sonatype

The Trust Economy of Software

How AI is Reshaping Software Supply Chain Risk for Financial Services

For years, most software supply chain attacks relied on scale. Attackers published malicious packages, cast a wide net, and hoped someone would eventually download them. That model is changing.

Analysis of Sonatype's malware intelligence data reveals a significant shift in attacker behavior. Volume is not the most important trend.

What is notable is where attackers are focusing their efforts. Rather than relying on broad distribution alone, attackers are increasingly trying to influence software decisions before code ever reaches production.

Sonatype's analysis of nearly 10,000 malware advisories shows targeted attacks, developer-focused malware, and sophisticated attack techniques all increased significantly during the AI era. As AI coding assistants accelerate software creation, they also accelerate the rate at which developers discover, evaluate, and consume new software dependencies.

Attackers have noticed.

In 2025, 53% of the malicious packages analyzed were designed to compromise developer environments during installation, often targeting credentials, secrets, or other sensitive information before traditional security controls can intervene.

Highly regulated industries often reveal security trends before they become mainstream. In Financial Services, Sonatype telemetry shows malicious packages reaching enterprise development workflows with increasing frequency, reinforcing that software supply chain attacks are already an operational reality.

The software supply chain has entered a new phase. Open source malware is becoming more targeted, more sophisticated, and more effective at exploiting trust. This report examines how software supply chain attacks have evolved in the AI era, why developers have become a primary target, and what the latest data reveals about the future of malicious open source threats.

75x

Increase in targeted malicious package advisories in just two years

47%

Of malicious packages now impersonate trusted software

53%

Of malicious packages targeted developers at install time

36%

Of malicious advisories now contain at least one stealth technique

The AI-Era Inflection Point

AI is accelerating how software components are discovered, evaluated, and adopted, creating more opportunities for attackers to influence software decisions.

The software industry has spent the last several years focused on a single question: how much faster can AI help developers write code? A less discussed question may prove just as important: how much faster can AI help developers choose software?

Modern applications are increasingly assembled rather than written. Open source components, third-party packages, containers, AI-generated code, and AI-generated recommendations all influence what eventually reaches production. Every application depends on a steady stream of decisions about what to install, what to trust, and what to build upon.

Historically, those decisions happened at human speed using current information. Developers searched documentation, evaluated libraries, compared alternatives, and made deliberate choices about which components entered their applications.

AI is changing that dynamic:

- Coding assistants can recommend software dependencies in seconds.
- Agents can generate implementations that rely on packages a developer has never previously encountered.
- Development teams can evaluate and adopt new components faster than ever before.

The productivity benefits are well understood. Less understood is how AI changes the rate at which software components are discovered, evaluated, and adopted.

Sonatype's malware intelligence data shows malicious open source activity accelerated significantly beginning in 2024. More importantly, attackers appear to be shifting from a volume strategy toward a precision strategy designed to influence which software developers choose in the first place.

In 2025, Sonatype researchers identified 4,001 malware advisories, representing a 4x increase over the pre-AI baseline of 1,004 advisories per year.

The increase was not limited to open source malware volume.

WHAT IS A MALICIOUS PACKAGE ADVISORY?

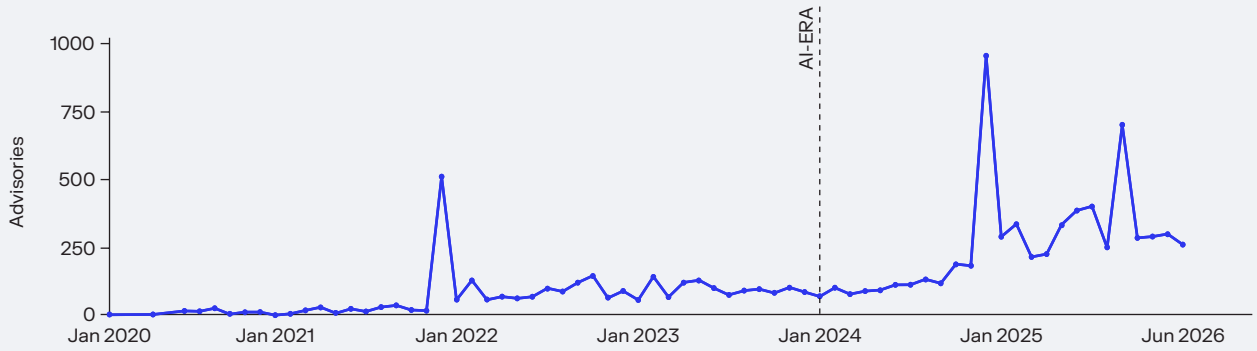
A malicious package advisory is a security alert for an open source package, or a cluster of likely-related packages, published in a public registry that was intentionally created or modified for malicious intent.

