Daily Intelligence Update | 17 November 2025

Researchers are tracking the rapid expansion of a newly emerged ransomware operation known as Kawa4096, active since June 2025 and already impacting finance, education, and service-sector organizations, with most confirmed victims located in the United States and Japan. The group maintains a Tor-based leak site and follows a double-extortion model, with its retro console-style interface drawing comparisons to the Akira ransomware operation—leading analysts to assess the possibility of shared operators, borrowed tooling, or deliberate stylistic imitation. Examination of the malware shows a highly structured execution flow: when launched without parameters, it reinvokes itself using the -all argument, creates a mutex called SAY_HI_2025 to avoid multiple running instances, and loads embedded configuration data defining exclusion lists, restricted directories, filenames to skip, and processes to terminate. To accelerate encryption while still ensuring irreversible damage, the malware employs a partial chunk-based method encrypting roughly 25% of each 64 KB segment and appends a randomized nine-character string to altered files. Its ransom note, !!Restore-My-file-Kavva[.]txt, mirrors text associated with Qilin ransomware and provides both an onion service and a QTOX identifier for negotiation. Recovery efforts are further impeded by the malware's deletion of shadow copies via vssadmin and wmic commands executed using WMI.

As Kawa4096 operations continue to grow, another major development has unfolded with the takedown of the RaccoonO365 phishing-as-a-service ecosystem, which enabled widespread credential theft from Microsoft 365 users. Microsoft's Digital Crimes Unit, working with researchers across multiple organizations, executed a coordinated disruption effort that included seizing 338 domains tied to the operation under a U.S. court order, removing linked Worker scripts, and suspending associated accounts. Tracked by analysts as Storm-2246, RaccoonO365 sold subscription-based access to brand-spoofing phishing kits imitating Microsoft, SharePoint, DocuSign, and other commonly targeted platforms. The operation employed Cloudflare Turnstile and bot-screening techniques to restrict access to intended victims and is believed to have facilitated the theft of more than 5,000 Microsoft 365 credentials across 94 countries since 2024. Microsoft attributes the service to Joshua Ogundipe, reportedly based in Nigeria, who allegedly marketed the kit through Telegram and earned over $100,000 in cryptocurrency. Following the takedown, messages circulated within cybercriminal channels urging customers to migrate to new infrastructure, indicating attempts to rebuild the service elsewhere.

Alongside these disruptions, researchers have identified a financially motivated campaign attributed to Storm-2657, in which attackers compromise HR and payroll accounts to redirect employee salary payments into accounts they control. Targeting U.S.-based organizations primarily during early and mid-2025, the group focuses on SaaS platforms such as Workday but is assessed to pose risk to any payroll system containing banking or compensation data. Rather than exploiting software vulnerabilities, Storm-2657 relies on social-engineering methods—including phishing and adversary-in-the-middle techniques—to capture credentials and MFA codes, allowing them to infiltrate Exchange Online accounts and connected HR systems through single sign-on flows. Once inside, actors modify direct-deposit information, create inbox rules to suppress alerts, and enroll attacker-controlled phone numbers as MFA devices to maintain access. Investigators have confirmed compromises of eleven accounts across three U.S. universities since March 2025, which in turn were used to deliver nearly 6,000 phishing emails to individuals at twenty-five academic institutions. Lures often referenced illnesses or misconduct, exploiting urgency to increase engagement. Additional reporting, referring to the actor as Payroll Pirates, indicates targeting across government, insurance, and retail sectors. Analysts have identified more than 150 supporting domains, and some of the university-focused activity may also be intended to gather sensitive personal data for future fraud. Security teams recommend deploying phishing-resistant MFA, monitoring for unusual MFA registrations or inbox rule creation, and requiring secondary verification for any payroll or banking-related profile changes.

Amid these attack campaigns, researchers have disclosed a significant vulnerability affecting the Rust async-tar ecosystem, raising concerns over file-overwrite and remote code execution scenarios. The

flaw—tracked as CVE-2025-62518 and referred to as TARmageddon—was identified in August 2025 and affects async-tar along with several forks, including the widely integrated tokio-tar library. The vulnerability stems from improper handling of PAX extended headers in conjunction with ustar headers, allowing crafted TAR archives to embed nested entries that the parser misinterprets as legitimate files. This logic flaw enables overwriting of critical files within extraction paths, which under certain conditions could lead to arbitrary code execution, such as replacing configuration files, altering environment definitions, or hijacking build processes. Impacted projects include tools like testcontainers and wasmCloud, and maintainers have warned that tokio-tar, last updated in July 2023, is effectively unmaintained. Users are being advised to migrate to astral-tokio-tar, which has released version 0.5.6 to address the issue. According to developers, earlier versions incorrectly advanced stream offsets when handling PAX headers containing size overrides, enabling inner archive data to masquerade as valid top-level entries. Analysts note that a malicious package—such as one uploaded to PyPI—could exploit this behavior by embedding harmful files within nested TAR structures that overwrite legitimate metadata during installation, highlighting the broader supply-chain implications of the vulnerability.
