Hive Pro

Threat Level

Red

HiveForce Labs

# THREAT ADVISORY

## ATTACK REPORT

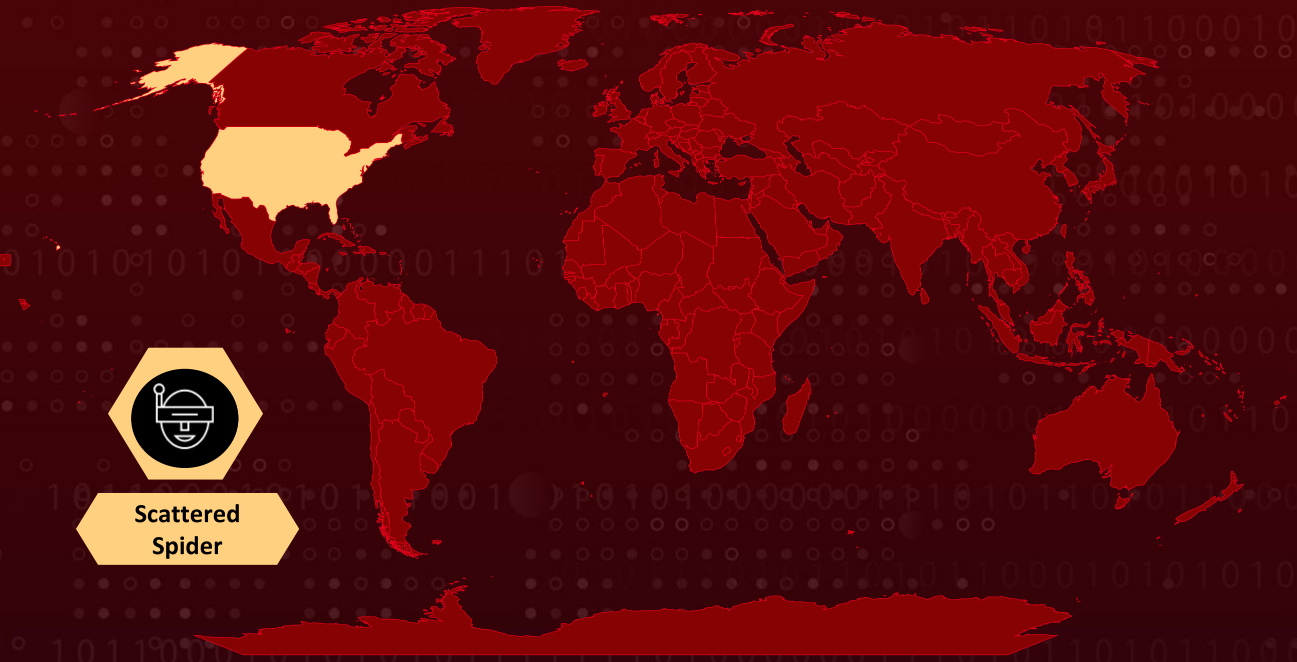
# Scattered Spider's Hypervisor Attack on VMware vSphere

| Date of Publication | Admiralty Code | TA Number |
|---|---|---|
| July 29, 2025 | A1 | TA2025235 |

# Summary

**First Seen:** June 2025
**Targeted Country:** United States
**Targeted Platforms:** VMware vSphere, Windows
**Threat Actor:** Scattered Spider (aka UNC3944, Starfraud, 0ktapus, Storm-0875, LUCR-3, Scatter Swine, Muddled Libra, Octo Tempest and 0ktapus)
**Targeted Industries:** Retail, Airline, Insurance
**Attack:** Scattered Spider launched a mid-2025 campaign targeting VMware vSphere environments by using social engineering to gain Active Directory access, then exploiting vCenter and ESXi for credential theft and ransomware deployment. They bypass traditional defenses by operating at the hypervisor level, extracting data from offline-mounted virtual disks. This infrastructure-focused attack avoids malware and relies on built-in tools, making detection difficult. The campaign highlights the urgent need for hardened identity controls, vSphere monitoring, and resilient backup strategies.

## Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

# Attack Details

#1

In mid-2025, threat actor Scattered Spider, also known as UNC3944 or Octo Tempest, launched a targeted campaign against organizations using VMware vSphere environments. This group, notorious for using social engineering and SIM swapping tactics, shifted focus toward infrastructure-level attacks that bypass traditional endpoint defenses. Their campaign begins with compromising helpdesk personnel or identity workflows through techniques like vishing or MFA reset manipulation, ultimately gaining administrative access to Active Directory environments.

#2

Once inside, the attackers pivot laterally to VMware vCenter servers and ESXi hosts. They frequently reboot vCenter appliances into single-user mode to gain root access and enable SSH, which is typically disabled in hardened environments. This access allows them to mount virtual disks from domain controllers offline and extract sensitive credentials, especially the NTDS.dit file and SYSTEM registry hives, without triggering endpoint or EDR alerts, as these actions occur entirely outside the guest operating systems.

#3

Scattered Spider leverages these privileges to steal data and, in many cases, deploy ransomware directly from the hypervisor level. Because vSphere environments manage multiple virtual machines and business-critical services, this allows the group to rapidly encrypt or destroy large portions of an enterprise's infrastructure. They also frequently delete or tamper with backup systems, making recovery nearly impossible if adequate segmentation and immutability protections are not in place.

#4

What makes this campaign especially dangerous is its stealth and speed. By avoiding malware and relying instead on built-in system tools, Scattered Spider can achieve their objectives without tripping conventional security monitoring. Their deep understanding of vSphere and identity infrastructure allows them to operate with surgical precision. Defenders must now treat the virtualization layer as a prime attack surface, requiring hardened identity controls, infrastructure logging, and resilient backup strategies.

# Recommendations

**Identity and Access Control:** Organizations should implement phishing-resistant multi-factor authentication (MFA), such as FIDO2 security keys or authenticator apps with number matching, and eliminate weaker methods like SMS or voice-based MFA. Helpdesk processes must be hardened with strict identity verification procedures, including callbacks to known contacts or on-camera validation, to prevent social engineering-based account takeovers.

**vSphere and ESXi Hardening:** To reduce exposure at the virtualization layer, ESXi Lockdown Mode should be enabled, and direct SSH access to hypervisors must be disabled. Access to vCenter should follow least-privilege principles, and Active Directory-integrated accounts with administrative privileges should be minimized or removed entirely. Limiting domain access to vSphere systems significantly narrows the attack surface.

**Logging and Detection Enhancements:** It is essential to centralize logging from vCenter and ESXi into a SIEM to correlate with Active Directory events. Security teams should monitor for specific indicators such as VmReconfiguredEvent, AD Event ID 4728, unauthorized reboots, and offline disk mounts. Detecting early signs of compromise in infrastructure layers requires visibility well beyond endpoint security tools.

**Backup Protection and Resilience:** Backup systems must be isolated from production domains and configured with immutable or air-gapped storage to prevent sabotage during an attack. Encrypting virtual machines, particularly domain controllers and other Tier-0 assets, ensures that even if virtual disks are accessed offline, the data remains protected. Continuous monitoring of backup activities helps detect tampering or unauthorized restoration attempts.

## Potential MITRE ATT&CK TTPs

| | | | |
|---|---|---|---|
| TA0043<br>Reconnaissance | TA0042<br>Resource Development | TA0001<br>Initial Access | TA0002<br>Execution |
| TA0007<br>Discovery | TA0008<br>Lateral Movement | TA0009<br>Collection | TA0011<br>Command and Control |

