Checkmarx

June 2024 | Threat Trends

What are Malicious Open Source Packages Targeting Most?

During the month of June, the Checkmarx security research team studied our internal repository of over 385,000 malicious packages found in the wild. Here are the three trending goals of those malicious packages.

Trend 01

Exfiltrate host information – 58.44%

Everyone is a target - from individuals to large enterprises to government agencies. Data exfiltration attacks are among some of the most damaging and destructive out there. More than half of the malicious packages we studied in June 2024 were designed to exfiltrate data, like operating system information, hostname, mac addresses, and more.

Explore these blog posts for real-world examples of this type of attack:

- Webhook Party – Malicious packages caught exfiltrating data via legit webhook services
- When the Hunter Becomes the Hunted

Trend 02

Malicious code downloads – 24.12%

Threat actors continually evolve their methods for tricking users to download malicious code from seemingly secure or trustworthy sources. For example, one technique involves the embedding of pixels containing malicious code within VAST video ads. Many of the attacks we studied were designed to occur in multiple stages. Ultimately, they download and execute additional malicious code from an external resource.

For more information and examples, consider these resources:

- Alert: CDN Service “polyfill.io” Used by 100K+ Websites Provided Malicious Code in Responses
- New Technique to Trick Developers Detected in an Open Source Supply Chain Attack
- A New South Korean Group Emerges, Disrupting the Open Source Ecosystem

Trend 03

Exfiltrate credentials – 17.44%

System credentials are a highly prized target. Credentials include information like passwords, browser cookies, API keys, and anything that can grant access to system. The Codecov attack is one example of a highly destructive campaign that exploited an error in Codecov’s Docker image creation process to steal credentials from hundreds of their customers systems.

Get more detail on this type of malicious code from these research blog posts:

- Attacker Caught Hijacking Packages Using Multiple Techniques to Steal AWS Credentials
- Surprise: When Dependabot Contributes Malicious Code

Take Preventive Action

Checkmarx One covers all the bases from secure code training, SAST and DAST to SCA, API security and supply chain security.

Learn More

Discover the Checkmarx Supply Chain Threat Intelligence API that delivers software supply chain security threat intelligence directly into your preferred dashboard or integrated develop-