Malicious Packages Hidden in NPM | FortiGuard Labs

By Jin Lee, Jenna Wang

Published: 2023-10-02 · Archived: 2026-04-05 21:08:04 UTC

Affected platforms: All platforms where NPM packages can be installed
Impacted parties: Any individuals or institutions that have these malicious packages installed
Impact: Leak of credentials, sensitive information, source code, etc.
Severity level: High

Over the past few months, the FortiGuard Labs team has discovered several malicious packages hidden in NPM (Node Package Manager), the largest software registry for the JavaScript programming language. These packages were found through a system dedicated to discover malicious open-source packages from various ecosystems e.g. PyPI, NPM. In this blog, we will look at some of these packages, grouping them based on similar styles of code or functions.

In general, most of these malicious packages use install scripts that run pre or post-install. Whenever an NPM package is installed, those scripts are run as well. An example of this is shown below.

Every package we found aims to steal sensitive data, such as system or user information, via a webhook or file-sharing link. Let’s explore the sets of packages below.

The First Set:

- @expue/webpack (version 0.0.3-alpha.0)
- @expue/core (version 0.0.3-alpha.0)
- @expue/vue3-renderer (version 0.0.3-alpha.0)
- @fixedwidthtable/fixedwidthtable (version 0.0.2)
- @virtualsearchtable/virtualsearchtable (version 0.1.1)

This first set shows an obfuscated index.js script. However, we can identify some clues in the strings that may raise suspicions. Let’s try to simplify this code.

After cleaning up the script, we can see it exfiltrates sensitive data, including Kubernetes configurations, SSH keys, and other critical information. It also gathers basic system fingerprinting details, like username, IP address, and hostname, without any prior warning.

The Second Set:

- **binarium-crm** (versions 1.0.0, 1.0.9, 1.9.9)
- **career-service-client-0.1.6** (versions 0.1.6, 0.1.13, 0.1.15)
- **hh-dep-monitoring** (versions 0.1.5, 0.1.14)
- **orbitplate** (versions 1.0.4, 1.0.6)

The index.js in this second set of packages sends an HTTP GET request to a specific URL, including query parameters. It scans for particular files and directories that may contain sensitive information. This script also enables the unauthorized extraction of critical developer data, including source code and configuration files. The targeted files and directories may contain highly valuable intellectual property and sensitive information, such as various application and service credentials. It then archives these files and directories and uploads the resulting archives to an FTP server.

The Third Set:

- @zola-helpers/client (versions 1.0.1, 1.0.2, 1.0.3)
- suncorp-styleguide-base (versions 1.0.3, 1.0.4, 1.0.5)

In this set, the index.mjs install script uses a Discord webhook to exfiltrate sensitive data, such as system information, username, and folder contents.

The Fourth Set:

- @next-translate-root/i18n (versions 1.0.1, 1.0.2)
- @ag-grid-react/lib (version 1.0.1)
- @next-translate-root/locales (versions 1.0.0, 1.0.1, 1.0.2)

As with the third set, this fourth set also uses an index.mjs install script and a Discord webhook to exfiltrate sensitive data. But this time, they use an alternate style of coding.

The Fifth Set:

- @dtx-company/flowcode-generator-types (version 200000.0.2)

This fifth set uses an index.js install script to exfiltrate host and username info and home users' home directory contents via a webhook.

The Sixth Set:

- squarespace-abtest (version 1.0.1)
- ruamel.taml.clib (version 0.1.2)
- regily (version 1.0.0)
- developer-scaffold-full-width-wrapper (versions 1.9.9, 21.0.9)
- @abb-americas/angular-utilities (version 1.0.0)
- @abb-americas/image-scaler (version 1.0.0)
- @abdulmz/mz-test (version 1.1.1)
- @ikea-aoa/component-financial-services (version 99.0.1)
- @ikea-aoa/component-lightbox (version 99.0.1)
- @ikea-aoa/component-popover (version 99.0.0)

This set—the most commonly found style—uses yet another index.js install script to exfiltrate information.

The Seventh Set:

- @cima/prism-utils (versions 23.2.1, 23.2.2)

In this set, the packages use an installer.js install script to carry out the attack, similar to the previous two, but we can see that the environment variable 'NODE_TLS_REJECT_UNAUTHORIZED' is set to '0'. This disables TLS certificate validation, which may make the connection insecure and vulnerable to man-in-the-middle attacks.

