THREAT CURE
RE-ARCHITECT YOUR THREAT LANDSCAPE

ThreatCure

Cyber Threat Advisory

Rising Warlock Ransomware Campaigns

CATEGORY

Ransomware Campaign

SEVERITY

High

Platforms

Windows

IMPACT

- Operational Disruption
- Data Theft & Exposure
- Financial Losses
- Reputational Damage

Description

Warlock Ransomware

Warlock ransomware campaigns have accelerated sharply in 2025, affecting organizations across industries and geographies. The group is exploiting unpatched, internet-facing Microsoft SharePoint servers to gain initial access, using the "ToolShell" exploit chain tied to multiple zero-day vulnerabilities. Once inside, affiliates execute a double-extortion model combining sensitive data theft with widespread file encryption.

Prominent breaches, such as those against Colt Technology Services and Orange Belgium, illustrate the severity of this threat. To date, Warlock has claimed more than 60 victims worldwide across telecom, finance, government, manufacturing, technology, and consumer sectors.

Attack Techniques

Initial Access

- In these incidents, Warlock operators primarily targeted internet-exposed, unpatched on-premises Microsoft SharePoint servers.
- They exploited a set of recently disclosed zero-day vulnerabilities:
  - **CVE-2025-49704**
  - **CVE-2025-49706**
  - **CVE-2025-53770**
  - **CVE-2025-53771**
- Collectively known as the “ToolShell” exploit chain, these flaws enable unauthenticated access and arbitrary command execution on vulnerable SharePoint instances.

2. **Establishing Persistence & Credential Theft**
   - Deployment of web shells.
   - Credential harvesting and privilege escalation.
3. **Lateral Movement**
   - Tools such as PsExec and Impacket used to move stealthily through the environment.
4. **Data Theft & Ransomware Deployment**
   - Sensitive information exfiltrated before encryption.
   - File encryption appends “.x2anylock” extensions.
   - Victims pressured via public leak sites.

Indicator of Compromise

SHA-256

a919844f8f5e6655fd465be0cc0223946807dd324fcfe4ee93e9f0e6d607061e

f711b14efb7792033b7ac954ebcfaec8141eb0abafef9c17e769ff96e8fecdf3

aca888bbb300f75d69dd56bc22f87d0ed4e0f6b8ed5421ef26fc3523980b64ad

d1f9ace720d863fd174753e89b9e889d2e2f71a287fde66158bb2b5752307474

da8de7257c6897d2220cdf9d4755b15aeb38715807e3665716d2ee761c266fdb

bba75dc056ef7f9c4ade39b32174c5980233fc1551c41aca9487019191764bac

SHA-1

22a7cd4bc7c5920d2e82a8ec7b79b64fd6335f72

b9c60c84be9bb503333e82f2e0b4024ce0d500c4

a5fa4b82f9fdad3f807d84f855f111aca600f1e2

1b14acdc80b4ea8e734d40f85a6d1b8765fc1b15

cf0da7f6450f09c8958e253bd606b83aa80558f2

0488509b4dbc16dcb6d5f531e3c8b9a59b69e522

Indicator of Compromise

MD5

2c01e4b57b4d7e01e755dc2dca53d9b8
363dfaa9fc77ae1f899049428a86d17e
23ee7c55dc6308099d90d0ad6d9f1709
1b5e6b1f7c46aaaaaecc49352e0e41eb
68bd43a00ba948f435ecbdd402914298
bf9f0c82c2ee89c7bc5480adc5e9494e

Recommended Defensive Measures

1. **Patch SharePoint Immediately**
   - Apply Microsoft’s updates for CVE-2025-49704, CVE-2025-49706, CVE-2025-53770, CVE-2025-53771.
   - Run vulnerability assessments to confirm compliance.
2. **Detection & Monitoring**
   - Deploy EDR and SIEM correlation rules to detect web shell activity and unusual PsExec/Impacket usage.
   - Monitor SharePoint logs for suspicious execution chains.
3. **Access & Network Segmentation**
   - Enforce least-privilege access policies.
   - Separate critical servers from general user networks.
4. **Backup & Recovery**
   - Maintain secure, offline backups.
   - Test recovery processes under simulated ransomware scenarios.

ThreatCure

Cyber Threat Advisory

Secure your byte world

Rising Warlock Ransomware Campaigns

Get Started Today

For more information about the ThreatCure ShieldOps Platform
or to schedule a demo, please contact:

- Website: www.threatcure.net
- Email: info@threatcure.net