



SOFTWARE SUPPLY CHAIN SECURITY RETROSPECT

Shaping a safer
2024

a report by Luis Rodríguez,
CTO & co-Founder of Xygeni

Table of Content

Introduction.....	3
Highlights (“by the numbers”).....	4
The Attack Landscape.....	5
Summary of the most relevant attacks.....	10
Maturity: Adoption of security frameworks and practices..	15
Evolution of Standards and Regulations.....	19
The emergence of AI.....	22
The Future: What We Expect for 2024.....	25
References.....	27

About the Author



Luís Rodríguez
Co-founder and CTO of Xygeni

Luís Rodríguez, a physicist and mathematician, brings significant experience to the field of software security, focusing on static analysis and software supply chain security. As the co-founder and Chief Technology Officer (CTO) of Xygeni, Rodríguez contributes his expertise to the company's leadership and innovation in the realm of software security.



©2024 Xygeni Security
Author: Luís Rodríguez
Special thanks to
Jesús Cuadrado.



Introduction

Now that the 2023 is over, many “state of cybersecurity” reports are popping up. The most recent: is the [NSA 2023 Cybersecurity Year in Review](#). We at Xygeni hope that our analysis of the events in this turbulent year could help with facing the threats to the software supply chain.

Modern software is key for our societies. But its complexity is overwhelming. It is estimated that [at least 90% of companies](#) rely on open-source software, and based on a report by Synopsys in 2022, [97% of commercial codebases](#) use open-source components. Dev(Sec)Ops and cloud-native approaches continued growing this year, and AI adoption started to be a concern.

In the current state of the software supply chain, (SSC) security, cyber threats and attacks remain a significant concern for companies and individuals

alike. In addition, the rise of remote work and the increased reliance on cloud-based services has expanded the attack surface, making securing the software supply chain more challenging.

The software industry is now realizing (much later than the bad actors) that the supply chain has become a deliberate attack vector. How to secure this mess? How can I trust software from both the open-source community and from my commercial software providers? How can I give confidence to my software consumers that I am not delivering deadly vulnerabilities or malware?

This report is Xygeni’s view on the events and trends in software supply chain security that occurred in 2023 and an initial assessment of what 2024 will bring us.

Keynotes

- ▶ What are the outstanding facts in numbers.
- ▶ How bad actors evolved their activity, with a summary of the most prominent attack cases.
- ▶ How the industry evolved for maturing its software security posture, particularly about the build and deployment of software.
- ▶ The rise of standards and regulations will be relevant for the next few years.
- ▶ The role of the emergent AI and ML technologies and how they will modulate
- ▶ And last but not least, a glimpse into the near future: what we expect for 2024.



Highlights ("by the numbers")

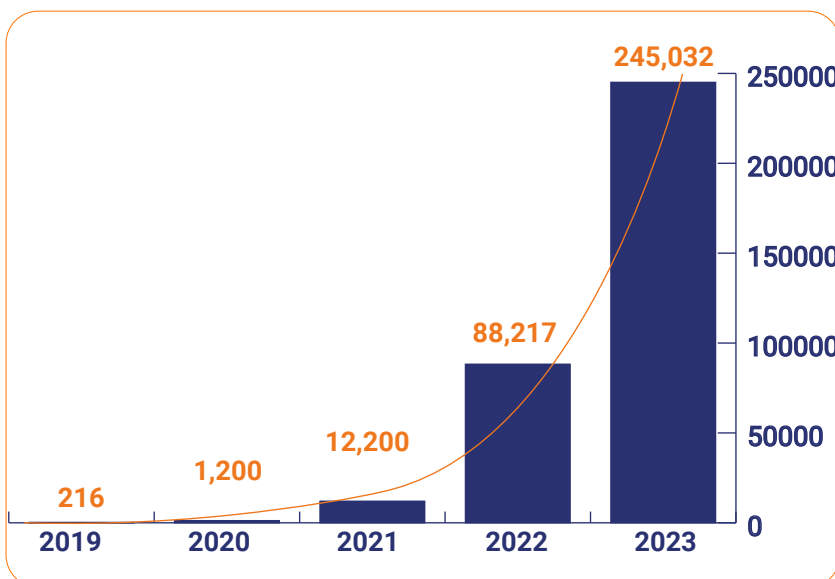
Some call 2023 the year of [‘digital forest fires’](#). Incidents like those affecting PyTorch, 3CX or MOVEit Transfer made headlines.

