

Spirals: New Stealthy Ransomware Deployed Against Asian IT Company

✓ security.com/threat-intelligence/ransomware-spirals-extortion



A previously unseen ransomware family, named Spirals by its operators, was deployed in a double extortion attack against an IT services company in South Asia in June 2026, the Symantec Threat Hunter Team can reveal. The Rust-based payload is either a new ransomware threat or one purpose-built for this attack. The actor behind the attack remains unknown

The attackers moved quickly. Less than 24 hours after the initial breach, the ransomware payload was being pushed to machines on the network. They obtained initial access by compromising an internet-facing IIS web server and uploading an ASP.NET web shell. Over a rapid three-hour interactive session, they established persistent access, uninstalled endpoint security software, dumped the Security Account Manager (SAM) hive, and set up covert remote access before later deploying the payload across the network.

On the day of initial access, the operator used the web shell to spawn `cmd.exe` and `powershell.exe` commands through the IIS worker process, enabling a hands-on-keyboard session. The operator performed local privilege escalation via a User Account Control (UAC) bypass, enabled Remote Desktop Protocol (RDP) and created a local account for persistence. They also enumerated users and network shares, listed installed program directories, and attempted to uninstall security tools using `wmic` and `mpcmdrun.exe`.

Credential material was harvested by dumping the Security Account Manager (SAM) hive to a password-protected archive. Later, during WMI-based lateral movement activities, the attackers also dumped LSASS process memory on multiple machines using rundll32.exe and comsvcs.dll. For covert command-and-control, the operator ran a reverse-SOCKS proxy (revsocks) to an external IP on port 443 and additionally exposed local RDP externally through a renamed Cloudflare tunnel binary. Payloads and tools were delivered from the same external IP and from two external staging domains, in some cases, using .jpg extensions to disguise the files.

The following day, the operator began deploying the ransomware payload across the victim's network using PsExec running as SYSTEM. The payload was named bitsadmin.exe, likely to masquerade as the legitimate Windows utility associated with the Background Intelligent Transfer Service. It encrypted files on impacted machines.

Spirals ransomware

The Spirals ransomware note was written to `C:\RECOVERY_SECTION.log`. Investigators also discovered the attackers' onion site, where they refer to the ransomware as Spirals. The ransom note threatens to publish stolen data after six days if a ransom is not paid and directs victims to a Tor portal for negotiations. This points to a typical double extortion attack, where attackers threaten to leak stolen data in addition to encrypting files.

The ransomware itself is a full-featured file-encrypting ransomware written in Rust. Its capabilities include defense evasion, encryption, lateral movement, process termination, obfuscation, and privilege escalation. Files are encrypted with per-file AES-128 keys wrapped using an attacker-controlled ECDH P-256 public key. Files larger than 5 MB are encrypted intermittently across jittered chunks for speed.

Full attack chain

The attackers obtained initial access by compromising an internet-facing IIS web server via an ASP.NET web shell. The first observed malicious activity occurred on June 16, 2026, at 22:21 local time, when a cluster of tunneling and reverse-proxy tools appeared on the first compromised host. These tools were placed under a web production directory and inside the Windows Tasks folder, paths that are consistent with access to or through an internet facing web server.

Three separate network-tunneling utilities were deployed to the host in the first 10 minutes of activity. The first, named tunn.exe (SHA256:

7f0d49b11d0a3697685622ce510c570199bf2dc76515b3f9a6b6735de8c9134b), appeared initially under a public web production directory:

```
CSIDL_PROFILE\public\tunn.exe
```

A second copy was then placed in the Windows Tasks folder, which is a common staging location used to blend in with legitimate scheduled task binaries:

```
CSIDL_WINDOWS\tasks\tunn.exe
```

Shortly afterwards, the revsocks.exe (SHA256: 4cab935d0ec400059a3fcdc95b6623efdd51a61dff401fba8d5da244cc2de649) reverse SOCKS proxy tool was dropped and executed in the same locations. The attackers also deployed the Chisel tunneling tool, renamed as chrome.exe to blend in with the Google Chrome browser:

```
CSIDL_WINDOWS\tasks\chrome.exe
```

A Cloudflare Tunnel client was also deployed to the web production directory, providing yet another channel for encrypted outbound communication:

```
CSIDL_DRIVE_FIXED\webprodprojects\wicapfiles\cloudflared-windows-amd64.exe
```

This combination of tunneling tools established multiple redundant channels for the attackers to maintain connectivity through the environment's network controls. Around the same time, a token impersonation tool named tokens.exe was executed from another web project directory, likely to acquire elevated privileges on the host:

```
CSIDL_DRIVE_FIXED\webprodprojects\[REMOVED]\tokens.exe
```

By 23:07, telemetry showed ransomware precursor activity on the initially compromised host, including attempts to disable security tools and download additional tooling.

Beginning at 23:33 on June 16, the attackers began using WMI for lateral movement from the initially compromised host toward other machines on the network. The activity involved multiple abused accounts, including accounts assessed as likely, or built-in, domain administrator accounts. More than a dozen machines were targeted within the first few minutes, with the cadence and command structure consistent with automated lateral movement rather than manual targeting.

