EnCyb

Severity: High

Advisory Type: Threat

RecoverIt Malware Persistence via Windows Service Recovery

Advisory Report

TLP: WHITE

SECURITY THREAT ADVISORY COUNCIL (STAC)

Empowering organizations with cutting-edge cybersecurity strategies to combat emerging digital threats effectively.

EXECUTIVE SUMMARY

A new tool named RecoverIt abuses the legitimate Windows Service Failure Recovery mechanism to execute malicious payloads with elevated privileges and maintain persistence. By configuring services to run attacker-controlled commands upon failure, the technique avoids traditional exploit-based indicators and blends into normal system behaviour. This living-off-the-land approach enables stealthy, repeated execution of malware on Windows systems, posing a high risk across multiple sectors.

- Active Region: Global
- Affected Sector: Multiple sectors
- Affected Product: Windows Systems
- Severity: High
- Published Date: February 09, 2026

TECHNICAL DETAILS

- **Initial Access:** RecoverIt is deployed after initial access is obtained through phishing, malware infection, or compromised credentials.
- **Abuse of Windows Service Failure Recovery:** The tool creates or modifies a Windows service and configures service failure actions to execute an attacker-defined command or binary. When the service crashes or is forcibly stopped, Windows automatically launches the configured recovery command.
- **Payload Execution:** The recovery action is set to execute a malicious payload, script, or loader instead of restarting the service.
- **Evasion Techniques:** Abuse of legitimate Windows service functionality avoids exploit-based indicators. No registry autoruns or scheduled tasks are required.

IMPACT

- Execution of malicious payloads with SYSTEM-level privileges.
- Long-term persistence across system reboots.
- Increased difficulty in detection and forensic analysis.
- Abuse of trusted Windows components to bypass security controls.
- Potential deployment of additional malware, ransomware, or backdoors.

RECOMMENDATIONS

- Restrict service creation and modification to authorized administrators only.
- Audit Windows services for unexpected or suspicious failure recovery actions.
- Enforce least privilege and reduce unnecessary service permissions.
- Prevent services from launching cmd.exe, powershell.exe, or scripting engines unless explicitly required and approved.

REFERENCE

- New recoverit tool abuses windows service failure recovery
- Defense Evasion - The service run failed successfully

SECURE, SCALE, SUCCEED WITH

CONFIDENCE

EnCyb

www.encyb.com/contact-us/ EnCyb soc@encyb.com www.encyb.com