINE SNAPSHOT

- **SEPTEMBER 3** 1:35 PM — Connection to malicious IP observed from MCNPS
- **SEPTEMBER 6** 11:01 PM — NTLM privilege escalation behavior flagged
- **SEPTEMBER 6** 11:23 PM - 11:43 PM — Microsoft Defender disabled on MCNPS and second host (VIEWPOINT2016)
- **SEPTEMBER 7** 2:12 AM - 2:26 AM — SMBexec service install alert triggered, Mass account password reset executed
- **SEPTEMBER 7** 5:00 PM — Client initiates SOC investigation
- **SEPTEMBER 7** 9:45 PM — Live Teams bridge opened with external IR partner
- **OCTOBER 11** 3:01 PM — Final logs retrieved; case closed

CYFLARE SOC SUMMARY AND RECOMMENDATIONS

CyFlare's SOC identified and contained a privilege escalation attack involving NTLM token abuse, Defender tampering, and remote service installation via SMBexec. Despite log delays and disabled endpoint protections, the coordinated response prevented broader lateral movement and exfiltration. To strengthen defenses, **enable Defender tamper protection, disable legacy NTLM protocols, monitor for Impacket and SMBexec activity, apply outbound IP filtering, and extend log retention with least privilege enforcement.**

Schedule a Demo of CyFlare's Managed EDR Services Today!

www.cyflare.com | sales@cyflare.com

REV01_0525