مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Warlock Ransomware Campaign Targeting Microsoft SharePoint Servers

Tracking #:432317625
Date:22-08-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council observed the Warlock ransomware group exploiting unpatched Microsoft SharePoint servers and outdated Veeam software to gain remote code execution and deploy web shells for persistence and reconnaissance.

TECHNICAL DETAILS:

The Warlock ransomware group exploiting unpatched on-premises Microsoft SharePoint servers, leveraging critical vulnerabilities to achieve remote code execution (RCE) and initial network access. This campaign, first observed in mid-2025, demonstrates advanced tactics including web shell deployment, privilege escalation, credential theft, and data exfiltration, culminating in ransomware deployment based on a LockBit 3.0 derivative.

Initial Exploitation

- Exploited Vulnerabilities:
  - Microsoft SharePoint deserialization flaws – allowing authentication bypass and arbitrary code execution.
  - CVE-2023-27532 – affecting Veeam Backup software for lateral pivoting.
- Techniques:
  Attackers send crafted HTTP POST requests to upload web shells for remote control and reconnaissance.

Attack Chain Overview

- Initial Access: Exploitation of SharePoint and Veeam vulnerabilities.
- Web Shell Deployment: Enables command execution and persistence.
- Privilege Escalation:
  - Abuse of Group Policy Objects (GPOs) to create new GPOs, activate the guest account, and add it to Administrators.
- Defense Evasion & Discovery:
  - Use of native Windows tools (cmd.exe, nltest, ipconfig, tasklist) for enumeration.
- Credential Access:
  - Mimikatz for plaintext password dumping.
  - Registry hive dumping (SAM, SECURITY) via CrackMapExec.
- Lateral Movement:
  - SMB share propagation with malicious binaries disguised as vmtools.exe.
  - Security solution termination using malicious driver googleApiUtil64.sys, guided by log.txt.
- Ransomware Deployment:
  - Files encrypted with .x2anylock extension.
  - Ransom note dropped in affected directories.
  - Exfiltration to Proton Drive via RClone masquerading as TrendSecurity.exe.
- Additional Techniques:
  - DLL sideloading (e.g., MpCmdRun.exe, jcef_helper.exe).
  - Disk wiping with writenull.exe to prevent recovery.

Ransomware Characteristics

- Derivative of LockBit 3.0.

- Avoids encrypting whitelisted extensions, system directories, and specific system names for stealth.

Indicators of Compromise (IOCs)

- Attached in Excel

RECOMMENDATIONS:

- Apply patches immediately for Microsoft SharePoint and Veeam vulnerabilities.
- Restrict GPO modifications to authorized administrators and monitor for new GPO creation or guest account activation.
- Harden SMB shares by disabling unnecessary access and enforcing strong authentication.
- Deploy EDR/XDR solutions to detect suspicious process executions, credential dumping tools, and RDP enabling.
- Monitor for known IOCs, unusual RClone activity, and renamed binaries.
- Implement offline backups and test recovery procedures regularly.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.trendmicro.com/en_us/research/25/h/warlock-ransomware.html