| | | | |
|---|---|---|---|
| **TA0003**<br>Persistence | **TA0004**<br>Privilege Escalation | **TA0005**<br>Defense Evasion | **TA0006**<br>Credential Access |
| **TA0010**<br>Exfiltration | **TA0040**<br>Impact | **T1657**<br>Financial Theft | **T1567**<br>Exfiltration Over Web Service |
| **T1566.004**<br>Spearphishing Voice | **T1598**<br>Phishing for Information | **T1566**<br>Phishing | **T1059.001**<br>PowerShell |
| **T1490**<br>Inhibit System Recovery | **T1547**<br>Boot or Logon Autostart Execution | **T1078.002**<br>Domain Accounts | **T1078**<br>Valid Accounts |
| **T1548.001**<br>Setuid and Setgid | **T1204**<br>User Execution | **T1136**<br>Create Account | **T1548**<br>Abuse Elevation Control Mechanism |
| **T1562.001**<br>Disable or Modify Tools | **T1562**<br>Impair Defenses | **T1036.005**<br>Match Legitimate Name or Location | **T1036**<br>Masquerading |
| **T1003.003**<br>NTDS | **T1003**<br>OS Credential Dumping | **T1555**<br>Credentials from Password Stores | **T1018**<br>Remote System Discovery |
| **T1087.002**<br>Domain Account | **T1087**<br>Account Discovery | **T1555.003**<br>Credentials from Web Browsers | **T1021**<br>Remote Services |
| **T1005**<br>Data from Local System | **T1486**<br>Data Encrypted for Impact | | |

## References

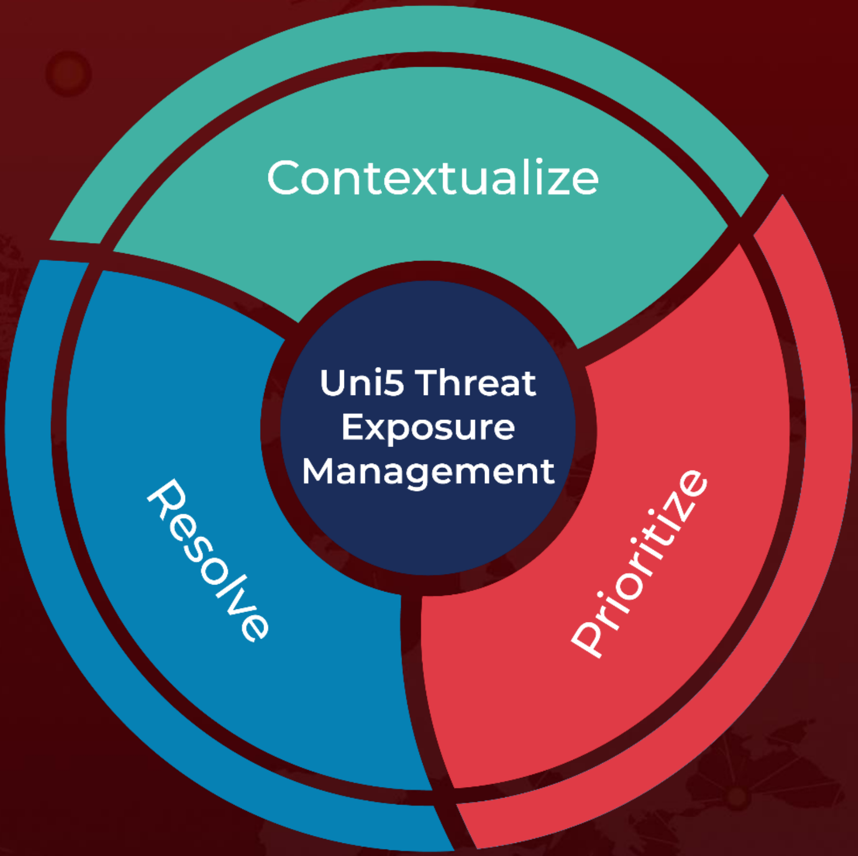
https://cloud.google.com/blog/topics/threat-intelligence/defending-vsphere-from-unc3944

https://hivepro.com/threat-advisory/scattered-spider-cyber-threat-key-findings-and-security-measures/

# 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 free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

**July 29, 2025 • 8:30 AM**

More at www.hivepro.com