We have tough work for the near future. Today, **82% of organizations are vulnerable to software supply chain attacks**. Furthermore, software supply chain attacks are expected to increase in frequency and severity in 2023. According to NTT Ltd, the technology sector is the most targeted industry for supply chain attacks, accounting for 28% of all attacks.

Open source software (OSS) is everywhere. [Around 70% to 90% of a contemporary application “stack” comprises pre-existing OSS](#). Such flexibility comes with a cost. Attackers know this, so [malicious packages pushed on public registries this year raised to a whopping 245,032 instances](#). This doubles the aggregated number from previous years, showing exponential growth. And we said malicious, not vulnerable.

Security on OSS projects seems to have worsened during 2023. According to the scores by OpenSSF Scorecard ran by the end of [nov’ 2023](#), 1,235,931 projects ran the scorecard (with a modest 1% increment from 2022), but the mean for the score decreased from 4.3 to 3, with 75% of the projects with a score below 3.2. More on this later.

Malicious Open Source Packages per Year



82%

of organizations are vulnerable to software supply chain attacks.

*Venofi. [Report](#) from a global survey of 1,000 CIOs.

28%

of all supply chain attacks target the technology sector

* NTT Ltd

70%

to 90% of a contemporary application “stack” comprises pre-existing OSS.

* Sonatype. [Report State of Software Supply Chain](#)

245,032

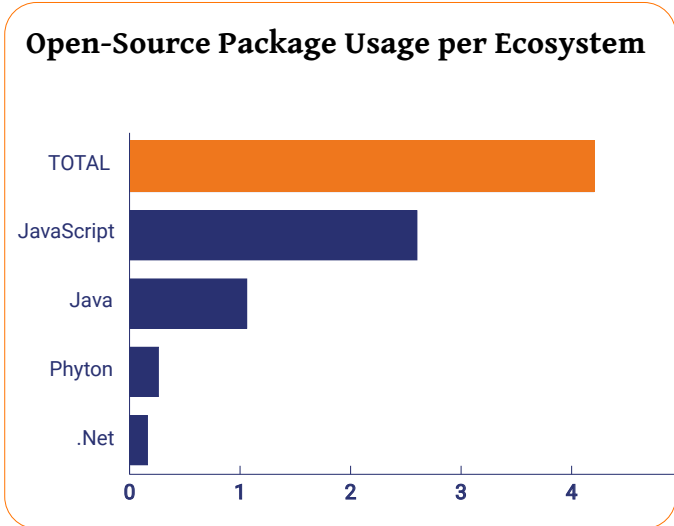
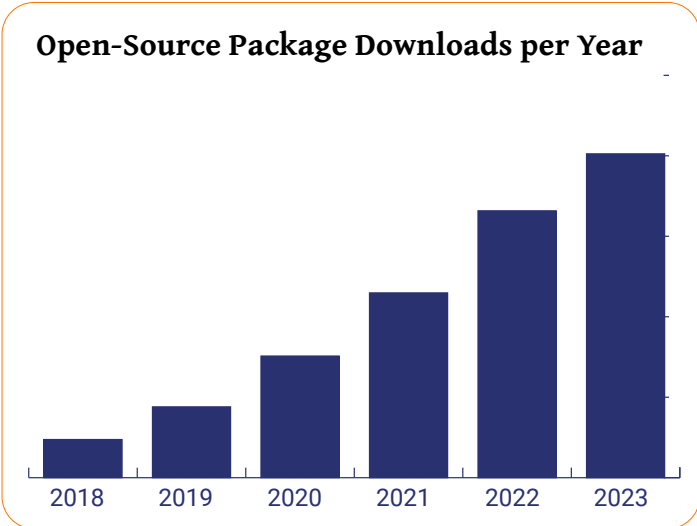
malicious packages were pushed onto public registries this year

* Sonatype. [Report State of Software Supply Chain](#)



The Attack Landscape

A larger dependency on open-source software implies that open-source has undeniably become a large attack vector. Watch at downloads for OSS packages, in the trillions (1012):



The industry needs to work collectively on the standards, processes, education, and tooling to mitigate risks to global supply chains. This is not a problem a single organization can solve on its own.

