WARLOCK GROUP

[/ˈwɔːrlɒk gruːp/]

Warlock Group (GOLD SALEM / Storm-2603) is a ransomware operator active since March 2025, exploiting Microsoft SharePoint via the ToolShell vulnerability chain to deliver its custom payload across manufacturing, technology, and healthcare sectors globally. By mid-September 2025, approximately 60 victims had been listed on its Tor leak site. Microsoft assesses the cluster with moderate confidence as China-based.

IDENTITY

Attribution	: Identified by Secureworks CTU as GOLD SALEM, Microsoft as Storm-2603, and Unit 42 as cluster CL-CRI-1040. Microsoft assesses with moderate confidence that the group is China-based.
Active Since	: March 2025
Aliases	: Warlock Group, GOLD SALEM, Storm-2603, CL-CRI-1040
Motivation	: Primarily financially motivated through double-extortion ransomware operations, though some evidence suggests potential dual espionage/financial interests.

TTPs

Initial Access	: Exploitation of Microsoft SharePoint “ToolShell” vulnerabilities (CVE-2025-49704, CVE-2025-49706, CVE-2025-53770, CVE-2025-53771).
Persistence	: Deployment of ASPX web shells (e.g., spinstall0.aspx); use of AK47 custom C2 framework with DNS and HTTP variants; occasional abuse of VS Code tunnels and Velociraptor for persistence and remote access.
Tools & Malware	: Mimikatz for credential theft (LSASS dump), PsExec and Impacket for lateral movement, BYOVD techniques to disable EDR, Group Policy Objects (GPO) for mass ransomware deployment.
Techniques	: Double-extortion ransomware scheme involving encryption of systems combined with data exfiltration for public leaks; data exfiltration and publication via Tor-based leak site.

TARGET PROFILE

Target Sectors	: Manufacturing, technology, telecom, healthcare, construction, and select government entities.
Geographies Targeted	: Predominantly North America, Europe, and South America, with activity observed in APAC and Latin America.

THREAT ASSESSMENT

Risk Level	: High – the group demonstrates rapid growth and active exploitation of zero-day vulnerabilities.
Most Recent Activity	: As of September 2025, around 60 victims listed on Warlock’s leak site. Campaigns include exploitation of SharePoint vulnerabilities, widespread use of custom AK47 C2, and large-scale ransomware deployments.
Evolution	: Initially linked to LockBit 3.0 affiliate activity before transitioning into an independent ransomware operation with its own infrastructure and leak site. Increasing sophistication in operational security, tooling, and recruitment from underground forums.

NOTABLE OPERATIONS

- **March 2025:** First observed leveraging SharePoint ToolShell vulnerabilities for initial access.
- **April–May 2025:** Multiple intrusions against enterprises in North America and Europe; leak site launched.
- **August 2025:** Exploited new SharePoint zero-days to deploy Warlock ransomware in high-profile incidents.
- **September 2025:** Expanded victim list to ~60 organizations globally, spanning manufacturing, healthcare, and telecom sectors.