

The Worm That Keeps on Digging: TeamPCP Hits @antv in Latest Wave

✦ wiz.io/blog/mini-shai-hulud-teampcp-hits-antv-supply-chain

Rami McCarthy, Benjamin Read, Merav Bar

May 19, 2026



The ongoing software supply chain campaign targeting the open source ecosystem reemerged on May 19th, affecting NPM packages, GitHub Actions, and a VSCode extension. The distributed malware was designed to harvest credentials, exfiltrate sensitive data, and establish persistent access on infected systems.

As the activity unfolded publicly, Wiz Research independently observed related malicious activity in real time across developer and CI/CD environments.

Based on infrastructure analysis, malware behavior, and operational overlaps identified during the investigation, Wiz attributes this activity to the threat actor known as "[TeamPCP](#)".

What Happened

Researchers have dissected a coordinated software supply chain attack campaign affecting multiple components within the developer ecosystem, including npm packages (prominently those in the @antv namespace), GitHub Actions (e.g actions-cool/issues-helper) and a VSCode extension (nrwl.angular-console v18.95.0).

Upon installation of the npm packages, the malicious code initiated a multi-stage infection chain designed to retrieve additional payloads from GitHub-hosted infrastructure. In several cases, the payloads were stored in orphaned GitHub commits, likely as an attempt to evade detection and maintain operational resilience. The malware then used bun to install and execute secondary payloads responsible for credential theft and persistence.

The malware collected a wide range of sensitive artifacts from infected systems, including GitHub tokens, SSH keys, cloud credentials, browser-stored secrets, and other developer-related authentication material. Exfiltration occurred through attacker-created public GitHub repositories generated from the victim environment. Investigators observed repositories created with the description:

```
niagA oG eW ereH :duluH-iahS
```

In addition to credential theft, the malware established persistence by installing a Python-based backdoor at:

~/.local/share/kitty/cat.py

The backdoor periodically polled GitHub for signed command-and-control messages containing the string: firedalazer

When a valid signed instruction is identified, the malware retrieves and executes remote Python code from attacker-controlled infrastructure, effectively providing the operators with ongoing remote execution capabilities on compromised systems. To date, **this command and control infrastructure has not been observed active**.

Investigation into additional impacted packages and infrastructure remains ongoing.

Attribution

Wiz Research assesses with moderate confidence that this activity is associated with the threat actor known as "[TeamPCP](#)". The attribution is based on infrastructure overlaps, malware functionality, operational patterns, and tradecraft observed throughout the investigation.

While the investigation remains ongoing, the campaign demonstrates coordination and operational maturity consistent with previous activity linked to the group.

Indicators of Compromise

File Paths

~/.local/share/kitty/cat.py

GitHub Repository Description

niagA oG eW ereH :duluH-iahS

Command-and-Control Trigger

firedalazer

Network Indicators

Indicator	Role
api.github.com/search/commits?q=firedalazer	Backdoor polling to Github for commands
m-kosche.com (185.95.159.32)	Backup Malware C2

Host Indicators

File	Purpose	Hash
Backdoor	Stored at ~/.local/share/kitty/cat.py`	MD5: b06b126b9e26af03a7ef2f8b8e90d446 Sha-1: 783b4019fc5b942a29846132d28441c8fc31bed8 SHA256: fb5c97557230a27460fdab01fafcfabeaa49590bafd5b6ef30501aa9e0a51142,
persistence	macOS ~/Library/LaunchAgents/com.user.kitty-monitor.plist Linux ~/config/systemd/user/kitty-monitor.service	

What Steps Should Security Teams Take

- Organizations should immediately investigate developer workstations, CI/CD environments, and repositories for signs of compromise. Teams should audit systems for the affected packages, GitHub Actions, and VSCode extensions, while also reviewing GitHub activity for unauthorized repositories, newly created access tokens, or suspicious workflow executions.
- Because the malware targets developer credentials and secrets, organizations should assume potential exposure of GitHub tokens, SSH keys, cloud credentials, and CI/CD secrets, and rotate them accordingly.
- Security teams should also hunt for persistence mechanisms and unusual outbound GitHub communication, including the presence of the following file: `~/.local/share/kitty/cat.py/`
- Finally, organizations should strengthen software supply chain defenses by implementing dependency allowlisting, SBOM generation, package verification, and improved monitoring of developer and build environments.

