CYBER DEFENSE AGAINST CL0P RANSOMWARE GANG'S MOVEIT EXPLOIT

CL0P is a ransomware gang that emerged in 2019 and increased its profile with cyberattacks early in 2023. In June 2023, its attack through the MOVEit file-sharing software impacted many commercial organizations, federal agencies, and state and local government entities.

Celerium's Compromise Defender™ -- a cyber defense solution that detects and automatically blocks, contains, and disrupts cyber threats and compromise activity -- provided cyber defense against the MOVEit cyberattack.

Celerium quickly implemented IOCs from CISA for the defense of organizations against the MOVEit vulnerability and associated CL0P ransomware threat. Beyond the MOVEit threat, Celerium's Compromise Defender solution can be used against future attacks and threats from CL0P, malware campaigns, and phishing attacks – including those automatically generated by ChatGPT and other AI-enabled technologies and threat actors.

Solution implementation takes 30 minutes or less and draws upon several sources of threat intelligence, including the latest threat intelligence from CISA, to detect and automatically block IOCs and malicious IP addresses related to cyber threats like the MOVEit vulnerability.

COMPROMISE DEFENDER STANDARD EDITION

- Detects and disrupts network threats and compromise activity such as reconnaissance, C2 server activity, scanning, and more.
- Works with popular public-facing perimeter firewalls.
- Automated: No integration with SIEMs or other security tools is required.
- Autonomous: No day-to-day management is required.
- Real Time: Block lists are re-optimized every 15 minutes.
- Contains an integrated analysis platform and integrated reporting platform.
- Can be used by communities to provide dashboards of common operating pictures and situational awareness of community threats and trends.

IMPLEMENTATION:

- Non-intrusive implementation at the firewall -- no new hardware or black boxes to install and no software to download.
- Implementation takes 30 minutes or less.
- Utilizes a **Decision Engine** hosted on the secure AWS cloud.
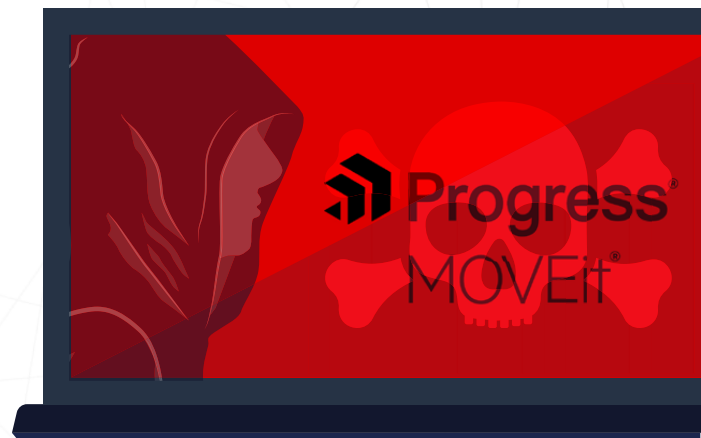
For pricing or inquiries, contact Celerium online at www.Celerium.com or via email at info@celerium.com