After removing large-scale abuse campaigns that can distort open source malware counts, the number of distinct malicious payloads still increased by more than 50% compared to the pre-AI period. Attackers were not simply publishing more malware. They were experimenting with more techniques, delivery mechanisms, and approaches to compromising software development environments.

FIGURE 1

Malicious Open Source Activity Accelerated in the AI Era

Annual malware advisories remained relatively stable from 2021 through 2023 before accelerating sharply beginning in 2024. By 2025, annual advisories had grown to 4 times the pre-AI baseline, signaling a significant increase in malicious open source activity.



Attackers are adapting to the same forces reshaping software development: automation, faster dependency adoption, and increasing reliance on software recommendations.

Software selection is accelerating alongside software creation. Developers are evaluating more components, more updates, and more recommendations than ever before, often under increasing pressure to move quickly.

That changes the economics of software supply chain attacks. Influencing a software decision can be more valuable than exploiting a vulnerability after deployment.

THE RESULT IS A DEVELOPMENT ENVIRONMENT WHERE TRUST DECISIONS HAPPEN FASTER AND ATTACKERS HAVE MORE OPPORTUNITIES TO INFLUENCE WHAT ENTERS THE SOFTWARE LIFECYCLE.

The Rise of Precision Targeting

Software supply chain attacks are shifting from broad open source malware distribution to precision targeted. Rather than publishing malicious packages and hoping for widespread adoption, attackers are increasingly impersonating trusted software because influencing a software dependency decision is often more effective than exploiting a deployed application.

For most of the past decade, software supply chain attacks followed a fairly simple formula: publish malware, maximize exposure, and wait for victims. The strategy was built around probability: the more packages an attacker could push into an ecosystem, the better their chances of reaching someone valuable.

The data indicates attackers are increasingly prioritizing impersonation and trust-based deception over broad distribution alone.

Between 2021 and 2024, targeted attacks accounted for just 2% to 4% of classified open source malware advisories annually. In 2025, that figure jumped to 47.3%, making targeted malware one of the dominant forms of malicious open source activity observed during the year.

The shift becomes even more striking when viewed in absolute terms. Sonatype researchers identified 28 targeted open source malware advisories in 2023. By 2025, that number had grown to 1,576.

Beyond Typosquatting:

HOW PRECISION ATTACKS WORK

For years, software supply chain attacks relied on simple misspellings to catch developers typing quickly.

Today's attacks rely on something more effective: familiarity.

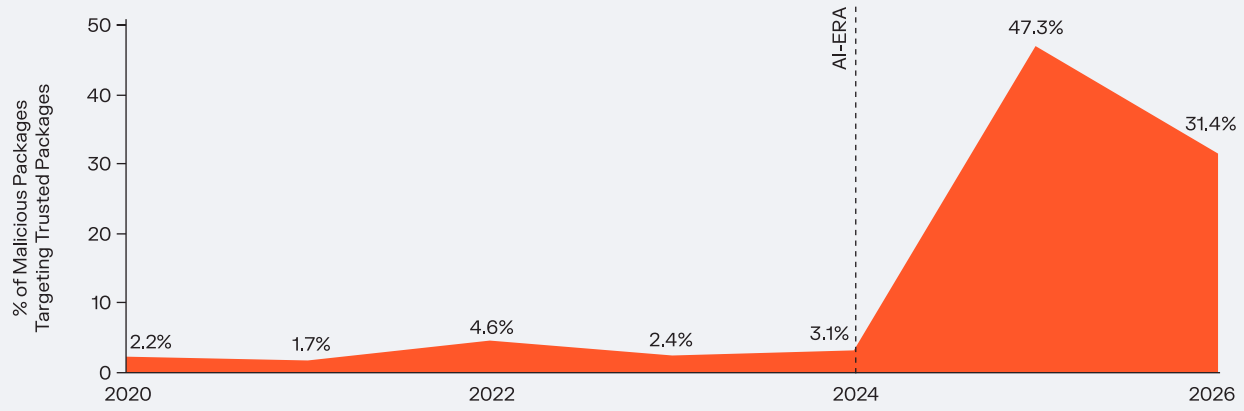
Previous Sonatype research found that only 9% of malicious packages used traditional typosquatting alone. Most used names designed to appear legitimate, including helper libraries, plugins, utilities, integrations, and ecosystem-adjacent packages.

