Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

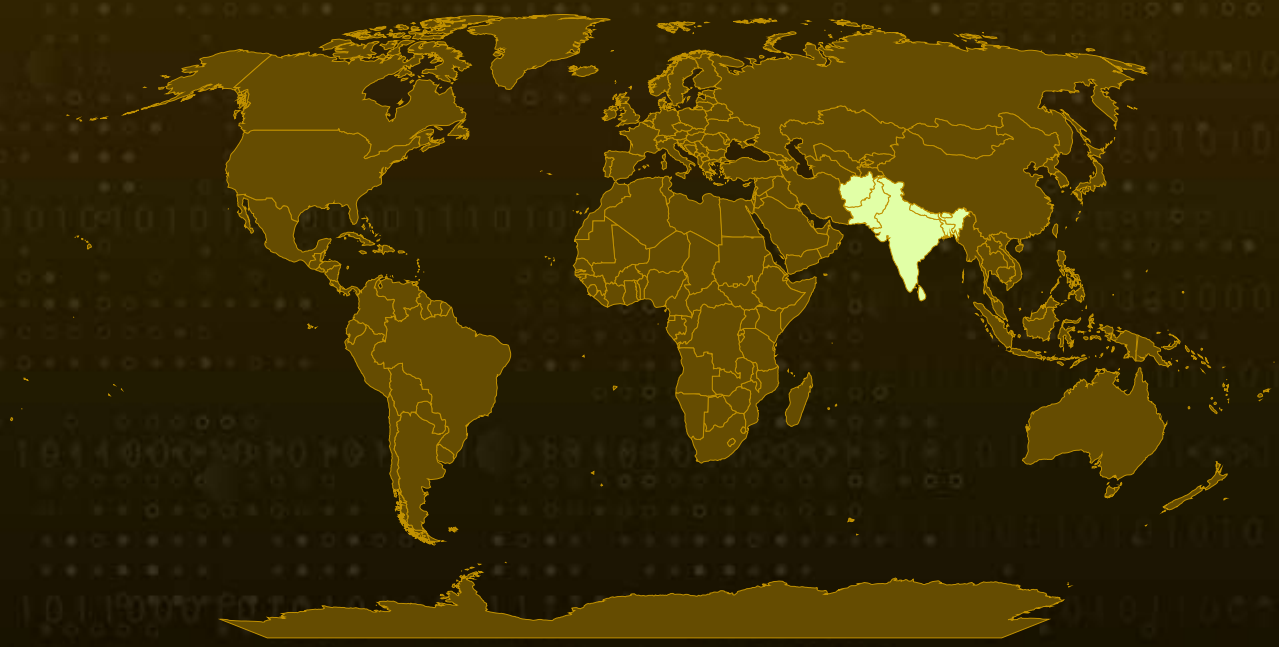
Spirals: The Ransomware That Doesn't Wait

Date of Publication	Admiralty Code	TA Number
July 17, 2026	A1	TA2026204

Summary

First Seen: June 16, 2026
Targeted Region: South Asia
Targeted Platform: Windows
Targeted Products: Microsoft IIS, ASP.NET, Microsoft Windows Defender, Microsoft Exchange, Microsoft Hyper-V, VMware, Veeam, Acronis, Veritas, Commvault, Microsoft SQL Server, Oracle, MySQL, PostgreSQL, Intuit, SAP, Lotus Domino
Targeted Industry: IT Services
Malware: Spirals
Attack: Spirals is a previously undocumented Rust-based ransomware family deployed against an IT services company in South Asia in June 2026. The operators completed the intrusion from initial access via an ASP.NET web shell on an internet-facing IIS server to network-wide encryption via PsExec in less than 24 hours. The payload uses per-file AES-128 keys wrapped with an attacker-controlled ECDH P-256 public key, applies intermittent encryption to files larger than 5 MB, and enforces a double-extortion model with a 6-day data-leak deadline.

Attack Regions



Targeted Non-Targeted

Attack Details

#1

The Spirals operators gained initial access on June 16, 2026, by compromising an internet-facing Microsoft IIS web server and uploading an ASP.NET web shell. Through the IIS worker process, they spawned cmd.exe and PowerShell to run an interactive, hands-on keyboard session. Within the first ten minutes, they deployed three network tunneling utilities: revsocks, Chisel, and a Cloudflare Tunnel client under legitimate-looking directories to establish redundant encrypted outbound channels.

#2

The operator then bypassed User Account Control for local privilege escalation, enabled Remote Desktop Protocol, and created a local account for persistence. A token impersonation tool was used to acquire further elevated privileges, and endpoint security tools were targeted for uninstallation. Additional payloads were retrieved from external staging infrastructure, in some cases disguised with .jpg extensions to bypass content inspection.

#3

Credentials were harvested by dumping the Security Account Manager hive to a password-protected archive and, later, by dumping LSASS process memory on multiple machines. The attackers then used WMI to move from the initial host to more than a dozen machines within minutes, leveraging accounts assessed as likely or built-in domain administrators. The cadence was consistent with automated tooling, and Active Directory enumeration during the foothold phase appears to have produced the target list for the subsequent mass deployment.

#4

The next day, the operator switched to PsExec running as SYSTEM to push a base64-encoded PowerShell payload to domain controllers, file servers, application servers, virtual machines, and workstations. The payload disabled Windows Defender, removed its threat definitions, and stopped 23 backup, database, and virtualization services, including Exchange, Hyper-V, VMware, Veeam, SQL Server, Oracle, and PostgreSQL, to release file handles before encryption.