The following day, June 17, the attackers shifted to PsExec as their primary deployment mechanism. Beginning at 14:44, PsExec remote sessions began delivering an identical base64-encoded PowerShell payload to machines across the environment. The decoded

payload performed two actions in sequence. First, it disabled Windows Defender's real-time monitoring and removed its threat definitions:

```
C:\progra~1\window~1\MpCmdRun.exe -RemoveDefinitions -All -  
DisableRealtimeMonitoring $true -Set-Mp Preference -DisableIOAVProtection  
$true
```

Second, it enumerated and forcibly stopped any running services whose names, display names, or descriptions matched a broad list of 23 backup, database, and virtualization products, including: Exchange, Hyper-V, VMware, Veeam, Acronis, Veritas, Commvault, SQL Server, Oracle, MySQL, PostgreSQL, Intuit, SAP, and Lotus Domino. Stopping these services before encryption is standard ransomware practice as it ensures that open file handles held by database and backup processes do not interfere with the encryptor's access to data files.

```
$p=@("*excha*", "*hyper*", "*vmms*", "*vmcompute*", "*virtual*", "*veeam*", "*backup*",  
"*acronis*", "*veritas*", "*commvault*", "*SQL Server*", "*oracle*", "*mysql*", "*postgre*",  
"*intuit*", "*sage*", "*sap*", "*domino*"); $p|%{$pt=$_;Get-WmiObject Win32_Service|?{($_.Name -like $pt)-  
or($_.DisplayName -like $pt)-or($_.Description -like $pt)}|?{($_.State -eq  
'Running')}|%{Stop-Service -Name $_.Name -Force -EA 0}}
```

Beginning at approximately 14:12 on June 17, a single host used psexec.exe to push the same payload to an extensive list of remote machines in rapid succession: more than one new target every few seconds for a period of approximately 30 minutes. The command was repeated for each target hostname in turn, with the same base64-encoded PowerShell blob delivered across the board:

```
CSIDL_WINDOWS\psexec.exe -accepteula -d -s \\<target> powershell -nop -w 1 -  
enc <base64-payload>
```

Targets included domain controllers, file servers, application servers, virtual machines, and a range of workstations bearing naming conventions consistent with a large enterprise environment. The breadth and pace of this push strongly suggests that the attackers had already compiled a target list, likely derived from Active Directory enumeration during the foothold phase, before initiating the mass deployment.

The ransomware payload (bitsadmin.exe) was placed across multiple locations to maximize coverage:

```
CSIDL_WINDOWS\bitsadmin.exe
```

```
CSIDL_PROFILE\desktop\bitsadmin.exe
```

CSIDL_WINDOWS\sysvol_dfsr\domain\scripts\bitsadmin.exe

\\[REMOVED]\esd\bitsadmin.exe

The placement in the SYSVOL domain scripts directory and on a network share hosted by a domain controller is particularly significant as both locations are replicated or accessible across the domain, providing a mechanism for the payload to reach machines that were not directly targeted by PsExec. In one case, Spirals (SHA256: 0f9574dc38e5c34a31153f0bcc603c6ec29cb3bf65c3d25380dbe86d42573141) was delivered as a renamed executable in the user's Temp directory:

CSIDL_PROFILE\appdata\local\temp\vbr2116.exe

The file was dropped by a process presenting as svchost.exe, a further layer of masquerading consistent with the attackers' broader pattern of impersonating legitimate Windows components.

While we have so far only seen this ransomware on one victim network, its capabilities and stealth point to the actors behind it being skilled operators who could easily launch more wide-ranging campaigns.

Protection/Mitigation

For the latest protection updates, please visit the [Symantec Protection Bulletin](#).

Indicator of Compromise (IOCs)

File indicators

0f9574dc38e5c34a31153f0bcc603c6ec29cb3bf65c3d25380dbe86d42573141 – Spirals ransomware – bitsadmin.exe, vbr2116.exe

4cab935d0ec400059a3fcdc95b6623efdd51a61dff401fba8d5da244cc2de649 – Revsocks – revsocks.exe

7f0d49b11d0a3697685622ce510c570199bf2dc76515b3f9a6b6735de8c9134b – Tunnel – tunn.exe

83a7e51f3787ac5a8a9884edd0a58ddbef380969aa6529d282a461a1a614a892 – Suspicious file

84b9a9a1668145df04faa3d0e118e2f0acbebd3d9d260baf3a355b44c815c22d – Chisel – chrome.exe

862a3ca7e944ccf0ff3a6d556b34faade4b68343015c35a014a43725ac14a2a1 – Token Impersonation Tool – tokens.exe

b5d598b00cc3a28cab5812d9f762819334614bae452db4e7f23eefe7b081556 – Cloudflared
– cloudflared-windows-amd64.exe

Network indicators

185.141.216[.]194

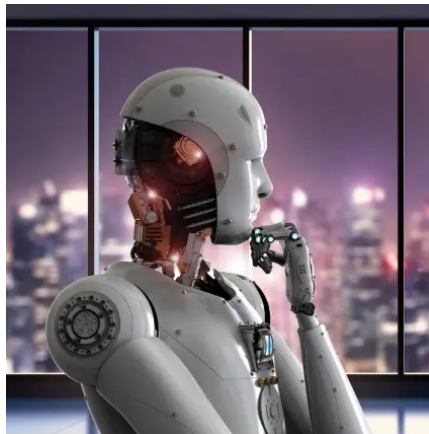
hxxp://185.141.216[.]194/cd.jpg

hxxp://185.141.216[.]194/cd.zip

hxxps://computer.kplus[.]com/cd.zip

hxxps://beta.padmin[.]com/mybenefits/Templates/cd.zip

About the Author



Threat Hunter Team

Symantec and Carbon Black

The Threat Hunter Team is a group of security experts within Broadcom whose mission is to investigate targeted attacks, drive enhanced protection in Symantec and Carbon Black products, and offer analysis that helps customers respond to attacks.