How Wiz Can Help

Wiz customers can use [the pre-built queries and advisory](#) in the [Wiz Threat Intel Center](#) to search for relevant instances in their environment. Wiz Research will continue to update that advisory as the situation develops.

References

- [nrwl impact report](#)
- [Original GitHub Thread](#)
- [StepSecurity Blog on VSCode](#)
- [StepSecurity Blog on GitHub Actions](#)
- [Socket Blog on Overall Compromises](#)

Appendix

Affected GitHub Actions

Column A	Column B
Name	Affected Versions
actions-cool/maintain-one-comment	All tags for a limited time
actions-cool/issues-helper	All tags for a limited time

Compromised VSCode Extension

Column A	Column B
Name	Affected Version
nrwl.angular-console	18.95.0

Malicious NPM Packages

Column A	Column B
Package	Affected Versions
@antv/a8	0.1.1, 0.2.1
@antv/adjust	0.3.5, 0.4.5
@antv/algorithm	0.2.26, 0.3.26
@antv/async-hook	2.3.9, 2.4.9
@antv/attr	0.4.5, 0.5.5
@antv/ava	3.5.1, 3.6.1
@antv/ava-react	3.4.2, 3.5.2
@antv/awards	0.1.9, 0.2.9
@antv/calendar-heatmap	1.2.2, 1.3.2
@antv/chart-linter	1.2.6, 1.3.6
@antv/chart-node-g6	0.1.4, 0.2.4
@antv/chart-visualization-skills	0.2.3, 0.3.3
@antv/ckb	2.1.4, 2.2.4
@antv/color-schema	0.3.3, 0.4.3
@antv/color-util	2.1.6, 2.2.6
@antv/component	2.2.11, 2.3.11
@antv/coord	0.5.7, 0.6.7
@antv/d3-color	1.1.0, 1.2.0
@antv/d3-interpolate	1.1.3, 1.2.3
@antv/data-samples	1.1.1, 1.2.1
@antv/data-set	0.12.8, 0.13.8
@antv/data-wizard	2.1.4, 2.2.4
@antv/dipper-component	0.1.4, 0.2.4
@antv/dipper-hooks	0.3.1, 0.4.1
@antv/dipper-map	1.1.10, 1.2.10
@antv/dom-util	2.1.4, 2.2.4
@antv/dumi-theme-antv	0.9.4, 0.10.4

Column A	Column B
@antv/dw-analyzer	1.2.5, 1.3.5
@antv/dw-random	1.2.7, 1.3.7
@antv/dw-transform	1.2.7, 1.3.7
@antv/dw-util	1.2.4, 1.3.4
@antv/event-emitter	0.2.3, 0.3.3
@antv/expr	1.1.2, 1.2.2
@antv/f-charts	0.1.0, 0.2.0
@antv/f-engine	1.11.0, 1.12.0
@antv/f-lottie	1.11.0, 1.12.0
@antv/f-my	1.11.0, 1.12.0
@antv/f-react	1.11.0, 1.12.0
@antv/f-test-utils	1.1.9, 1.2.9
@antv/f-vue	1.11.0, 1.12.0
@antv/f-wx	1.11.0, 1.12.0
@antv/f2	5.15.0, 5.16.0
@antv/f2-algorithm	5.8.0, 5.9.0
@antv/f2-canvas	1.1.5, 1.2.5
@antv/f2-context	0.1.1, 0.2.1
@antv/f2-graphic	0.1.16, 0.2.16
@antv/f2-my	4.1.52, 4.2.52
@antv/f2-react	5.15.0, 5.16.0
@antv/f2-site	4.1.42, 4.2.42
@antv/f2-vue	4.1.33, 4.2.33
@antv/f2-wordcloud	5.15.0, 5.16.0
@antv/f2-wx	4.1.51, 4.2.51
@antv/f6	0.1.19, 0.2.19
@antv/f6-alipay	0.1.7, 0.2.7
@antv/f6-core	0.1.2, 0.2.2
@antv/f6-element	0.1.1, 0.2.1

