Cactus

[/ˈkæk.təs/]

The Cactus Ransomware Group is a financially motivated, high-risk threat active since 2023, known for ransomware-based extortion, data theft, and disruption. By 2025, it expanded operations by exploiting VPN vulnerabilities and using stealthy, defense-evasive techniques, impacting over 100 victims. The group mainly targets enterprises in manufacturing, professional services, critical infrastructure, and technology across the US, UK, and Europe.

IDENTITY

Attribution	: Financially motivated ransomware group.
Active Since	: 2023
Aliases	: GOLD VILLAGE, TA2101, Storm-0216, DEV-0216, UNC2198, TWISTED SPIDER, Maze Team.
Motivation	: Financial extortion, operational disruption, data theft.

TTPs

Initial Access	- Exploitation of vulnerabilities in VPN appliances (notably unpatched or exposed VPN services) - Credential harvesting from remote access systems - Brute-force and password spraying on internet-facing applications
Persistence	- Modification of Windows scheduled tasks - Abuse of ntuser.dat for AES key passing to maintain covert access
Execution	- Deployment of backdoors through remote management tools
Command & Control (C2)	- Chisel for covert tunneling and lateral movement - Encrypted C2 channels leveraging HTTPS traffic - Use of compromised VPN infrastructure for C2 relay
Malware & Tools	- Custom Cactus ransomware payload with encrypted configuration - Rclone for data exfiltration to cloud storage - Chisel for tunneling and lateral movement - Living-off-the-land tools (PowerShell, PsExec, WMI)
Techniques	- Double extortion (data theft + encryption) - Encrypted payload staging to evade detection - Privilege escalation using known Windows vulnerabilities - Disruption of backup systems prior to encryption

TARGET PROFILE

Targeted Sectors	- Corporate enterprises - Manufacturing and industrial sectors - Professional and managed service providers - Critical infrastructure operators - Technology and software companies
Geographies Targeted	- United States - United Kingdom - Wider Europe (especially Western and Central Europe)

THREAT ASSESSMENT

Risk Level	: High.
Recent Activity	: Over 100 confirmed victims as of 2025; rapid exploitation of newly disclosed VPN vulnerabilities.
Evolution	: Increasing operational sophistication; adoption of stealthier lateral movement and encryption techniques; broadened targeting scope.

NOTABLE OPERATIONS

- **2023:** First observed campaigns leveraging VPN appliance vulnerabilities.
- **2024:** Expansion into large enterprise networks; increased data theft prior to encryption.
- **2025:** Over 100 known victims; widespread use of Chisel tunneling and ntuser.dat AES-key persistence mechanism.