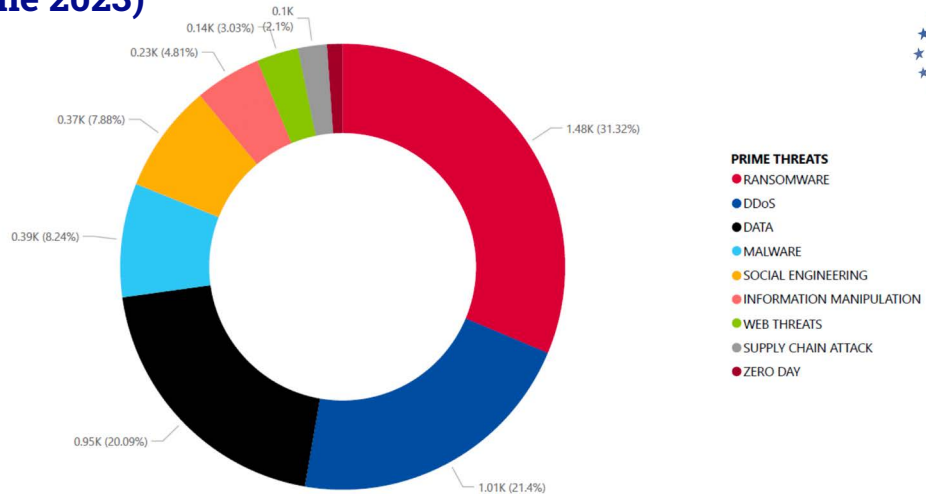
During 2023 cyber attacks were on the rise. The EU Agency for Cybersecurity, ENISA, published an important report, the [ENISA Threat Landscape 2023](#), which gave a count of 2,580 security incidents with 220 incidents specifically targeting two or more member states, and the public administration the most impacted sector.

ENISA Threat Landscape 2023



Looking at the trends, ransomware and denial-of-service (DoS) attacks were the most frequent, but targeted attacks on the SSC were observed.

Breakdown of analysed incidents by threat type (July 2022 till June 2023)

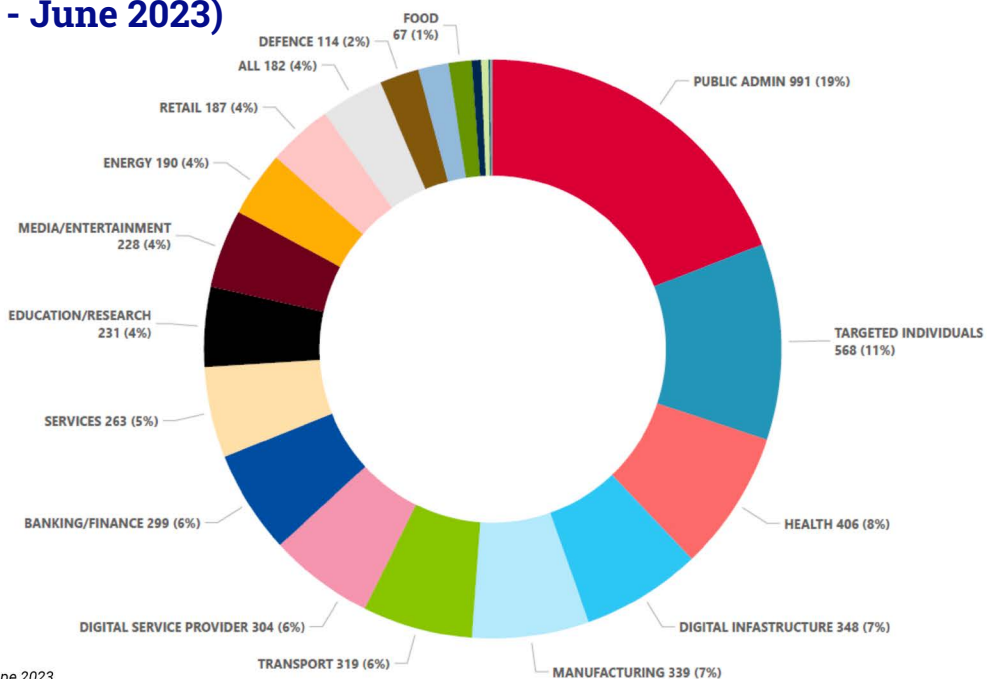


Source Enisa Threat Landscape 2023

Interestingly, the report records a surge in artificial intelligence (AI) chatbots impacting the cybersecurity threat landscape, noting that 'cheap fakes' and AI-enabled manipulation of information continue to be a cause for concern.