Column A	Column B
@antv/f6-hammerjs	0.1.2, 0.2.2
@antv/f6-plugin	1.1.6, 1.2.6
@antv/f6-ui	1.1.3, 1.2.3
@antv/f6-wx	0.1.7, 0.2.7
@antv/g	6.4.1, 6.5.1
@antv/g-base	0.6.16, 0.7.16
@antv/g-camera-api	2.1.45, 2.2.45
@antv/g-canvas	2.3.0, 2.4.0
@antv/g-canvaskit	1.2.1, 1.3.1
@antv/g-compatible	1.1.11, 1.2.11
@antv/g-components	2.1.42, 2.2.42
@antv/g-css-layout-api	1.1.38, 1.2.38
@antv/g-css-typed-om-api	1.1.38, 1.2.38
@antv/g-device-api	1.7.13, 1.8.13
@antv/g-dom-mutation-observer-api	2.1.42, 2.2.42
@antv/g-gesture	3.1.42, 3.2.42
@antv/g-image-exporter	1.1.42, 1.2.42
@antv/g-layout-blocklike	1.8.49, 1.9.49
@antv/g-lite	2.8.0, 2.9.0
@antv/g-lottie-player	1.2.1, 1.3.1
@antv/g-math	3.2.0, 3.3.0
@antv/g-mobile	1.2.5, 1.3.5
@antv/g-mobile-canvas	1.2.1, 1.3.1
@antv/g-mobile-canvas-element	1.1.42, 1.2.42
@antv/g-mobile-svg	1.2.1, 1.3.1
@antv/g-mobile-webgl	1.2.1, 1.3.1
@antv/g-pattern	2.1.42, 2.2.42
@antv/g-perf	1.1.0, 1.2.0
@antv/g-plugin-3d	2.2.1, 2.3.1

Column A	Column B
@antv/g-plugin-a11y	1.5.1, 1.6.1
@antv/g-plugin-annotation	1.3.0, 1.4.0
@antv/g-plugin-box2d	2.2.1, 2.3.1
@antv/g-plugin-canvas-path-generator	2.2.26, 2.3.26
@antv/g-plugin-canvas-picker	2.4.1, 2.5.1
@antv/g-plugin-canvas-renderer	2.6.1, 2.7.1
@antv/g-plugin-canvaskit-renderer	2.4.1, 2.5.1
@antv/g-plugin-control	2.2.1, 2.3.1
@antv/g-plugin-css-select	2.2.1, 2.3.1
@antv/g-plugin-device-renderer	2.7.1, 2.8.1
@antv/g-plugin-dom-interaction	2.2.31, 2.3.31
@antv/g-plugin-dragndrop	2.2.1, 2.3.1
@antv/g-plugin-gesture	2.2.1, 2.3.1
@antv/g-plugin-gpgpu	1.10.20, 1.11.20
@antv/g-plugin-html-renderer	2.4.1, 2.5.1
@antv/g-plugin-image-loader	2.4.1, 2.5.1
@antv/g-plugin-matterjs	2.2.1, 2.3.1
@antv/g-plugin-mobile-interaction	1.1.42, 1.2.42
@antv/g-plugin-physics	2.2.1, 2.3.1
@antv/g-plugin-rough-canvas-renderer	2.2.1, 2.3.1
@antv/g-plugin-rough-svg-renderer	2.2.1, 2.3.1
@antv/g-plugin-svg-picker	2.1.46, 2.2.46
@antv/g-plugin-svg-renderer	2.5.1, 2.6.1
@antv/g-plugin-webgl-device	1.10.17, 1.11.17
@antv/g-plugin-webgl-renderer	1.1.26, 1.2.26
@antv/g-plugin-webgpu-device	1.10.17, 1.11.17
@antv/g-plugin-yoga	2.4.1, 2.5.1
@antv/g-plugin-zdog-canvas-renderer	2.2.1, 2.3.1
@antv/g-plugin-zdog-svg-renderer	2.2.1, 2.3.1