Rather than waiting for a typo, attackers are betting on trust.

FIGURE 2

Targeted Malware Became Mainstream in 2025

For four consecutive years, targeted attacks represented only a small percentage of classified malware advisories. In 2025, that share increased dramatically to 47.3%, signaling a major shift toward precision attacks designed to impersonate trusted software and exploit developer trust.



Rather than short-term volatility, the magnitude of this increase suggests a meaningful shift in how attackers approach software supply chain compromise. For years, software supply chain attacks were largely a numbers game. Publish enough malicious packages and eventually someone would install one.

The data points to a different approach. Attackers are investing more effort in appearing legitimate by mimicking trusted projects, familiar tooling, popular frameworks, and ecosystem-adjacent packages.

The objective has shifted from simply getting malware published to influencing software decisions, which is increasingly significant as modern software becomes assembled rather than

written. Developers routinely evaluate new packages, AI-generated recommendations, framework extensions, integrations, and utility libraries. Most of those decisions are made quickly because they have to be.

Attackers are designing campaigns around a simple reality: developers evaluate more software than ever and spend less time evaluating each individual decision.

As software becomes increasingly assembled from existing components, influencing software selection becomes an increasingly attractive attack vector.

> **ATTACKERS ARE INCREASINGLY FOCUSED ON INFLUENCING WHICH SOFTWARE GETS SELECTED IN THE FIRST PLACE.**

Developers are the Enterprise Attack Vector

Developers have become a primary target of software supply chain attacks and are targeted during installation, before traditional security controls can inspect the resulting software.

In 2025, 53% of malicious packages analyzed were designed to compromise developer machines at install time, often before traditional security controls have a chance to inspect the resulting application. These attacks frequently use package installation behavior, such as preinstall or postinstall hooks, to execute when a developer adds new software dependencies.

Sonatype observed 581 developer-targeting advisories in 2023. By 2025, that number had grown to 2,116, a 3.6x increase.

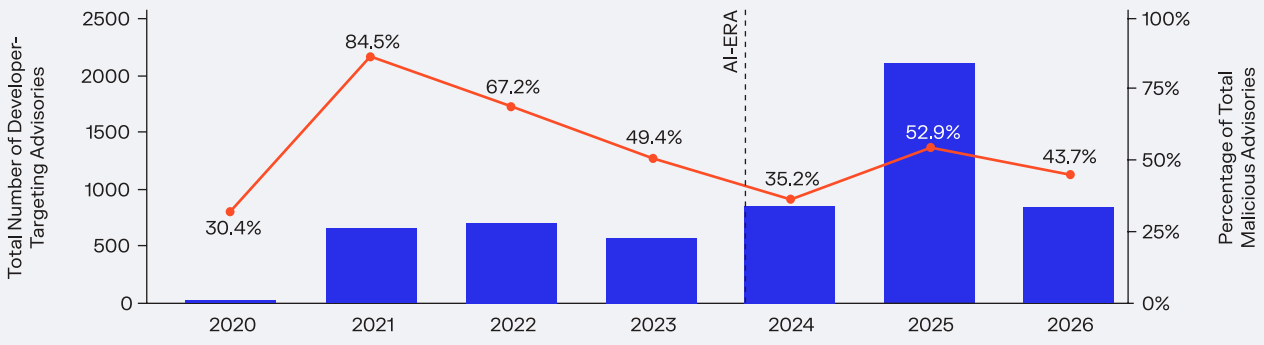
This shift moves risk earlier in the software lifecycle. The danger is not limited to vulnerable code that reaches production. It can begin when a developer installs a package, accepts a recommendation, or pulls software dependencies into a local environment.