The Eighth Set:

- discorddd.jss (versions 1.4.9, 1.5.0, 1.6.4)
- saaaaaaaaaaaaaaaaaaaaa (version 1.4.1)

This package automatically downloads and executes a potentially malicious executable file from a URL to a C:/ directory.

The Ninth Set:

- evernote-thrift (version 1.9.99)
- en-features-rollout (version 1.90.9)
- en-conduit-electron (version 1.90.9)
- en-conduit-electron-auth (version 1.90.9)
- en-conduit-electron-worker (version1.90.9)
- en-thrift-internal (version 2.30.9)
- en-conduit-electron-renderer (version 1.90.9)

This package uses another script style to gather system information, including the victim's public IP address and then exfiltrates this information to a discord webhook.

Conclusion

This blog groups together a collection of malicious NPM packages that use install scripts to steal users' sensitive info based on styles of code or functions. End users should watch for packages that employ suspicious install scripts and exercise caution. We will continue hunting for and reporting malicious packages to help users avoid becoming victims.

Fortinet Protections

Fortiguard AntiVirus detects the malicious files identified in this report as

@zola-helpers/client-1.0.1 index.mjs: JS/WebHook.CNYS!tr
@zola-helpers/client-1.0.2 index.mjs: JS/WebHook.CNYS!tr
@zola-helpers/client-1.0.3 index.mjs: JS/WebHook.CNYS!tr
@next-translate-root/i18n-1.0.1 index.mjs: JS/WebHook.CNYS!tr
@next-translate-root/i18n-1.0.2 index.mjs: JS/WebHook.CNYS!tr

suncorp-styleguide-base-1.0.3 index.mjs: JS/WebHook.CNYS!tr
suncorp-styleguide-base-1.0.4 index.mjs: JS/WebHook.CNYS!tr
suncorp-styleguide-base-1.0.5 index.mjs: JS/WebHook.CNYS!tr
@ag-grid-react/lib-1.0.1 index.mjs: JS/WebHook.CNYS!tr
@next-translate-root/locales-1.0.0 index.mjs: JS/WebHook.CNYS!tr
@next-translate-root/locales-1.0.1 index.mjs: JS/WebHook.CNYS!tr
@next-translate-root/locales-1.0.2 index.mjs: JS/WebHook.CNYS!tr
@dtx-company/flowcode-generator-types-200000.0.2 index.js: JS/Agent.OAST!tr
squarespace-abtest-1.0.1 index.js: JS/Agent.OAST!tr
ruamel.taml.clib-0.1.2 index.js: JS/Agent.OAST!tr
regily-1.0.0 index.js: JS/Agent.OAST!tr
developer-scaffold-full-width-wrapper-1.9.9 index.js: JS/Agent.OAST!tr
developer-scaffold-full-width-wrapper-21.0.9 index.js: JS/Agent.OAST!tr
@abb-americas/angular-utilities-1.0.0 index.js: JS/Agent.OAST!tr
@abb-americas/image-scaler-1.0.0 index.js: JS/Agent.OAST!tr
@abdulmz/mz-test-1.1.1 index.js: JS/Agent.OAST!tr
@ikea-aoa/component-financial-services index.js: JS/Agent.OAST!tr
@ikea-aoa/component-lightbox-99.0.1 index.js: JS/Agent.OAST!tr
@ikea-aoa/component-popover-99.0.0 index.js: JS/Agent.OAST!tr
@cima/prism-utils-23.2.1 installer.js: JS/Agent.OAST!tr.dldr
@cima/prism-utils-23.2.2 installer.js: JS/Agent.OAST!tr.dldr
discorddd.jss-1.4.9 index.js: JS/Agent.CDPC!tr.dldr
discorddd.jss-1.5.0 index.js: JS/Agent.CDPC!tr.dldr
discorddd.jss-1.6.4 index.js: JS/Agent.CDPC!tr.dldr
saaaaaaaaaaaaaaaaaaaaaa-1.4.2 index.js: JS/Agent.CDPC!tr.dldr
evernote-thrift-1.9.99 index.js: JS/WebHook.ESY!tr
en-features-rollout-1.90.9 index.js: JS/WebHook.ESY!tr
en-conduit-electron-1.90.9 index.js: JS/WebHook.ESY!tr
en-conduit-electron-auth-1.90.9 index.js: JS/WebHook.ESY!tr
en-conduit-electron-worker-1.90.9 index.js: JS/WebHook.ESY!tr
en-thrift-internal-2.30.9 index.js: JS/WebHook.ESY!tr
en-conduit-electron-renderer-1.90.9 index.js: JS/WebHook.ESY!tr
@expue/webpack-0.0.3-alpha.0 index.js: JS/Agent.ATTC!tr
@expue/core-0.0.3-alpha.0 index.js: JS/Agent.ATTC!tr
@expue/vue3-renderer-0.0.3-alpha.0 index.js: JS/Agent.ATTC!tr
@fixedwidthtable/fixedwidthtable-0.0.2 index.js: JS/Agent.ATTC!tr
@virtualsearchtable/virtualsearchtable-0.1.1 index.js: JS/Agent.ATTC!tr
binarium-crm 1.0.0 index.js: JS/Agent.CFRE!tr.dldr
binarium-crm 1.0.9 index.js: JS/Agent.CFRE!tr.dldr
binarium-crm 1.9.9 index.js: JS/Agent.CFRE!tr.dldr
career-service-client-0.1.6 index.js: JS/Agent.CFRE!tr.dldr
career-service-client-0.1.13 index.js: JS/Agent.CFRE!tr.dldr