Column A	Column B
@antv/g-shader-components	2.1.0, 2.2.0
@antv/g-svg	2.2.1, 2.3.1
@antv/g-web-animations-api	2.2.32, 2.3.32
@antv/g-web-components	2.2.1, 2.3.1
@antv/g-webgl	2.2.1, 2.3.1
@antv/g-webgl-compute	0.1.1, 0.2.1
@antv/g-webgpu	2.2.1, 2.3.1
@antv/g-webgpu-compiler	0.8.2, 0.9.2
@antv/g-webgpu-core	0.8.2, 0.9.2
@antv/g-webgpu-engine	0.8.2, 0.9.2
@antv/g-webgpu-raytracer	0.6.1, 0.7.1
@antv/g-webgpu-unitchart	0.6.1, 0.7.1
@antv/g2	5.5.8, 5.6.8
@antv/g2-brush	0.1.2, 0.2.2
@antv/g2-extension-3d	0.3.0, 0.4.0
@antv/g2-extension-ava	0.3.0, 0.4.0
@antv/g2-extension-plot	0.3.2, 0.4.2
@antv/g2-plugin-slider	2.2.1, 2.3.1
@antv/g2-ssr	0.3.0, 0.4.0
@antv/g2plot	2.5.35, 2.6.35
@antv/g2plot-schemas	1.3.2, 1.4.2
@antv/g6	5.2.1, 5.3.1
@antv/g6-alipay	0.1.1, 0.2.1
@antv/g6-cli	0.1.4, 0.2.4
@antv/g6-core	0.9.24, 0.10.24
@antv/g6-editor	1.3.0, 1.4.0
@antv/g6-element	0.9.25, 0.10.25
@antv/g6-extension-3d	0.2.23, 0.3.23
@antv/g6-extension-react	0.3.7, 0.4.7

Column A	Column B
@antv/g6-mobile	0.2.2, 0.3.2
@antv/g6-pc	0.9.25, 0.10.25
@antv/g6-plugin	0.9.25, 0.10.25
@antv/g6-plugin-map-view	0.1.4, 0.2.4
@antv/g6-plugins	1.1.9, 1.2.9
@antv/g6-react-node	1.5.8, 1.6.8
@antv/g6-ssr	0.2.1, 0.3.1
@antv/g6-wx	0.1.1, 0.2.1
@antv/gatsby-theme	0.2.0, 0.3.0
@antv/geo-coord	1.1.8, 1.2.8
@antv/gi-assets-advance	2.6.22, 2.7.22
@antv/gi-assets-algorithm	2.4.19, 2.5.19
@antv/gi-assets-basic	2.5.40, 2.6.40
@antv/gi-assets-galaxybase	1.3.15, 1.4.15
@antv/gi-assets-graphscope	2.2.15, 2.3.15
@antv/gi-assets-hugegraph	1.2.15, 1.3.15
@antv/gi-assets-janusgraph	1.2.15, 1.3.15
@antv/gi-assets-neo4j	2.2.15, 2.3.15
@antv/gi-assets-scene	2.3.21, 2.4.21
@antv/gi-assets-tugraph	2.2.15, 2.3.15
@antv/gi-assets-tugraph-analytics	0.3.15, 0.4.15
@antv/gi-assets-xlab	0.2.30, 0.3.30
@antv/gi-cli	1.3.11, 1.4.11
@antv/gi-common-components	1.4.16, 1.5.16
@antv/gi-mock-data	1.1.5, 1.2.5
@antv/gi-public-data	1.1.1, 1.2.1
@antv/gi-sdk	3.1.0, 3.2.0
@antv/gi-sdk-app	1.3.10, 1.4.10
@antv/gi-theme-antd	0.7.11, 0.8.11

