3 September 2025

Researchers uncovered a targeted supply chain compromise of the popular VS Code extension ETHcode, widely used by Ethereum developers. In June 2025, a malicious pull request from a throwaway GitHub account introduced a dependency named keythereum-utils, crafted to resemble a legitimate package. Hidden within were just two lines of obfuscated code that executed a PowerShell script to fetch a second-stage payload. The extension, with nearly 6,000 installs, was automatically updated for many users before being removed from the VS Code Marketplace. A clean release (0.5.1) followed in early July. Analysts emphasize the need for stronger vetting of contributors, dependency reviews, and automated detection of tampered packages to prevent similar incidents.

A separate discovery exposed Plague, a Linux backdoor embedded within malicious Pluggable Authentication Modules (PAM). Plague silently bypasses authentication, granting attackers undetected SSH persistence while erasing traces of activity. Despite variants appearing on VirusTotal for more than a year, the malware often evaded detection due to sophisticated anti-analysis measures, evolving obfuscation techniques, and session sanitization features. Researchers noted Plague unset environment variables, redirected shell history to /dev/null, and leveraged custom obfuscation routines resembling cryptographic generators. Analysts relied on custom IDA Pro plugins and Unicorn emulation to extract strings and memory offsets, revealing its stealth capabilities and long-term presence.

In East Asia, a newly identified campaign dubbed TAOTH leveraged abandoned infrastructure to deliver multi-stage espionage malware. Threat actors hijacked an outdated update server for the Sogou Zhuyin IME in October 2024 and paired it with spear-phishing operations to distribute tools including TOSHIS, DESFY, GTELAM, and C6DOOR. These tools collectively enabled shellcode loading, spyware data collection, and backdoor access via HTTP/WebSocket channels. Hundreds of victims have been confirmed across China, Taiwan, Hong Kong, Japan, and South Korea, with a focus on dissidents, journalists, researchers, and business executives. Analysts advise immediate removal of outdated Sogou software and enhanced validation of app permissions to mitigate similar supply chain compromises.

Political tensions also shaped the week's threat landscape. The Russian investment platform Investment Projects confirmed a cyberattack by pro-Ukraine group Cyber Anarchy Squad, which claimed to exfiltrate databases and employee files, later leaking samples online. The platform was forced offline but has since restored partial functionality, urging customers to reset credentials. The group, active since 2022, has previously employed tools such as Mimikatz and Revenge RAT in disruptive campaigns targeting Russian infrastructure.

Meanwhile, Zscaler confirmed a data breach tied to the ongoing Drift-Salesforce supply chain incident. Attackers exploited stolen OAuth tokens from the compromised Drift integration to access Salesforce, exfiltrating customer details including personal contact data, licensing information, and support case records. Zscaler stressed that its core products and infrastructure were unaffected but acknowledged exposure of customer data. The incident is attributed to UNC6395, which has targeted similar credentials across AWS, Snowflake, and Google Workspace. Both Salesforce and Google have temporarily disabled Drift integrations, while impacted organizations rotate tokens and strengthen authentication.

This week's findings illustrate the growing blend of supply chain abuse, stealthy persistence techniques, and politically driven disruption. Developer ecosystems, enterprise SaaS integrations, and legacy infrastructure remain particularly vulnerable, requiring defenders to prioritize code integrity checks,

authentication monitoring, and rigorous patch hygiene while preparing for adversaries who exploit both technical weaknesses and geopolitical opportunities.

Critical Start is a leading provider of Managed Detection and Response (MDR) services, combining AI acceleration with expert human validation to eliminate false positives, reduce alert noise, and deliver fast, reliable threat resolution.

With a US-based, 24/7/365 Security Operations Center and a 90% analyst retention rate, Critical Start delivers both proactive and reactive MDR for large enterprises across North America. Its MDR is built to 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.