career-service-client-0.1.15 index.js: JS/Agent.CFRE!tr.dldr
hh-dep-monitoring-0.1.5 index.js: JS/Agent.CFRE!tr.dldr
hh-dep-monitoring-0.1.14 index.js: JS/Agent.CFRE!tr.dldr
orbitplate-1.0.4 index.js: JS/Agent.CFRE!tr.dldr
orbitplate-1.0.6 index.js: JS/Agent.CFRE!tr.dldr

The FortiGuard AntiVirus service is supported by FortiGate, FortiMail, FortiClient, and FortiEDR. Customers running current AntiVirus updates are protected.

The FortiGuard Web Filtering Service detects and blocks the download URLs cited in this report as Malicious.

The FortiDevSec SCA scanner detects malicious packages, including those cited in this report that may operate as dependencies in users' projects in test phases, and prevents those dependencies from being introduced into users' products.

If you believe these or any other cybersecurity threat has impacted your organization, please contact our Global FortiGuard Incident Response Team.

IOCs

@zola-helpers/client-1.0.1 index.mjs

MD5: e905c2915762e6c1fa57ff3b444411da

@zola-helpers/client-1.0.2 index.mjs

MD5: 1e5a38b17453379af9107a9afce0963f

@zola-helpers/client-1.0.3 index.mjs

MD5: c7325f2347833eba9869926226027330

@next-translate-root/i18n-1.0.1 index.mjs

MD5: cb37bd25c3011ffdd10c0db976c77b45

@next-translate-root/i18n-1.0.2 index.mjs

MD5: c4bf513d91909de6d8c8e28fe317950a

suncorp-styleguide-base-1.0.3 index.mjs

MD5: 404c75ee8c8a2241e94773a5f46cd372

suncorp-styleguide-base-1.0.4 index.mjs

MD5: 0b4da6e4a3d7f0d43afc1ce5a567aeed

suncorp-styleguide-base-1.0.5 index.mjs

MD5: fbf108d9534e2a065ba62198d7ab226c

@ag-grid-react/lib-1.0.1 index.mjs

MD5: 42d7f4f9e4d837c5f1217165e92d0136

@next-translate-root/locales-1.0.0 index.mjs

MD5: 312368807bee4e8876acec4dba528f13

@next-translate-root/locales-1.0.1 index.mjs

MD5: cb37bd25c3011ffdd10c0db976c77b45

@next-translate-root/locales-1.0.2 index.mjs

MD5: c4bf513d91909de6d8c8e28fe317950a

@dtx-company/flowcode-generator-types-200000.0.2 index.js

MD5: 1b80da13c2d440b51de3e3b1f84b30b6

squarespace-abtest-1.0.1 index.js

MD5: 0976fc4401a315d8182828d07b0e4a02

ruamel.taml.clib-0.1.2 index.js

MD5: 489af9e516d133f8341bc50068b3a505

regily-1.0.0 index.js

MD5: 8333f68439addfe5d80d7cf8646d74f6

developer-scaffold-full-width-wrapper-1.9.9 index.js

MD5: c627ce5ec695ea663b88a09fb31ea319

developer-scaffold-full-width-wrapper-21.0.9 index.js

MD5: 563cf757e5f61a592f53506c81360e4a

@abb-americas/angular-utilities-1.0.0 index.js

MD5: 2965d88976fee79d1e3ef69e5edc5d83

@abb-americas/image-scaler-1.0.0 index.js

