Daily Intelligence Update | 22 September 2025

Researchers have uncovered the first documented cases of collaboration between the Russian-aligned espionage groups Gamaredon and Turla in Ukraine, marking a notable development in Moscow's cyber operations. In February 2025, telemetry revealed that Gamaredon's PteroGraphin tool was used to restart Turla's Kazuar backdoor on a compromised system. Over the following months, Kazuar v2 was observed being deployed directly by Gamaredon's tools, including PteroOdd and PteroPaste, signaling an active cooperative relationship. Gamaredon, active since 2013, has typically focused on widespread compromises within Ukrainian government institutions, while Turla has historically concentrated on diplomatic and high-value government entities across Europe and the Middle East. Analysts suggest that this collaboration, consistent with both groups' reported ties to Russia's FSB, likely involves Gamaredon providing broad initial access for Turla to selectively infiltrate high-priority systems. By mid-2025, activity linked to this partnership had reportedly intensified, underscoring a more coordinated Russian effort to combine scale and precision in its cyber campaigns.

In parallel, researchers have identified RatOn, a newly discovered Android malware that blends Remote Access Trojan (RAT) capabilities with Automated Transaction System (ATS) features to target both cryptocurrency wallets and mobile banking apps. First detected in July 2025, RatOn is distributed via adult-themed domains and circumvents Android restrictions by abusing Accessibility services to secure Device Admin privileges and other elevated permissions. The malware executes overlay attacks to steal sensitive data such as recovery phrases and PIN codes, and it automates fraudulent money transfers by manipulating legitimate apps. Notably, it has been seen targeting apps like MetaMask, Trust Wallet, and George Česko in the Czech Republic, adjusting transaction limits and entering payment data without user interaction. The combination of RAT functionality and ATS automation suggests that RatOn is designed for both surveillance and high-volume financial theft, making it a serious threat to mobile users across multiple regions.

Meanwhile, Apple has released backported security updates to older iPhone and iPad models to address an actively exploited zero-day vulnerability tracked as CVE-2025-43300. Originally patched on August 20 in iOS 18.6.2, iPadOS 18.6.2, and macOS, the flaw resides in the Image I/O framework and stems from an out-of-bounds write condition that can be exploited to trigger crashes, corrupt data, or achieve remote code execution. Apple confirmed the vulnerability had been exploited in targeted attacks against specific individuals, prompting the company to extend fixes to legacy devices including the iPhone 6s, iPhone SE (1st generation), iPhone 7, iPhone 8, iPad Air 2, and iPad mini 4. The newly released iOS 15.8.5 and iPadOS 15.8.5 updates, among others, improve bounds checking to prevent exploitation. The move highlights the continued targeting of older devices by sophisticated threat actors and reinforces the importance of patching even for legacy platforms still in widespread use.

---

detect threats early and respond quickly, with every action backed by contractual service-level agreements that ensure trusted outcomes for security teams.

For more information, visit www.criticalstart.com.