

ChainVeil and ViteVenom are DPRK's PolinRider Campaign

By cb482791-4ef1-4762-96ad-b0ca4bdd538e

Published: 2026-07-17 · Archived: 2026-07-21 02:01:30 UTC

On June 16, 2026, Checkmarx Zero published [a detailed breakdown](#) of an npm supply chain campaign they named "ChainVeil." It's careful work: they pulled together nine malicious packages, a 77KB remote access trojan (RAT), a four-tier blockchain command channel spanning TRON, Aptos, and Binance Smart Chain. Four weeks later, on July 14, they followed up with [a sequel](#) on "ViteVenom," seven typosquats targeting the Vite ecosystem. They assessed with high confidence that it shares an operator with ChainVeil, while noting that "blockchain attribution carries inherent limitations" and that "a shared-infrastructure-as-a-service model cannot be ruled out."

When we read their analysis, blockchain components immediately reminded us of PolinRider. That specific combination of chains is a signature we've seen before: PolinRider pioneered cryptowallet multiplexing using exactly that mix.

PolinRider is a massively successful Lazarus Group (North Korean state-sponsored) campaign that emerged in early 2026. Initially it weaponized credentials stolen by [TasksJacker](#), and we consider it a parallel or sub-campaign to [Contagious Interview](#). We support this attribution through shared infrastructure and matching tradecraft. Since we first reported it in March, it's grown 6.5x and spread from GitHub into Go, Packagist, npm, and PyPI. We've attributed 4,295 malicious assets to this campaign, and extracted well over 10k IOCs.

The evidence for PolinRider attribution

We checked our dataset (publicly available in our [PolinRider dossier](#)). Both TRON wallets anchoring ChainVeil's command channel, the Aptos fallback address, and both XOR decryption keys are ones we published in our [March 8 report on PolinRider](#), 100 days before Checkmarx's ChainVeil report existed and 71 days before ChainVeil's first malicious npm package was published.

The overlap isn't approximate. Five values are byte-for-byte identical across both reports:

- XOR key 2[gWfGj;<:-93Z^C
- XOR key m6:tTh^D)cBz?NM]
- TRON wallet TMfKQEd7TJJJa5xNZJZ2Lep838vrzrs7mAP
- TRON wallet TXfxHUet9pJVU1BgVkBAbrES4YUc1nGzcG
- Aptos address 0xbe037400670fbf1c32364f762975908dc43eeb38759263e7dfcdabc76380811e

By the time Checkmarx captured it, the primary TRON wallet had been rotated 17 times, part of 17 distinct payload updates tracked back to June 2025, nearly a year before Checkmarx published. The secondary wallet had rotated once. That's a signal of a long-running, actively managed piece of infrastructure. The same wallets and

keys also anchor our [March 31 report on TasksJacker](#), the credential-harvesting operation we've already linked to PolinRider as its precursor phase.

Our conclusion, based on the shared infrastructure, is ChainVeil/ViteVenom aren't from a new threat actor or a unique campaign. It's PolinRider, running directly against the npm and Vite ecosystems. If you're tracking ChainVeil, ViteVenom, and PolinRider as separate entries, merging them gives you the full picture, and every wallet, marker, and package below feeds the same detection surface.



The pattern holds beyond the wallets, too. ChainVeil's IOC table shows an A6- prefix constant across every campaign marker: A6-519-81, A6-420, A6-317, A6-318. That prefix isn't unique to those nine packages. It's a

trend we discussed on Episode #10 of our podcast, where Paul McCarty talked about seeing the same pattern in DPRK-owned packages `tailwind-color-shades` (marker `a6-shadow-15`) and `secure-box` (marker `a6-orion-271`). A naming scheme that persists across packages and timeframes is an operator's signature.

The targeting also fits. ChainVeil's packages (`tailwindcss-merge`, `tailwindcss-animates-kit`, `clsx-tailwind`) and the packages we've attributed to PolinRider, including `tailwind-mainanimation`, published by the npm user "allavin" and documented in our March 8 report, use different names. They're not a shared IOC but they typosquat the same narrow slice of the Tailwind and Vite tooling namespace.

Summary of timeline and packages

Timeline

Date	Event
March 8, 2026	OpenSourceMalware publishes first PolinRider report with both TRON wallets, the Aptos address, and both XOR keys, attributed to DPRK/Lazarus
May 18, 2026	First two "ChainVeil" npm packages published
June 6-10, 2026	ChainVeil publication of seven npm packages
June 16, 2026	Checkmarx publishes ChainVeil report, names operator "SuccessKey," lists the same two TRON wallets, the same Aptos address, and the same two XOR keys
June 28-July 13, 2026	ViteVenom's seven packages published in this window
July 15, 2026	OpenSourceMalware publishes updated PolinRider report (4,367 repos total), noting the blockchain infrastructure is "unchanged from April"

Here's a chronological look at the typosquatted packages. While we've identified the malicious version(s) for each, it's important to note that these are DPRK-owned packages and versions should be considered malicious. Some are still live on npm as of the publishing of this article, while others have been removed entirely or replaced with 0.0.1-security placeholders.

Published	Package	Malicious versions	Maintainer	Campaign (Checkmarx)
May 18, 2026	tailwindcss-animatics	1.0.1	successkeyteck	ChainVeil
May 18, 2026	tailwindcss-animates-kit	1.0.1	successkeyteck	ChainVeil
Jun 6, 2026	tailwindcss-merge	1.0.1, 1.0.2, 1.0.3, 1.0.4	successkeyteck	ChainVeil
Jun 6, 2026	sass-formats	1.0.2, 1.0.3, 1.0.4, 1.0.5	successkeyteck	ChainVeil
Jun 6, 2026	clsx-tailwind	1.0.1	successkeyteck	ChainVeil
Jun 6, 2026	typeorm-encrypt	1.0.1	successkeyteck	ChainVeil
Jun 7, 2026	rate-limit-flexible	1.0.1, 1.0.2	successkeyteck	ChainVeil
Jun 9, 2026	sass-format	1.0.1	successkeyteck	ChainVeil
Jun 10, 2026	rate-limits-flexible	1.0.1	successkeyteck	ChainVeil
Jun 28, 2026	@vite-mcp/vite-type	6.44.1	vite-mcp	ViteVenom
Jun 28, 2026	@vite-pro/vite-ui	2.5.10	vite-pro	ViteVenom
Jun 28, 2026	@vitets/vite-ts	1.5.10	vitets	ViteVenom

Published	Package	Malicious versions	Maintainer	Campaign (Checkmarx)
Jun 28, 2026	@vite-ts/vite-ui	6.44.1	vite-ts	ViteVenom
Jul 8, 2026	@vite-tab/tab	3.15.10	vite-tab	ViteVenom
Jul 8, 2026	@vite-ln/build-ts	5.15.10	vite-ln	ViteVenom
Jul 13, 2026	@uw010010/vite-tree	3.4.2, 3.4.3, 3.6.1	uw010010	ViteVenom

We'll keep this record updated as the picture develops, and we'd welcome hearing from Checkmarx or anyone else who's mapped related infrastructure. More eyes on this dataset makes correlation easier for everyone defending against it.

Learn more

Source: <https://opensourcemalware.com/blog/chainveil-and-vitevenom-dprk-polinrider-campaign>