CRITICALSTART®

Daily Intelligence Update | 6 October 2025

The growing threat of macOS infostealers has become a defining trend in 2025, as Apple devices—once perceived as more secure—are increasingly targeted by cybercriminals. Dark web chatter and underground market activity suggest macOS infostealers are in high demand, with offerings now delivered through Malware-as-a-Service subscription models that provide customer support and regular updates. These tools exfiltrate credentials, cookies, cryptocurrency wallets, and SaaS tokens, all of which can be directly monetized or resold. The combination of Apple's wealthy consumer base and rising enterprise adoption has made macOS endpoints strategic assets, particularly in corporate environments where they can provide attackers with access to developer tools, VPNs, and cloud platforms. Modern macOS malware now bypasses native protections, maintains persistence, and is priced at a premium compared to Windows infostealers, reflecting both scarcity and profitability. Analysts warn that organizations must begin treating macOS security with the same urgency as Windows, investing in monitoring, awareness, and controls to mitigate this rapidly maturing threat.

Meanwhile, researchers are tracking a wave of disruptive ransomware and phishing operations. CyberVolk, a pro-Russia ransomware group active since 2024, has been targeting critical infrastructure and public institutions in countries including Japan, France, and the UK. Its ransomware leverages AES-256 GCM and ChaCha20-Poly1305 encryption, but its design fatally omits nonce storage, rendering decryption impossible even with the correct key. Victims receive ransom notes with hardcoded decryption keys that are guaranteed to fail, meaning recovery depends entirely on having resilient backups. At the same time, a phishing campaign dubbed ZipLine is abusing "Contact Us" forms to target supply chain and manufacturing firms in the U.S. Attackers build trust over weeks of email exchanges before sending malicious ZIP files that load MixShell, an in-memory implant communicating via DNS tunneling and evading defenses through AMSI bypass and COM hijacking. Another trend involves fake Microsoft OAuth applications, where phishing kits like Tycoon are used to impersonate trusted brands such as Adobe, DocuSign, and RingCentral. By tricking users into approving malicious OAuth apps, attackers bypass MFA protections, steal session tokens, and gain account access—an approach that continues to evolve and expand across Microsoft 365 tenants.

The extortion landscape also continues to fragment, with researchers observing a new ransomware blog, SECUROTROP, which lists sixteen victims, twelve of which already have their data published for download. The group appears to have splintered from Qilin, as multiple victims first listed under Qilin later appeared on SECUROTROP's site. The overlap suggests either a rebranding or an operational split, reinforcing the trend of fluid alliances within the ransomware ecosystem.

Other emerging threats include VoidProxy, a newly discovered Phishing-as-a-Service platform that enables highly evasive adversary-in-the-middle attacks against Microsoft, Google, and Okta accounts. Using multilayered infrastructure with disposable domains, Cloudflare Workers, CAPTCHA challenges, and dynamic DNS, VoidProxy intercepts real-time authentication flows, stealing credentials, MFA codes, and session tokens. For Okta-federated accounts, it deploys second-stage phishing pages that mimic SSO flows, capturing tokens and handing attackers immediate access through an admin panel hosted on serverless platforms.

September also saw a surge in hacktivist activity across multiple regions. Groups like Malaysia Hacktivist, Tengkorak Cyber Crew, Hezi Rash, and Mr. Hamza led campaigns involving DDoS, defacement, and claimed data leaks. The pro-Russian group TwoNet exposed data from Spain’s C1b3rWall cyber conference, while Enlace Hacktivista leaked 600 GB tied to China’s Great Firewall project. Hezi Rash launched #OpJapan, while other groups like Keymous and Nullsec Philippines continued targeting France and China, respectively. CyberVolk extended its campaign rhetoric against Western and Japanese entities, and Handala Hacktivists claimed insider access to an Israeli space firm, signaling that politically motivated campaigns remain highly active and unpredictable.

On the vulnerability front, researchers disclosed a flaw in OnePlus OxygenOS, tracked as CVE-2025-10184, that allows apps to access SMS data and metadata without requiring user permissions. The issue, introduced by modifications to Android’s Telephony package, includes an SQL injection weakness that lets attackers brute-force SMS content from device databases. Affecting OxygenOS versions 12 through 15 on devices like the OnePlus 8T and 10 Pro, the flaw significantly increases the risk of credential theft and OTP interception. OnePlus has confirmed the issue and pledged a patch in mid-October, but in the meantime, users are advised to reduce app exposure, adopt secure authenticator apps, and rely on encrypted messaging platforms for sensitive communications.
