

# Weekly Intelligence Summary

Report Date: 22.09.2025

Intelligence Cut-off Date: 19.09.2025

**Weekly Focus: Shai-Hulud campaign compromises 187 npm packages to harvest secrets and self-propagate**

**Researchers have uncovered a large-scale supply chain compromise, dubbed the Shai-Hulud campaign, which inserted malicious code into at least 187 npm packages, including the widely used @ctrl/tinycolor. The operation leveraged the npm ecosystem to harvest secrets and enable worm-like self-propagation across maintainer accounts.**

The campaign began by compromising maintainer accounts linked to @ctrl/tinycolor, before spreading to more than 180 other packages. Malicious versions deployed a bundle.js file that executed on installation, using TruffleHog to scan for API keys and cloud credentials and exfiltrating results via GitHub workflows. The malware also attempted to automatically republish trojanised packages under legitimate accounts, enabling rapid propagation and compounding the risk to downstream projects reliant on transitive dependencies.

This activity significantly increased the likelihood of credential exposure and collateral impact, even for trusted vendor namespaces. Although vendors confirmed no compromise of products despite affected packages, the incident shows how widespread infiltration of developer ecosystems can produce systemic risk. The Shai-Hulud campaign builds on a pattern of adversaries weaponising open-source supply chains, echoing earlier compromises of npm and Go modules as well as state-linked abuse of GitHub.

## Why It Matters...

The incident illustrates how adversaries are embedding themselves within trusted development platforms rather than relying on external spoofing, complicating attribution and prolonging dwell time. By exploiting the natural trust in npm packages, threat actors increase the chance of sensitive data exposure while undermining confidence in the integrity of open-source dependencies.

For organisations, the incident demonstrates that authentication or popularity alone cannot be relied upon as proof of legitimacy. Building resilience requires stronger protection of maintainer accounts, tighter governance of dependencies, and continuous monitoring of build environments. Supply chain security should evolve to integrate threat intelligence and developer awareness into everyday workflows, balancing the openness of developer ecosystems with safeguards capable of resisting sustained adversary exploitation.

## Intelligence Overview

### Education

The UK Information Commissioner's Office (ICO) has warned that students are responsible for the majority of school data breaches. The findings highlight the ongoing challenge for educational institutions in balancing digital accessibility with robust cyber hygiene.

In the United States, the Uvalde school district in Texas was forced to shut down critical systems following a ransomware attack, disrupting teaching operations and parent communications.

### Data breach

Fairmont Federal Credit Union disclosed that a 2023 data breach impacted 187,000 individuals, exposing sensitive financial and personal information linked to its members.

Luxury fashion group Kering confirmed a breach affecting customer data across its flagship brands, including Gucci, Balenciaga, and Alexander McQueen, raising concerns over the security of high-value retail customer information.

### Ransomware

Researchers have observed the emergence of Yurei ransomware, a strain built from publicly available open-source code that enables rapid adaptation and distribution by multiple threat actors.

The Everest ransomware group claimed a breach of BMW, stealing audit documents, and is threatening to leak them if ransom demands are not met.