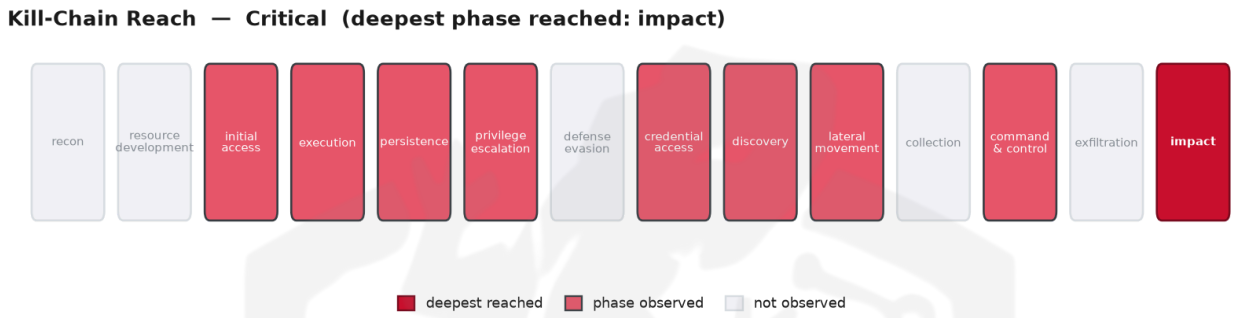
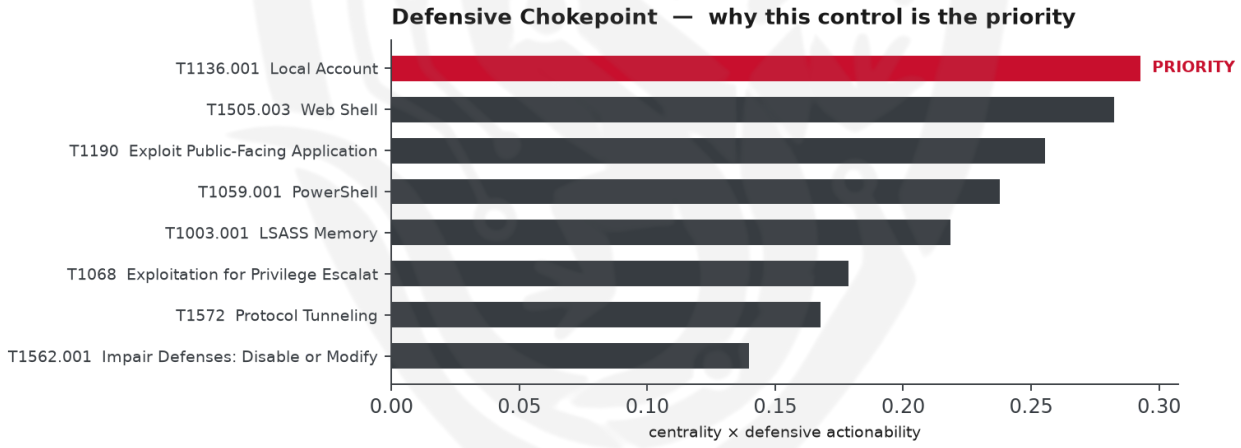
THREAT REPORT: UNKNOWN_ADVERSARY SPIRALS RANSOMWARE CAMPAIGN

Visual Summary



How far down the attack chain this campaign reached; deepest phase in crimson.



The control that most disrupts the attack (priority in crimson).

Summary

The observed cluster of activity has been attributed to the deployment of the Spirals ransomware against a technology company. The threat actor has utilized a range of malware families, including Spirals, ASP.NET web shell, and revsocks, to compromise the target. Priority should be given to monitoring for new local account creation and enforcing approval workflows for account provisioning. The operational risk band for this threat is Critical, indicating a high potential for impact.

Threat Overview

The threat actor, whose identity is currently unknown, has deployed the Spirals ransomware, leveraging various malware families to exploit the target. The central vulnerability exploited is currently unknown, but the actor has utilized techniques such as bypassing user account control, security account manager, and

protocol tunneling to achieve their goals. The victimology indicates that the target is a technology company, but the specific country and other details are insufficient.

Attack Chain and Priority Control

The observed techniques employed by the threat actor form a complex chain, including bypassing user account control, exploiting public-facing applications, and impairing defenses. The priority technique identified is T1136.001 Local Account, which serves as a critical chokepoint in the attack chain. To mitigate this threat, the priority control is to "Alert on new local/domain account creation (Event ID 4720/4728); enforce approval workflow for account provisioning."

Infrastructure and Corroboration

The malicious infrastructure associated with this campaign has been observed to be hosted on Rica Web Services. However, no malware families have been corroborated by abuse.ch, and there are no indicators with an AbuseIPDB confidence level of 80% or higher, with the highest confidence seen being 0%.

