Executive Summary

This week's brief covers 3 new threat campaigns sourced from Google Threat Intelligence (GTI), confirmed active. The most time-critical entry is the scattered spider SaaS hijack (CAMP.26.031), which uses SMS phishing and MFA fatigue attacks to hijack OKTA, Azure AD etc, to exfiltrate patient data via SharePoint and OneDrive.

Active Threat Campaigns- Healthcare & Technology

Campaign	Type	Key Techniques	Targets	Priority Action
Scattered Spider SaaS Identity Attack (CAMP.26.031) UNC3944	Credential Theft / Espionage	SMS phishing + MFA fatigue to hijack Okta, Azure AD, M365; exfiltrates patient/IP data via SharePoint and OneDrive	Healthcare, Tech, Insurance — US, UK, CA	**CRITICAL — Enforce phishing-resistant MFA (FIDO2); audit Okta app assignments; block legacy auth; alert on impossible-travel logins**
BlackSuit Ransomware HC Targeting (CAMP.26.033)	Financial / Ransomware	Exploits unpatched VPN/RDP; deploys custom encryptor; double extortion via leak site; targets EHR and PACS systems	Healthcare, Critical Infrastructure — US, EU	HIGH — Patch internet-facing VPN/RDP; verify EDR on all endpoints; test backup restoration; segment EHR from general network
PyPI Malicious Package Wave (CAMP.26.029)	Financial/Supply Chain	Trojanized Python packages mimic popular ML/data libs; harvest AWS/GCP creds and SSH keys; beacon to C2 over HTTPS	Technology, Healthcare DevOps — US, EU, KR	HIGH — Audit PyPI dependencies immediately; use private registry or allowlist; rotate cloud credentials and SSH keys; scan CI/CD pipelines

Top 3 Actions This Week

1. [CRITICAL] Stop Scattered Spider SaaS Identity Attacks — UNC3944 (CAMP.26.031)

Active since March 18, 2026, UNC3944 (Scattered Spider) is conducting a high-tempo identity attack campaign against healthcare payers, health-tech platforms, and enterprise technology firms across the US, UK, and Canada. The attack chain begins with targeted SMS phishing to harvest credentials, followed by MFA fatigue attacks or SIM-swap fraud to bypass authentication. Once inside, the actor pivots across Okta-connected SaaS applications, exfiltrates patient data and intellectual property via SharePoint and OneDrive, and establishes persistent access through rogue OAuth app registrations.

- Immediately enforce phishing-resistant MFA (FIDO2/WebAuthn hardware keys) on all privileged accounts and any accounts with access to EHR, billing, or IP data
- Audit Okta app assignments and Azure AD enterprise applications — revoke any unrecognized OAuth grants
- Block all legacy authentication protocols (Basic Auth, SMTP AUTH) across M365 and Azure AD
- Enable impossible-travel and anomalous sign-in risk policies in Conditional Access
- Notify employees of active SMS phishing campaign — do not approve unexpected MFA push prompts

2. [HIGH] Defend Against BlackSuit Ransomware Healthcare Targeting (CAMP.26.033)

Active since March 20, 2026, BlackSuit ransomware (the operational successor to Royal ransomware, itself a rebrand of Conti) has begun a targeted campaign against US and EU healthcare systems, specifically targeting organizations running unpatched Cisco VPN appliances and exposed RDP. Once inside, the group deploys a custom encryptor that specifically targets EHR databases (Epic, Cerner) and PACS/radiology systems, maximizing pressure for ransom payment. The group operates a double-extortion leak site.

- Immediately patch all internet-facing VPN appliances (Cisco ASA, Fortinet, Pulse) and disable unnecessary RDP exposure
- Verify endpoint detection and response (EDR) is deployed and active on all clinical endpoints, including imaging workstations
- Test backup restoration procedures — confirm immutable or air-gapped backups exist for EHR and PACS systems
- Segment EHR and radiology networks from general corporate networks using firewall rules
- Review recent authentication logs for VPN and RDP for unusual access patterns or off-hours activity

3. [HIGH] Block PyPI Malicious Package Supply Chain Attack (CAMP.26.029)

Active since March 15, 2026, a DPRK-affiliated actor (UNC6801) — distinct from the DPRK GitHub tampering campaign (CAMP.26.014) — is distributing malicious Python packages via PyPI that impersonate popular machine learning and data science libraries (e.g., typosquats of numpy, pandas, boto3, scikit-learn). Once installed, packages harvest AWS credentials, GCP service account keys, and SSH private keys, then beacon to a C2 server over HTTPS. Healthcare DevOps and technology engineering teams are primary targets. Note: This campaign is entirely separate from the February 9 Shai-Hulud NPM Worm (CAMP.25.079), which targeted the NPM/Node.js ecosystem.

- Audit all PyPI packages in use across development environments and CI/CD pipelines immediately
- Switch to a private package registry (Artifactory, AWS CodeArtifact) or implement an allowlist of approved packages
- Rotate all AWS access keys, GCP service account credentials, and SSH keys accessible from development machines
- Scan CI/CD pipeline configurations for recently added or modified install steps
- Alert on outbound HTTPS connections from build servers to non-corporate domains
-

Threat Metrics

Activity Trends

▲ Identity/SaaS attacks: significant escalation (Scattered Spider)

▲ Healthcare-targeted ransomware: +35% vs. prior week

▲ PyPI/Python supply chain attacks: emerging vector

▲ Iran-nexus wiper posture: sustained, no new confirmed incidents

▼ Ransomware incidents (broad): -8% vs. prior week

Cumulative IOC Count: 520+ (new this week)

File hashes: 71+

IP addresses: 55+

Domains: 69+

URLs: 131+

(Carried-over IOCs from prior briefs available in GTI portal)