Checkmarx

Jan 2024 | Supply Chain Security

# Threat Trends to Watch

The Checkmarx Security Research team analysis of industry data revealed that the top three trends in supply chain attacks that occurred in January are as follows.

## Trend 01

### Information and credential theft – 56% of attacks in January

There is a significant trend of attacks aiming to siphon sensitive data such as host information and user credentials. The occurrence of such breaches suggests that attackers are focusing on gaining unauthorized access to confidential data, which could be exploited for additional malicious activities. Most often attackers breach upstream servers or code repositories, then inject malicious payloads that are distributed downstream to many users.

However, other methods are used to steal credentials, as in the Codecov supply chain attack in 2021, which invoked the HTTP-based backdoor when the Inventory Manager plugin was loaded. This method used stolen credentials from a flawed Docker image creation process to modify the Codecov Bash Uploader, then modified the Codecov Bash Uploader hosted on the Codecov server itself to gather environment variables uploaded from customers' continuous integration/ continuous delivery (CI/CD) environments:

### More on credential theft:

- Surprise: When Dependabot Contributes Malicious Code →
- Attacker – hidden in plain sight for nearly six months – targeting Python developers →
- Threat Actor Continues to Plague the Open-Source Ecosystem with Sophisticated Info-Stealing Malware →

## Trend 02

### Dependency confusion and typosquatting tactics: 28% of attacks in January

We discovered a high volume of incidents involving malicious actors deploying packages whose names closely resemble those of legitimate and trusted libraries. Typosquatting is a type of social engineering attack that uses these purposely misspelled domains for a variety of malicious purposes.

In open source attacks, typosquatting attempts to trick developers into downloading and integrating malicious packages into their software unknowingly. In other cases, typosquatting is used for extortion by selling a misspelled domain name back to the brand owner.

### More on Typosquatting attacks:

- A new, stealthier type of Typosquatting attack spotted targeting NPM →
- Users of Telegram, AWS, and Alibaba Cloud targeted in latest supply chain attack →
- As Malicious Open Source Packages Proliferate, Checkmarx Announces Supply Chain Threat Intelligence for Faster, Easier Identification of Potential Threats →

## Trend 03

### Malware and backdoor injections – 16% of attacks in January

The data points to a prevalent use of malware and backdoors embedded within compromised packages. These infiltrations are designed to compromise systems by providing attackers with covert access, compromising data, or disrupting operations within targeted organizations.

Last year attackers were found to be using an outdated WordPress plugin, Eval PHP, to inject PHP code that delivered a payload that gave attackers remote code execution capabilities within the compromised site. Our own research this month discovered an attack that began by forwarding all exfiltrated data through a Telegram bot API to a security researcher's personal Telegram chat, then redirected the stolen data from the threat actor's chat to their own chat.

### More on malware and backdoor injections:

- When the Hunter Becomes the Hunted →
- How One Country is Impacting Supply Chains →
- Python Obfuscation Traps →

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.