BLACKFOG®

Threat Intelligence Brief

FOCUS
Warlock Ransomware

CROSS-SECTOR
Government / Education / Technology

Confronting Warlock Ransomware:
BlackFog's Prevention First Strategy in Action

Who is Warlock?

Warlock is a financially motivated ransomware strain deployed by Storm-2603, a suspected China-based threat actor. Leveraging the high-impact "ToolShell" SharePoint exploit chain (CVE-2025-49706 and CVE-2025-49704, plus bypasses CVE-2025-53770/53771), Storm-2603 has deployed Warlock ransomware on compromised on-premises SharePoint servers beginning around July 18, 2025.

Microsoft attributes the activity to multiple Chinese-affiliated groups—including Linen Typhoon, Violet Typhoon, and Storm-2603, noting that Storm-2603 has previously deployed both Warlock and LockBit variants.

Sectors Under Fire

At least 400 SharePoint servers (across over 148 organizations) have been compromised globally, including U.S. federal agencies such as the National Nuclear Security Administration, Department of Education, and Department of Health and Human Services.

Evolving TTPs: The SharePoint Attack Chain

1. **Exploitation of SharePoint zero-days -** CVE-2025-49704 (RCE) and CVE-2025-49706 (spoofing), along with public bypasses CVE-2025-53770/53771.
2. **ToolShell web shell deployment -** attackers upload variants like spinstall0.aspx, spinstall1.aspx, using w3wp.exe process for code execution and stealing ASP.NET machine key material.
3. **Recon and privilege validation -** commands like whoami via w3wp.exe.
4. **Defender disablement -** services.exe used to change registry and disable Microsoft Defender protections.
5. **Persistence -** scheduled tasks and modification of IIS configuration to launch disguised .NET assemblies.
6. **Credential theft and lateral movement -** Mimikatz, LSASS scraping, PsExec, Impacket toolkit, WMI.
7. **Mass ransomware deployment -** modifying GPOs to deploy Warlock across infected networks via storm-2603.

© 2025 BlackFog, Inc.

How BlackFog Stops Warlock

Real-time protection for stealthy, cloud-based threats

Blocks Ransomware via SharePoint Attack Chain: Inspects and halts suspicious outbound uploads, even via trusted platforms like SharePoint, preventing data theft or ransomware staging.

Detects Living-off-the-Land and Fileless Techniques: Behavior-based AI identifies PowerShell, w3wp.exe misuse, web shell activity, and scheduled tasks; all key elements of the ToolShell delivery chain.

Disrupts Lateral Movement and Policy Abuse: Anomaly detection and IP/domain restrictions stop tools like PsExec, Impacket, or GPO-based ransomware deployment before execution.

Tamper-Resistant + Non-Signature Detection: Blocks advanced persistence using IIS modifications, .NET assemblies, and stealth credential tools without relying solely on signatures.

BlackFog vs Warlock Ransomware

Threat Vector	Warlock / Storm-2603 Tactic	BlackFog Countermeasure
Initial Access	Exploiting SharePoint zero-days (ToolShell)	Real-time detection of web shell uploads, endpoint filtering
Web Shell & Persistence	spinstall0.aspx, scheduled tasks, IIS modifications	Behavioral monitoring, process isolation
Defender Evasion	services.exe manipulates registry to disable Defender	Tamper detection and Defender restoration alerts
Recon & Credential Theft	whoami, LSASS scraping via Mimikatz	Memory protection, anomaly detection, credential exfil prevention
Lateral Movement	PsExec, Impacket, WMI; GPObased ransomware deployment	Blocking lateral tools, GPO anomaly alerts, network isolation
Ransomware Deployment	Mass deployment of Warlock payload across domain via GPO	Policy enforcement, real-time execution blocking

Urgent Actions Recommended by Microsoft & CISA

Microsoft and CISA advise organizations with internet-facing on-prem SharePoint servers to:

- Apply cumulative security updates for SharePoint 2016, 2019, and Subscription Edition (addressing CVE-2025-49706, 49704, 53770, 53771)
- Enable AMSI (Full-Mode) and deploy Defender Antivirus + Defender for Endpoint
- Rotate ASP.NET machine keys & restart IIS on all servers
- Operate under the assumption of compromise, and activate incident response plans immediately

BLACKFOG®

Why BlackFog?

In a cyber landscape increasingly shaped by human-operated threats, organizations need more than reactive alerts, they need 24/7 real-time prevention. BlackFog delivers exactly that.

With its unique anti data exfiltration (ADX) technology, AI based behavioral threat detection, and dynamic blocking capabilities, BlackFog helps organizations prevent breaches by ensuring unauthorized data never leaves the network.

For organizations with lean internal teams, BlackFog's vCISO services provide expert leadership, streamlined incident response, and compliance-ready reporting, all tailored to the demands of that specific industry.

Ready to Learn More?

Visit blackfog.com or contact us at sales@blackfog.com

Award-winning Technology

MSP Today Product of the Year 2025 · Cybersecurity Breakthrough Award · Fortress Cyber Security Award · teiss Awards 2025 · Globee Awards · Cyber Security Excellence Awards Winner

Follow us:

Android · Chrome · Windows · Apple · iOS

Contact us for a demo

Start your free trial

Visit blackfog.com

© 2025 BlackFog, Inc.