Column A	Column B
@antv/github-config-cli	0.2.0, 0.3.0
@antv/gl-matrix	2.8.1, 2.9.1
@antv/gpt-vis	1.1.0, 1.2.0
@antv/gpt-vis-ssr	0.4.7, 0.5.7
@antv/graphin	3.1.5, 3.2.5
@antv/graphin-components	2.5.1, 2.6.1
@antv/graphin-graphscope	1.1.5, 1.2.5
@antv/graphin-icons	1.1.0, 1.2.0
@antv/graphlib	2.1.4, 2.2.4
@antv/hierarchy	0.8.1, 0.9.1
@antv/infographic	0.3.19, 0.4.19
@antv/insight-component	1.1.0, 1.2.0
@antv/interaction	0.2.5, 0.3.5
@antv/istanbul	0.1.0, 0.2.0
@antv/knowledge	1.2.4, 1.3.4
@antv/l7	2.26.10, 2.27.10
@antv/l7-component	2.26.10, 2.27.10
@antv/l7-composite-layers	0.18.1, 0.19.1
@antv/l7-core	2.26.10, 2.27.10
@antv/l7-district	2.4.12, 2.5.12
@antv/l7-draw	3.2.5, 3.3.5
@antv/l7-editor	1.2.13, 1.3.13
@antv/l7-extension-g-layer	1.1.0, 1.2.0
@antv/l7-layers	2.26.10, 2.27.10
@antv/l7-leaflet	1.1.2, 1.2.2
@antv/l7-map	2.26.10, 2.27.10
@antv/l7-mapkit	0.6.0, 0.7.0
@antv/l7-maps	2.26.10, 2.27.10
@antv/l7-mini	2.21.8, 2.22.8

Column A	Column B
@antv/l7-pass	1.1.0, 1.2.0
@antv/l7-react	2.5.3, 2.6.3
@antv/l7-renderer	2.26.10, 2.27.10
@antv/l7-scene	2.26.10, 2.27.10
@antv/l7-source	2.26.10, 2.27.10
@antv/l7-three	2.26.10, 2.27.10
@antv/l7-utils	2.26.10, 2.27.10
@antv/l7plot	0.6.11, 0.7.11
@antv/l7plot-component	0.1.11, 0.2.11
@antv/larkmap	1.6.1, 1.7.1
@antv/layout-gpu	1.2.7, 1.3.7
@antv/layout-wasm	1.5.2, 1.6.2
@antv/li-aiearth-assets	0.5.7, 0.6.7
@antv/li-analysis-assets	1.10.1, 1.11.1
@antv/li-core-assets	1.4.7, 1.5.7
@antv/li-editor	1.7.1, 1.8.1
@antv/li-p2	1.9.2, 1.10.2
@antv/li-sam-assets	0.2.4, 0.3.4
@antv/li-sdk	1.6.1, 1.7.1
@antv/lite-insight	2.2.1, 2.3.1
@antv/matrix-util	3.1.4, 3.2.4
@antv/mcp-server-antv	0.2.8, 0.3.8
@antv/mcp-server-chart	0.10.10, 0.11.10
@antv/my-f2	2.2.7, 2.3.7
@antv/my-f2-pc	0.2.1, 0.3.1
@antv/narrative-text-editor	0.3.20, 0.4.20
@antv/narrative-text-schema	0.4.7, 0.5.7
@antv/narrative-text-vis	0.4.16, 0.5.16
@antv/path-util	3.1.1, 3.2.1

Column A	Column B
@antv/react-g	2.2.1, 2.3.1
@antv/s2	2.8.1, 2.9.1
@antv/s2-react	2.4.1, 2.5.1
@antv/s2-react-components	2.2.2, 2.3.2
@antv/s2-ssr	0.2.1, 0.3.1
@antv/s2-vue	2.3.0, 2.4.0
@antv/sam	0.3.0, 0.4.0
@antv/scale	0.6.2, 0.7.2
@antv/semantic-release-pnpm	1.1.4, 1.2.4
@antv/smart-color	0.3.1, 0.4.1
@antv/stat	0.1.2, 0.2.2
@antv/t8	0.4.0, 0.5.0
@antv/thumbnails	2.1.0, 2.2.0
@antv/thumbnails-component	2.1.0, 2.2.0
@antv/torch	1.1.6, 1.2.6
@antv/translator	1.1.1, 1.2.1
@antv/util	3.4.11, 3.5.11
@antv/vendor	1.1.11, 1.2.11
@antv/vis-predict-engine	0.2.1, 0.3.1
@antv/webgpu-graph	1.1.0, 1.2.0
@antv/word-scale-chart	0.4.4, 0.5.4
@antv/wx-f2	2.2.1, 2.3.1
@antv/x6	3.2.7, 3.3.7
@antv/x6-angular-shape	3.1.1, 3.2.1
@antv/x6-common	2.1.17, 2.2.17
@antv/x6-components	0.11.7, 0.12.7
@antv/x6-geometry	2.1.5, 2.2.5
@antv/x6-plugin-clipboard	2.2.6, 2.3.6
@antv/x6-plugin-dnd	2.2.1, 2.3.1