A malicious package does not need to survive all the way to deployment to be successful. If it executes during installation, it can collect credentials, tokens, secrets, and system information long before a traditional security review occurs.

FIGURE 3

Most Malware Now Targets Developers Before Production

Developer-targeting malware increased 3.6x between 2023 and 2025, showing how attackers are moving earlier in the software development lifecycle.



Once there, malicious code can target credentials, secrets, host information, and access tokens before the software ever reaches CI/CD. By the time a traditional scan runs, the damage may already be done.

The developer workstation has become a front line of the software supply chain.

Software Supply Chain Attacks Are Getting Cheaper

Open source malware does not have to be elite to be effective anymore.

Techniques that once signaled a more deliberate, higher-effort software supply chain attack campaign are showing up more often across everyday malicious packages. Sonatype analyzed confirmed-malicious packages for structural complexity indicators, including obfuscation, multi-stage droppers, and backdoors. These are the patterns attackers use to hide behavior, delay analysis, and make malicious packages harder to classify quickly.

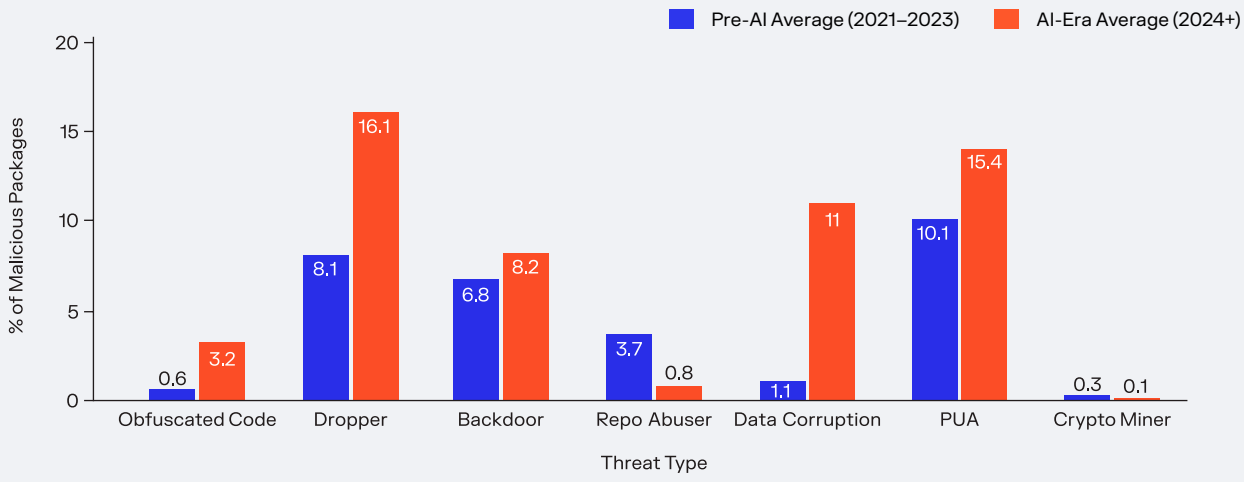
Before the AI era, 15.5% of malicious advisories contained at least one of these indicators. Since 2024, that share has increased to 25.5%. In other words, more than 1 in 4 malicious package advisories now include non-trivial implementation techniques.

Obfuscation saw the sharpest increase. Prior to 2024, fewer than 1% of malicious advisories used obfuscation. Today, obfuscation appears more than 8 times as often.

FIGURE 4

Sophisticated Malware Techniques Are Becoming More Common

The share of malware containing sophisticated implementation techniques increased from 15.5% before the AI era to 25.5% afterward. Obfuscation showed the largest increase, growing more than sixfold.



That does not prove AI caused the shift, but it does suggest attackers are operating in the same software reality as everyone else: code is faster to generate, easier to modify, and cheaper to adapt. The same forces helping developers move faster can also help attackers test more variants, hide intent more effectively, and iterate before defenders have a stable pattern to detect.

For defenders, volume is no longer the only problem. The average malicious package is becoming harder to understand on arrival.

