SECURITY ADVISORY

Axios npm Supply Chain Attack — March 31, 2026

Prepared by Warren Barr · barr-cyber.com · April 4, 2026

WHAT HAPPENED

On March 31, 2026, North Korean state-sponsored hackers compromised a widely used software package called Axios — one of the most downloaded JavaScript libraries in the world with over 100 million weekly installations. They published two malicious versions that silently installed a Remote Access Trojan (RAT) on any computer that updated or installed software during a roughly three-hour window that morning.

The RAT affects Windows, macOS, and Linux machines. It gives attackers persistent, silent access to the infected computer — and the machine looks completely clean.

> **This was a state-sponsored, pre-planned operation attributed to North Korea. It is not a minor incident.**

WHY THIS MAY AFFECT YOUR TEAM

You do not need to have installed Axios directly to be at risk. Axios is embedded as a hidden dependency in thousands of software packages, developer tools, and build systems. If anyone on your team:

- Ran a software update or installed any developer tools on March 31, 2026 between midnight and 3am UTC (roughly 6pm–9pm Mountain Time, March 30)
- Uses Node.js, npm, or any JavaScript-based development tooling
- Had automated build pipelines or CI/CD systems running during that window

...their machine may have received the RAT without any visible sign.

The malicious versions were removed from the public registry within three hours, but any machine that installed during the window remains compromised until remediated.

WHAT THE RAT DOES

- Establishes persistent, silent access to the infected machine for the attacker
- Steals credentials stored on the machine — passwords, API keys, cloud access tokens, SSH keys
- Phones home to a command-and-control server for further instructions
- Self-destructs its installation artifacts — the machine appears completely clean
- Can execute arbitrary follow-on commands or download additional payloads

> **A compromised machine should be treated as fully owned. Do not attempt to clean it — rebuild from a known-clean backup.**

AFFECTED SOFTWARE VERSIONS

Malicious — Do Not Use

```
axios  version 1.14.1
axios  version 0.30.4
plain-crypto-js  version 4.2.1   ← the hidden malicious dependency
```

Safe — Downgrade To

```
axios  version 1.14.0
axios  version 0.30.3
```

HOW TO CHECK — INSTRUCTIONS FOR YOUR TECHNICAL PERSON

The following commands can be run by anyone with access to a terminal or command prompt on the potentially affected machine. Copy and paste each command exactly as written. IMPORTANT — Read this first: If you run any of the commands below and the response says “npm is not recognized as an internal or external command” or “command not found” — STOP. This is good news. It means Node.js is not installed on this machine, which means the affected software was never present, and this machine is not at risk from this

specific attack. No further action is needed on this device. You are only at risk if npm is installed and recognized. If the commands run and return results — continue checking below.

On Windows — open Command Prompt or PowerShell

Check if affected Axios version is present:

```
npm list axios --depth=10
```

Look for axios@1.14.1 or axios@0.30.4 in the output. Either = compromised.

Check for the malicious dependency:

```
npm list plain-crypto-js
```

Any result = compromised.

Check for the Windows RAT artifact:

```
dir %PROGRAMDATA%\wt.exe
```

If wt.exe is found in that location and Windows Terminal was not manually installed = RAT artifact present.

Check for active connection to attacker server:

```
netstat -an | findstr 8000
```

Look for any connection to 142.11.206.73 or sfrclak.com = active RAT beaconing.

On macOS — open Terminal

Check if affected Axios version is present:

```
npm list axios --depth=10
```

Check for malicious dependency:

```
npm list plain-crypto-js
```

Check for macOS RAT artifact:

```
ls /Library/Caches/com.apple.act.mond
```

If this file exists and you don't recognise it = RAT artifact present.

Check for active C2 connection:

```
lsof -i :8000
```

On Linux — open Terminal

Check for RAT artifact:

```
ls /tmp/ld.py
```

If /tmp/ld.py exists = RAT artifact present.

Check npm and network:

```
npm list axios --depth=10
ss -tp | grep 8000
```

IF A MACHINE IS COMPROMISED

Step 1: Disconnect the machine from the internet and your network immediately.

Step 2: Do not attempt to clean or disinfect the machine. The RAT self-destructs its traces — standard antivirus will likely show nothing. The only safe remediation is a full rebuild from a known-clean backup or factory reset.

Step 3: Rotate every credential that may have been accessible on that machine:

- All passwords stored in browsers or password managers

- Cloud service credentials (AWS, Azure, Google Cloud)
- API keys and tokens
- SSH keys
- Any .env files or configuration files containing secrets

Step 4: Block the following at your firewall or router:

```
Domain:  sfrclak.com
IP:      142.11.206.73
Port:    8000 outbound
```

Step 5: Contact your IT security resource. If you do not have one, contact Warren directly.

INDICATORS OF COMPROMISE (IOCS)

Share these with your IT team or security vendor for immediate blocking and detection:

Malicious Domain

```
sfrclak[.]com
```

Malicious IP

```
142.11.206[.]73
```

C2 Port

```
TCP port 8000
```

Malicious npm Packages

```
axios@1.14.1
axios@0.30.4
plain-crypto-js@4.2.1
```

File Artifacts by OS

```
Windows:  %PROGRAMDATA%\wt.exe
macOS:    /Library/Caches/com.apple.act.mond
Linux:    /tmp/ld.py
```

ATTRIBUTION

This attack has been attributed by Microsoft, Google, Palo Alto Unit 42, and Sophos to North Korean state-sponsored threat actors. The operation was pre-planned with malicious infrastructure staged 18 hours before execution. Three separate platform-specific payloads were built in advance for Windows, macOS, and Linux. This is not a random opportunistic attack.

Sources: Microsoft Security Blog, Huntress, Elastic Security Labs, Palo Alto Unit 42, SANS Institute, Snyk, Sophos — all published April 1–2, 2026.

Questions or concerns? Contact Warren Barr directly.

barr-cyber.com · warrenbarr1022@gmail.com