Daily Intelligence Update | 17 October 2025

Researchers observed Chinese APT group Jewelbug (also known as REF7707, CL-STA-0049, and Earth Alux) targeting a Russian IT service provider in an intrusion that lasted from January to May 2025. This is significant as Chinese and Russian threat actors have historically avoided direct targeting of one another, and in this case Jewelbug appeared focused on carrying out a potential software supply chain attack by accessing code repositories and software build systems, which could have enabled them to distribute malicious updates across the provider's large Russian customer base. The attackers employed several hallmark TTPs, including use of a renamed Microsoft-signed Console Debugger (cdb[.]exe) as 7zup[.]exe to run shellcode, bypass whitelisting, and terminate security solutions, while persistence and privilege escalation relied on scheduled tasks and credential dumping. On the criminal side, Spanish retail giant Mango disclosed on October 14, 2025 that one of its external marketing service providers had suffered a breach exposing customer data such as first names, postal codes, phone numbers, and emails, though no financial data, passwords, or IDs were included. The following day, F5 confirmed a nation-state intrusion into its BIG-IP development environment dating back to August, in which adversaries exfiltrated source code and details of undisclosed vulnerabilities. While the company found no signs of supply chain tampering, intellectual property theft could support future exploitation, and limited customer configuration data was also exposed. F5 worked with CrowdStrike, Mandiant, and law enforcement to contain the incident, released hunting guides for the China-linked UNC5221's "Brickstorm" malware, and alongside CISA urged urgent patching, decommissioning end-of-support devices, and hardening of public-facing management interfaces. In parallel, researchers tracked the evolution of cybercrime services throughout September 2025, noting an Elite Malicious Software Suite marketed for $5,000 per month that combines RAT, stealer, HVNC, wallet-cracking, and remote control functions with customer logs stored locally rather than by the vendor. Another actor advertised HOOK Android Botnet rentals at $5,000 per month with over 1,000 prebuilt injectors and optional crypt services, while a separate vendor introduced the MacSync macOS Stealer for $1,500 per month, designed to harvest passwords, cookies, crypto wallets, and macOS keychain entries. Notably, MacSync restricts use in CIS countries, while its phishing module mimics the Ledger crypto app to steal recovery seeds. Together these developments underscore the growing intersection of state-backed campaigns, corporate data breaches, and the professionalization of cybercrime services, with adversaries leveraging supply chain intrusions, advanced malware frameworks, and MaaS offerings to expand reach and persistence across global enterprises.