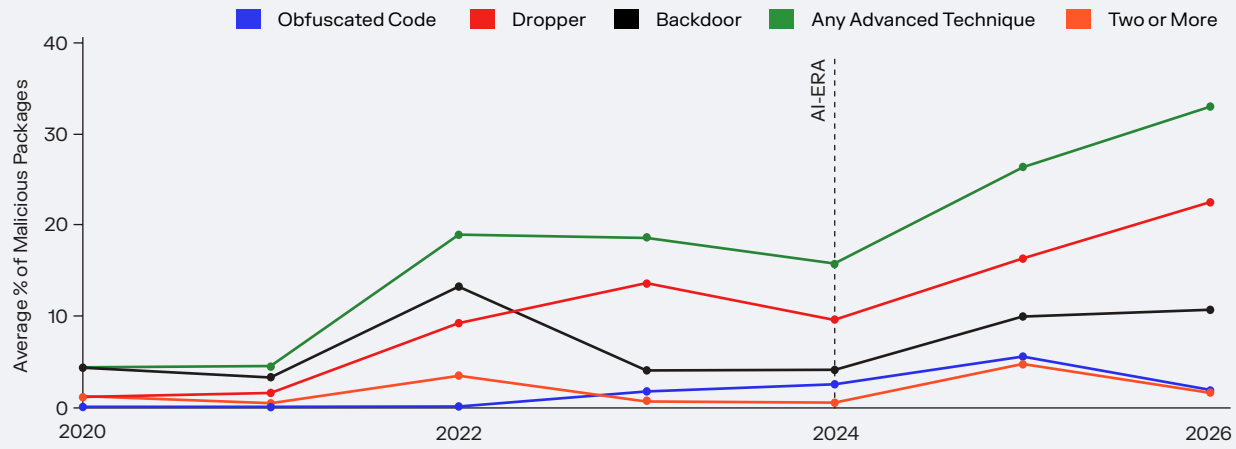
That changes what security teams need from detection. It is not enough to recognize yesterday's bad package after the pattern is obvious. Teams need to identify suspicious behavior, package integrity issues, and malicious intent before a package becomes another trusted dependency in the build.

AI-Era Attackers Are Investing More in Stealth

FIGURE 5

More Malicious Packages Use Advanced Implementation Techniques

Attackers increasingly rely on obfuscation, droppers, and backdoors to delay analysis and complicate investigations. The trend suggests that sophisticated malware is becoming more common, not just more numerous.



Before 2024, fewer than 1 in 5 malicious package advisories contained a structural complexity indicator. By 2026, that figure had grown to more than 2 out of every 5. Multi-stage droppers saw particularly rapid growth, while obfuscation and backdoors also became increasingly common.

This shift reflects a change in attacker economics. As software development accelerates, attackers are investing more effort in making malware survive scrutiny long enough to reach developer environments. The goal is no longer simply to publish malicious code. It is to make that code harder for defenders to quickly understand, classify, and respond to.

For defenders, that raises the cost of every investigation. As sophisticated implementation techniques become more common, organizations need greater confidence in the software they consume — not just after analysis, but before components ever enter the development lifecycle.

Financial Services is the Canary in the Code Mine

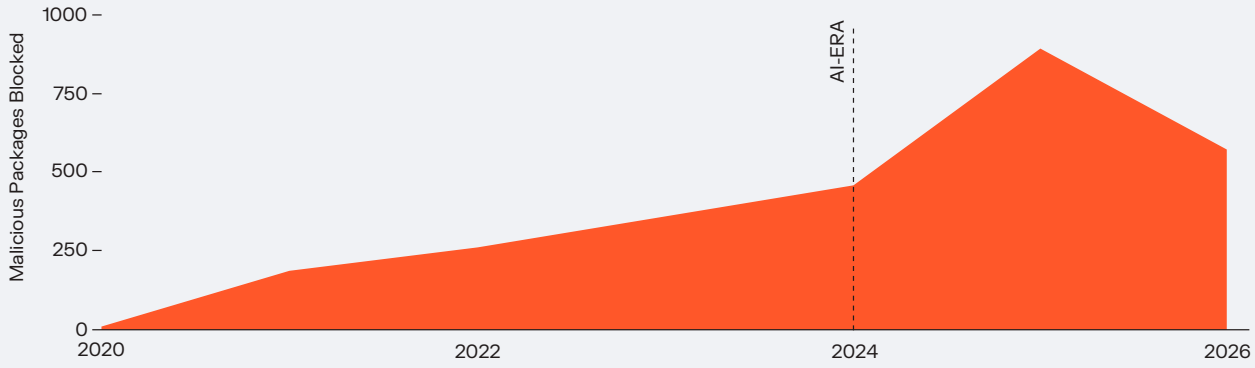
Threat intelligence reveals what attackers publish. Enterprise telemetry shows whether those attacks actually reach developers.