MD5: 0876c5969dc829f2f56b455ae38a2536

@abdulmz/mz-test-1.1.1 index.js

MD5: ecd47a29a7e5132f94b1c7c0689e2e5a

@ikea-aoa/component-financial-services-99.0.1 index.js

MD5: 025809495e179b4f7ef0db8af88381e7

@ikea-aoa/component-lightbox-99.0.1 index.js

MD5: 025809495e179b4f7ef0db8af88381e7

@ikea-aoa/component-popover-99.0.0 index.js

MD5: 025809495e179b4f7ef0db8af88381e7

@cima/prism-utils-23.2.1 installer.js

MD5: 42d84beccb38c08700920b70549f5a87

@cima/prism-utils-23.2.2 installer.js

MD5: 25de187869441c3aa506ddc5fe6839ea

discorddd.jss-1.4.9 index.js

MD5: dc60d3e82ff0273309a2a9e1b7f89ea3

discorddd.jss-1.5.0 index.js

MD5: 740eca0a347fe0d0aa8ca8ec4ebf2dd2

discorddd.jss-1.6.4 index.js

MD5: 5182a61ee33247e2a426c4ddfe8196dc

saaaaaaaaaaaaaaaaaaaaaa-1.4.2 index.js

MD5: 8458b6a4196e5d86e241c758ce89d1e5

evernote-thrift-1.9.99 index.js

MD5: 359f456996c39e7882afeda8fbbf226f

en-features-rollout-1.90.9 index.js

MD5: 0f67856db1e0c466d13079cc9cb16963

en-conduit-electron-1.90.9 index.js

MD5: 0f67856db1e0c466d13079cc9cb16963

en-conduit-electron-auth-1.90.9 index.js

MD5: 0f67856db1e0c466d13079cc9cb16963

en-conduit-electron-worker-1.90.9 index.js

MD5: 0f67856db1e0c466d13079cc9cb16963

en-thrift-internal-2.30.9 index.js

MD5: 0f67856db1e0c466d13079cc9cb16963

en-conduit-electron-renderer-1.90.9 index.js

MD5: 0f67856db1e0c466d13079cc9cb16963

@expue/webpack-0.0.3-alpha.0 index.js

MD5: 084c4c5a1d36fbdab6705a2fbd7e849e

@expue/core-0.0.3-alpha.0 index.js

MD5: 8b82f6112b22bd67cccc4ad238bfea7c

@expue/vue3-renderer-0.0.3-alpha.0 index.js

MD5: 084c4c5a1d36fbdab6705a2fbd7e849e

@fixedwidthtable/fixedwidthtable-0.0.2 index.js

MD5: 084c4c5a1d36fbdab6705a2fbd7e849e

@virtualsearchtable/virtualsearchtable-0.1.1 index.js

MD5: 37f9d6a97af8d7589bbc11aadcf185ec

binarium-crm-1.0.0 index.js

MD5: acf9777d3fabc82b49ddb096147de6a9

binarium-crm-1.0.9 index.js

MD5: acf9777d3fabc82b49ddb096147de6a9

binarium-crm-1.9.9 index.js

MD5: acf9777d3fabc82b49ddb096147de6a9

career-service-client-0.1.6 index.js

MD5: 3d1dbd501ebaae4745f6ec37850f9ff5

career-service-client-0.1.13 index.js

MD5: 3d1dbd501ebaae4745f6ec37850f9ff5

career-service-client-0.1.15 index.js

MD5: 3d1dbd501ebaae4745f6ec37850f9ff5

hh-dep-monitoring-0.1.5 index.js

MD5: 3d1dbd501ebaae4745f6ec37850f9ff5

hh-dep-monitoring-0.1.14 index.js

MD5: 3d1dbd501ebaae4745f6ec37850f9ff5

orbitplate-1.0.4 index.js

MD5: 3d1dbd501ebaae4745f6ec37850f9ff5

orbitplate-1.0.6 index.js

MD5: 3d1dbd501ebaae4745f6ec37850f9ff5