#5

The Rust-based Spirals payload was named bitsadmin.exe to masquerade as the legitimate Windows BITS utility and dropped in domain-replicated locations to reach machines not directly targeted by PsExec. Files were encrypted with per-file AES-128 keys wrapped using an attacker-controlled ECDH P-256 public key, with intermittent encryption applied to files larger than 5 MB for speed. A ransom note threatened to publish stolen data after six days and directed victims to a Tor negotiation portal, confirming the double-extortion model.

Recommendations

Monitor PsExec Mass Deployment: Alert on rapid, sequential PsExec executions targeting many remote hosts within short windows, especially when accompanied by base64-encoded PowerShell payloads delivered as SYSTEM, since this is the exact deployment pattern used to distribute the Spirals payload across the victim environment.

Enforce UAC Enforcement and LSA Protection: Configure UAC to its highest enforcement level, enable Credential Guard, and enable LSA protection (RunAsPPL) to defeat both the UAC bypass and the LSASS credential dumping via rundll32.exe with comsvcs.dll observed in this intrusion.

Restrict SYSVOL and Domain-Replicated Share Write Access: Audit and tightly restrict write permissions to SYSVOL, DFSR replicated shares, and administrative shares on domain controllers, since the Spirals operators placed the payload in these locations to achieve domain-wide reach beyond hosts directly targeted by PsExec.

Isolate and Segment Backup Infrastructure: Place backup, database, and hypervisor management planes on isolated network segments with distinct credentials, and ensure backup services cannot be enumerated or stopped by domain administrator accounts alone, since Spirals halted 23 categories of backup and virtualization services before encryption.

Maintain Immutable, Offline Backups: Keep immutable or offline copies of critical data outside the reach of production Active Directory, and validate restore procedures under time pressure, given the under-24-hour intrusion-to-encryption timeline demonstrated in this case.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
	T1505: Server Software Component	T1505.003: Web Shell
Execution	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
		T1059.003: Windows Command Shell
	T1047: Windows Management Instrumentation	
	T1569: System Services	T1569.002: Service Execution
Persistence	T1136: Create Account	T1136.001: Local Account
Privilege Escalation	T1548: Abuse Elevation Control Mechanism	T1548.002: Bypass User Account Control
	T1134: Access Token Manipulation	
Defense Evasion	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
	T1036: Masquerading	T1036.005: Match Legitimate Name or Location
		T1036.008: Masquerade File Type
	T1140: Deobfuscate/Decode Files or Information	
Credential Access	T1003: OS Credential Dumping	T1003.002: Security Account Manager
		T1003.001: LSASS Memory

Tactic	Technique	Sub-technique
Discovery	T1087: Account Discovery	
	T1135: Network Share Discovery	
	T1518: Software Discovery	T1518.001: Security Software Discovery
	T1057: Process Discovery	
Lateral Movement	T1021: Remote Services	T1021.002: SMB/Windows Admin Shares
		T1021.001: Remote Desktop Protocol
Collection	T1560: Archive Collected Data	T1560.001: Archive via Utility
Command and Control	T1572: Protocol Tunneling	
	T1090: Proxy	T1090.001: Internal Proxy
	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1105: Ingress Tool Transfer	
Exfiltration	T1041: Exfiltration Over C2 Channel	
Impact	T1486: Data Encrypted for Impact	
	T1489: Service Stop	
	T1490: Inhibit System Recovery	
	T1657: Financial Theft	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	0f9574dc38e5c34a31153f0bcc603c6ec29cb3bf65c3d25380dbe86d42573141, 4cab935d0ec400059a3fcdc95b6623efdd51a61dff401fba8d5da244cc2de649, 7f0d49b11d0a3697685622ce510c570199bf2dc76515b3f9a6b6735de8c9134b, 83a7e51f3787ac5a8a9884edd0a58ddbef380969aa6529d282a461a1a614a892, 84b9a9a1668145df04faa3d0e118e2f0acbebd3d9d260baf3a355b44c815c22d, 862a3ca7e944ccf0ff3a6d556b34faade4b68343015c35a014a43725ac14a2a1, b5d598b00cc3a28cabc5812d9f762819334614bae452db4e7f23eefe7b081556
IPv4	185[.]141[.]216[.]194
URLs	hxxp[:]//185[.]141[.]216[.]194/cd[.]jpg, hxxp[:]//185[.]141[.]216[.]194/cd[.]zip, hxxps[:]//computer[.]kplus[.]com/cd[.]zip, hxxps[:]//beta[.]padmin[.]com/mybenefits/Templates/cd[.]zip
Filenames	bitsadmin.exe, vbr2116.exe, revsocks.exe, tunn.exe, chrome.exe, tokens.exe, cloudflared-windows-amd64.exe, RECOVERY_SECTION.log
File Paths	C:\RECOVERY_SECTION.log, CSIDL_PROFILE\public\tunn.exe, CSIDL_WINDOWS\tasks\tunn.exe, CSIDL_WINDOWS\tasks\chrome.exe, CSIDL_DRIVE_FIXED\webprodprojects\wicapfiles\cloudflared-windows-amd64.exe, CSIDL_WINDOWS\bitsadmin.exe, CSIDL_PROFILE\desktop\bitsadmin.exe, CSIDL_WINDOWS\sysvol_dfsr\domain\scripts\bitsadmin.exe, CSIDL_PROFILE\appdata\local\temp\vbr2116.exe

References

https://www.security.com/threat-intelligence/ransomware-spirals-extortion

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

July 17, 2026 • 04:00 PM

More at www.hivepro.com