Across Sonatype-protected financial services organizations, malicious packages blocked before entering development environments have increased dramatically over the past several years. What began as isolated incidents has become a persistent operational reality, with a surge of malicious packages intercepted starting in 2025. That spike was not a fluke, as the number of attacks prevented for the sector in 2026 already represents more than 64% of last year's total.

FIGURE 5

Malicious Packages Blocked in Financial Services Continue to Rise

Sonatype-protected financial services organizations blocked increasingly more malicious packages each year between 2020 and 2026. By the end of Q2 2026, organizations had already blocked 572 malicious packages, more than 64% of the total blocked during all of 2025 (893 malicious packages), putting 2026 on pace to remain among the highest years on record.



This does not necessarily mean financial institutions are being targeted more aggressively than every other industry. Financial services organizations tend to operate mature software governance programs that provide clear visibility into software supply chain activity. As a result, they offer an early view into how modern attacks are evolving.

The broader implication is difficult to ignore. Malicious packages are no longer rare events hidden deep within public registries. They are increasingly reaching enterprise development workflows as developers evaluate more open source components, adopt AI-assisted coding tools, and make software decisions at machine speed.

Trust: The New Software Supply Chain Battleground

The data shows a threat landscape becoming more targeted, more sophisticated, and more effective at exploiting trust. Open source malware volume continues to rise, but the more important shift is attacker behavior. Precision attacks designed to impersonate trusted software, compromise developer environments, and evade traditional detection are becoming a defining feature of modern software supply chain risk.

On the other side, open source already serves as the foundation of most modern applications, and AI is accelerating how developers discover, evaluate, and consume software components. Decisions once made manually are increasingly shaped by automation, recommendations, and machine-speed workflows.

The findings suggest AI is accelerating the same forces already reshaping development: speed, scale, automation, and accessibility. Those forces benefit defenders and attackers alike.

> **THE NEXT SECURITY QUESTION MAY NOT BE SIMPLY WHETHER CODE CAN BE TRUSTED. IT MAY BE WHETHER THE SYSTEMS AND DECISIONS THAT SELECTED THAT CODE CAN BE TRUSTED TOO.**

The challenge is no longer limited to securing code after it enters the build. Organizations also need visibility into how software is selected, how trust is established, and how risk enters development workflows in the first place.

The next security question may not be whether code can be trusted. It may be whether the systems and decisions that selected that code can be trusted too.

Methodology

This analysis is based on Sonatype's malware intelligence dataset, which contains 9,747 verified malicious package advisories identified between January 2020 and May 2026. Advisories are created and classified by Sonatype's malware research team and represent groups of related malicious components rather than individual package versions.

The analysis uses a pre-AI baseline of 2021–2023 and compares it against the AI era, defined as 2024 onward. The year 2020 was excluded from baseline calculations due to limited sample size.

To evaluate open source malware trends, Sonatype analyzed advisory volume, targeting behavior, developer-focused attack techniques, structural complexity indicators, and detection performance. Structural complexity measurements focus on implementation techniques such as code obfuscation, multi-stage droppers, and backdoors, which provide insight into the sophistication of malicious packages beyond their intended outcomes.

Where appropriate, large-scale repository abuse campaigns were excluded from certain calculations to avoid overstating malware growth. These campaigns often involve automated publication of thousands of nearly identical packages and can distort measurements of payload diversity and attack sophistication.

The financial services analysis is based on anonymized telemetry from Sonatype-protected organizations and measures malicious packages blocked before entering enterprise development environments.

Several findings may be influenced by changes in attacker behavior, improvements in Sonatype's research capabilities, and ongoing refinements to malware classification methodologies. While these factors may affect absolute values, the directional trends observed throughout the analysis remained consistent across multiple independent measurements.