Column A	Column B
@antv/x6-plugin-export	2.2.6, 2.3.6
@antv/x6-plugin-history	2.3.4, 2.4.4
@antv/x6-plugin-keyboard	2.3.3, 2.4.3
@antv/x6-plugin-minimap	2.1.7, 2.2.7
@antv/x6-plugin-scroller	2.1.10, 2.2.10
@antv/x6-plugin-selection	2.3.2, 2.4.2
@antv/x6-plugin-snapline	2.2.7, 2.3.7
@antv/x6-plugin-stencil	2.2.5, 2.3.5
@antv/x6-plugin-transform	2.2.8, 2.3.8
@antv/x6-react	0.2.26, 0.3.26
@antv/x6-react-components	2.1.9, 2.2.9
@antv/x6-react-shape	3.1.1, 3.2.1
@antv/x6-vector	1.5.2, 1.6.2
@antv/x6-vue-shape	3.1.2, 3.2.2
@antv/x6-vue3-shape	1.1.0, 1.2.0
@antv/xflow	2.2.13, 2.3.13
@antv/xflow-core	1.1.55, 1.2.55
@antv/xflow-diff	1.1.0, 1.2.0
@antv/xflow-extension	1.1.55, 1.2.55
@antv/xflow-hook	1.1.55, 1.2.55
@lint-md/cli	2.1.0, 2.2.0
@lint-md/core	2.1.0, 2.2.0
@lint-md/parser	0.1.14, 0.2.14
@openclaw-cn/cli	1.4.1
@openclaw-cn/feishu	0.2.11
@openclaw-cn/libsignal	2.1.1
@openclaw-cn/toutiao-ops	1.2.4
@starmind/collector-cli	0.3.10
ai-figure	0.5.0, 0.6.0

Column A	Column B
amapcn	0.2.2, 0.3.2
ast-plugin	0.1.7, 0.2.7
babel-plugin-version	0.3.3, 0.4.3
boring-avatars-vanilla	1.1.2, 1.2.2
byte-parser	1.1.0, 1.2.0
canvas-nest.js	2.1.4, 2.2.4
echarts-for-react	3.1.7, 3.2.7
filesize.js	2.1.0, 2.2.0
fixed-round	1.1.2, 1.2.2
ganttt-for-react	0.3.0, 0.4.0
jest-canvas-mock	2.6.3, 2.7.3
jest-date-mock	1.1.11, 1.2.11
jest-electron	0.2.12, 0.3.12
jest-expect	0.1.1, 0.2.1
jest-less-loader	0.3.0, 0.4.0
jest-random-mock	1.1.0, 1.2.0
jest-url-loader	0.2.0, 0.3.0
limit-size	0.2.4, 0.3.4
lint-md	0.3.0, 0.4.0
lint-md-cli	0.2.2, 0.3.2
mcp-echarts	0.8.1, 0.9.1
mcp-mermaid	0.5.1, 0.6.1
miz	1.1.1, 1.2.1
nrwl.angular-console	18.95.0
onfire.js	2.1.1, 2.2.1
openclaw-cn	0.3.0
react-adsense	0.2.0, 0.3.0
relationship.js	1.3.9, 1.4.9
ribbon.js	1.1.2

Column A	Column B
size-sensor	1.1.4, 1.2.4
slice.js	1.2.1, 1.3.1
timeago-react	3.1.7, 3.2.7
timeago.js	4.1.2, 4.2.2
uri-parse	1.1.0, 1.2.0
word-width	1.1.1, 1.2.1
xmorse	1.1.0, 1.2.0

Tags

[#Research](#)