Daily Intelligence Update | 18 September 2025

Researchers have uncovered a new variant of the Hook Android banking trojan, now incorporating ransomware-style overlays, lockscreen bypass capabilities, and advanced screen-streaming for real-time monitoring. Delivered through phishing sites and GitHub-hosted APKs, the malware leverages Android Accessibility Services to automate fraud, capture credentials, and bypass security controls. Hook v3 reportedly supports 107 remote commands, including newly added functions such as PIN-capturing lockscreen mimicry and HTML-based card and NFC overlays. Commands like unlock_pin enable attackers to wake and unlock devices, while takencard and takenfc allow for phishing through crafted overlays. Early signs suggest the malware's operators are experimenting with RabbitMQ-based C2 infrastructure and potential Telegram-based communications, though these remain under development. Analysts also observed GitHub being used for payload delivery, with overlap between Hook and other Android malware families such as Ermac and Brokewell.

In parallel, researchers detailed a Linux malware campaign abusing a malicious shared object file, terminate[.]so, to initiate a multi-stage attack. Triggered by a Python loader, the malware decrypts an embedded payload using AES-CBC and drops two files: vcpktsvr, a legitimate-looking executable for DLL sideloading, and libcef[.]so, a malicious library that transmits system information to a Zulip channel controlled by the attackers. The campaign, active since July 2025, disguises C2 communications as legitimate HTTPS traffic while obfuscating DLL and API names through a custom hashing algorithm. Persistence is achieved by adding registry entries pointing to the dropped executable, enabling stealthy cross-platform attacks against both Linux and Windows environments. Researchers linked the activity to a Zulip account registered with a ProtonMail address, suggesting a persistent operator.

The Lumma Stealer has also resurfaced following its May 2025 takedown, during which authorities seized more than 2,300 domains tied to its infrastructure. Despite this disruption, the malware quickly reemerged with new infrastructure hosted on Russian data centers such as Selectel. Recent campaigns leverage deceptive lures like software cracks, AI-generated GitHub repositories, social media bait, and CAPTCHA pages using ClickFix-style PowerShell delivery to distribute payloads. Lumma continues to operate under a malware-as-a-service model, offering credential theft, clipboard capture, and screenshot exfiltration to a wide range of customers, lowering the barrier for less sophisticated cybercriminals.

Meanwhile, a new ransomware group dubbed BlackShrantac has emerged with a dark web leak site identified on September 17, 2025. At launch, the site listed two victims, with one victim's stolen data already made available for free download. The leaks included corporate logos and partially redacted domain names, enabling attribution of at least one organization. While the group has not yet provided details on its motives, terms, or operational scale, victims are instructed to communicate via TOR using a lengthy identifier string. The absence of an "About Us" section or broader context leaves BlackShrantac's long-term objectives unclear, but its early tactics align with typical double-extortion models.

Separately, the U.S. Department of Justice announced that Conor Brian Fitzpatrick, better known as Pompompurin, the former administrator of BreachForums, has been resentenced to three years in prison. Initially arrested in 2023 and briefly sentenced to time served plus 20 years of supervised release, his case was reopened following a Fourth Circuit ruling vacating the original sentencing. Fitzpatrick pleaded guilty to conspiracy to traffic in access devices, solicitation, and possession of child sexual abuse

material, and agreed to forfeit hundreds of domains, devices, and cryptocurrency tied to his operations. Authorities emphasized that his trafficking of stolen data and CSAM caused severe, lasting harm.

Finally, SAP has issued critical patches for multiple vulnerabilities across its NetWeaver and S/4HANA platforms. Among the most severe is CVE-2025-42944, a CVSS 10.0 deserialization flaw in the RMI-P4 module enabling unauthenticated remote code execution via malicious payloads sent to exposed ports. Additional vulnerabilities include CVE-2025-42922, which permits authenticated non-admin users to upload arbitrary files; CVE-2025-42958, which allows unauthorized access to sensitive IBM i-Series data due to missing authentication checks; and CVE-2025-42916, which lets privileged users delete S/4HANA database table contents. Although no exploitation has been observed in the wild, researchers urge organizations to apply patches immediately to prevent potentially devastating compromise.
