Checkmarx

Feb 2024 | Supply Chain Security

Threat Trends to Watch

Research performed by the Checkmarx security research team in February encountered new cases of the following types of attacks, which represent the continuation of attack techniques first seen in 2023 and earlier.

Trend 01

Abandoned digital assets

Attackers are exploiting abandoned digital assets, turning them into trojan horses in open-source ecosystems. Case studies like MavenGate and CocoaPods illustrate the danger, as do instances of hijacked Rubygems package names and compromised S3 buckets, along with email domain hijacking and the recent RepoJacking attack on GitHub repositories.

To help prevent attacks like these, the Checkmarx security research team recommends monitoring and reoccupying abandoned digital assets to keep them out of the hands of attackers.

For more details on these threat types, please see these blog posts:

- The Hidden Dangers of Abandoned Digital Assets in Open-Source Ecosystems
- CocoaPods Subdomain Hijacked: This is How
- Hijacking S3 Buckets: New Attack Technique Exploited in the Wild by Supply Chain Attackers
- Persistent Threat: New Exploit Puts Thousands of GitHub Repositories and Millions of Users at Risk

Trend 02

Abuse of legitimate services

Attackers are increasingly exploiting legitimate free services like Telegram for data extraction, leveraging their widespread use and encrypted communication features to mask malicious activities. By employing Telegram bots, attackers can automate data collection from unsuspecting victims, exploiting the platform's convenience and anonymity.

This tactic enables cybercriminals to evade detection while efficiently gathering sensitive information such as credentials, financial data, and personal details.

To prevent attacks like these, the research team advises paying attention to suspicious traffic sent from or to what are considered legitimate services, such as GitHub and Telegram. Attackers have recently been using this to stay under the radar.

For an in-depth look at this type of attack, review this research:

- How We Were Able to Infiltrate Attacker Telegram Bots

Trend 03

Denial of service on critical open-source package hosting

The "everything" package, with millions of dependencies, caused a limited Denial of Service (DoS) attack. This campaign launched in January by the NPM user "gdi2290" caused disruptions in the NPM registry. The package relied on every publicly available NPM package, leading to storage space exhaustion and build disruptions.

This is a difficult type of attack to prevent without the use of solutions like Checkmarx Supply Chain Security and Checkmarx Supply Chain Threat Intelligence.

For an expose' of this type of attack, review our recent blog post:

- When "Everything" Goes Wrong: NPM Dependency-Hell Campaign – 2024 Edition

Take Preventive Action

Start securing your supply chain

Get Started

Investigate the Checkmarx Supply Chain Threat Intelligence API that delivers threat intelligence like this directly into your preferred dashboard or integrated development environment.