Technical Appendix

Ground-truth telemetry from the source pulse; analytical scores are secondary and clearly labelled.

Observed Techniques (ATT&CK, expert-tagged by source)

- T1548.002 Bypass User Account Control
- T1003.002 Security Account Manager
- T1036.005 Match Legitimate Resource Name or Location
- T1489 Service Stop
- T1135 Network Share Discovery
- T1190 Exploit Public-Facing Application
- T1572 Protocol Tunneling
- T1505.003 Web Shell
- T1136.001 Local Account
- T1003.001 LSASS Memory
- T1083 File and Directory Discovery
- T1059.001 PowerShell
- T1562.001 Impair Defenses: Disable or Modify Tools
- T1068 Exploitation for Privilege Escalation
- T1486 Data Encrypted for Impact
- T1570 Lateral Tool Transfer
- T1059.003 Windows Command Shell
- T1021.001 Remote Desktop Protocol
- T1090.001 Internal Proxy

Analytical Scores

- Priority technique (graph chokepoint): T1136.001 Local Account (centrality 0.3082).
- Operational risk: Critical (score 1.0, reaches impact).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4842; reference threshold tau = 0.6).
- These are behavioural resemblances for defensive playbook cross-referencing, not an identity assessment. Where the source pulse names an actor, that attribution is authoritative; the overlaps below neither confirm nor contest it.

Nearest historical profiles by behavioural overlap (resemblance only):

Historical Profile	Behavioural Overlap
APT5	0.4842
Fox Kitten	0.4537
FIN13	0.4529
Agrius	0.4297
Medusa Group	0.4115

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.

Indicators of Compromise (defanged — non-clickable)

The network and file indicators observed in this activity are listed below for blocklisting:

Type	Indicator	Context
IP	185[.]141[.]216[.]194	AbuseIPDB 0% (CA) · AS26832 Rica Web Services
Domain	beta[.]padmin[.]com	
Domain	computer[.]kplus[.]com	
URL	hxxps://beta[.]padmin[.]com/mybenefits/Templates/cd[.]zip	
URL	hxxps://computer[.]kplus[.]com/cd[.]zip	
Hash	26a15a6a9bea58e9ad2ada9a6c8606b5	

Type	Indicator	Context
Hash	e25c56bd13eff7280e493bf58501c47891fe63bf	
Hash	0f9574dc38e5c34a31153f0bcc603c6ec29cb3bf65c3d25380dbe86d42573141	
Hash	4cab935d0ec400059a3fcdc95b6623efdd51a61dff401fba8d5da244cc2de649	
Hash	7f0d49b11d0a3697685622ce510c570199bf2dc76515b3f9a6b6735de8c9134b	
Hash	83a7e51f3787ac5a8a9884edd0a58ddbef380969aa6529d282a461a1a614a892	
Hash	84b9a9a1668145df04faa3d0e118e2f0acbebd3d9d260baf3a355b44c815c22d	
Hash	862a3ca7e944ccf0ff3a6d556b34faade4b68343015c35a014a43725ac14a2a1	
Hash	b5d598b00cc3a28cabc5812d9f762819334614bae452db4e7f23eefe7b081556	

Reputation by AbuseIPDB · malware attribution by abuse.ch · Geo/ASN data by IP2Location LITE.

Flame Cell // Adversary Pivot [BETA]

BETA. A hypothetical tabletop projection, anchored to documented ATT&CK behaviour and technique co-occurrence across 170 tracked groups. It is not a prediction; treat it as a war-game prompt and review before acting. Spot a pivot that looks wrong? norbert@salacti.com

- **Control applied:** T1136.001 Local Account (persistence)
- **Observed here:** the threat actor used T1505.003 Web Shell here as an alternative persistence technique.
- **Projected pivot:** T1505.003 Web Shell (persistence)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

The threat actor could pivot to using T1505.003 Web Shell to maintain access and execute commands on the compromised web server, potentially by exploiting vulnerabilities in web applications or injecting malicious code into existing web pages. This would likely allow the actor to bypass the blocked local account control and continue their campaign objectives. To counter this, the mandated defensive control of integrity-monitoring web-server directories for web shells and restricting server module/plugin installation should be implemented.

Detection and hardening for the pivot (T1505.003 Server Software Component)

- **Telemetry:** Web server logs; File integrity monitoring on web roots; EDR
- **Detect:**
  - New/modified files in web-accessible directories (aspx/php/jsp)
  - w3wp.exe / httpd spawning cmd.exe, powershell.exe or whoami
  - Anomalous POSTs to newly created endpoints in web access logs
- **Harden:**
  - File integrity monitoring on web roots; least-privilege service accounts
  - Remove dev tooling from production web servers; WAF in front
- **MITRE:** M1047 Audit, M1018 User Account Management, M1042 Disable or Remove Feature · DS0022 File, DS0009 Process, DS0015 Application Log