The attack landscape by sector shows that public admin (19%) and health (8%) were the most affected, but events targeting digital infrastructure (7%) and digital service providers (6%), so technology is an attractive target. Most threat actors, opportunistic by nature, were sector-agnostic.

Targeted sectors per number of incidents (July 2022 - June 2023)



Source Enisa Threat Landscape 2023

Attack Techniques in 2023



For attacking the software supply chain, the common approaches in 2023 for the initial breach kept involving spear phishing and social engineering, stolen credentials, and dependency attacks like typosquat packages. We observed a rise in attempts aimed at compromising CI/CD pipelines, with a few successful breaches.

During 2023 these methods were also the most prevalent, but additional, sophisticated techniques like [vishing](#) (Voice Phishing) using IA-generated, voice-mimicking messages targeting devops engineers were reported.

Malicious packages deployed in public registries are the most common attack, with a whopping 245,032 malicious packages. This figure more than doubles the total number from previous years combined!

In numeric terms, the most frequent attack is **dependency typosquatting**¹, where attackers mimic the names of existing popular packages on public registries, in the hope that developers may misspell the intended package name and accidentally download the malicious one.

One might be tempted to ignore such “trivial” attacks, assuming that developers are not so dumb as to mistype the name of a popular package. Do not! Unsophisticated cybercriminals always take the “path of least resistance”. Effective prevention should not stop at demanding due diligence from developers (“double-check the package name and make sure that it is the real thing”): use an internal registry for a white-listed set of allowed packages, plus detectors for potential typo-squats based on string similarity and other heuristics.

The cybercrime-as-a-service, **CaaS**, which started for ransomware and DDoS, now extends to phishing and malware spreading. They are used even by experienced cybercriminals because it allows them to diversify their attacks without much effort.

Insider threats, notably backdoors in software, were also reported. In today’s software, where development is externalized into third parties, never forget that evil can be at or “near” home.

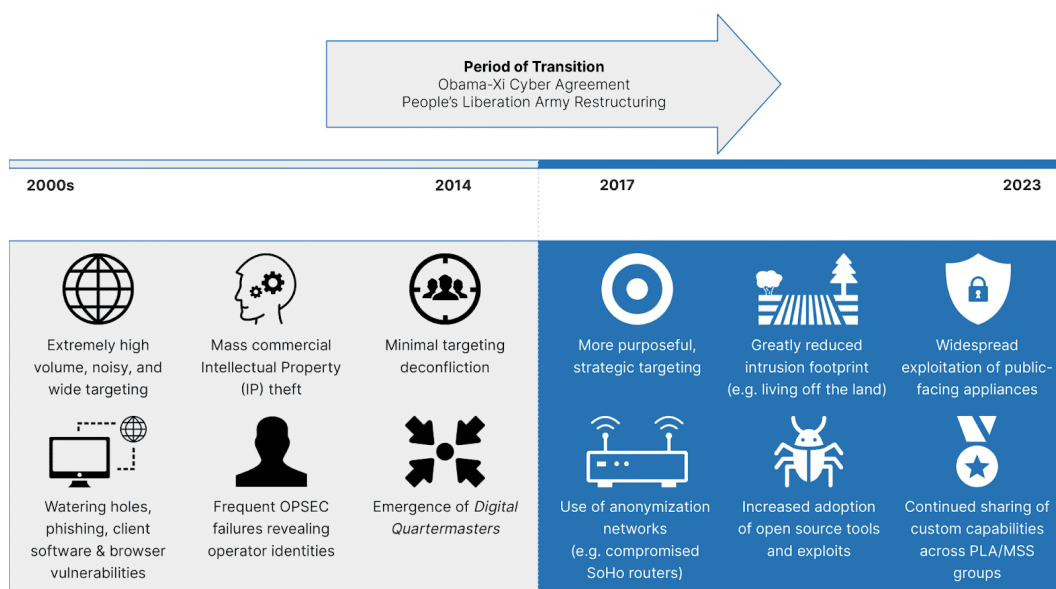
¹Spam packages are also ubiquitous; technically they do not convey attack code, but adware offering “magic elixirs” instead. They add a lot of noise. During 2023 we saw spikes in spam packages rate.

Advanced Threat Actors

From [CrowdStrike's 2023 Global Threat Report](#), geopolitics is often the driving force for the attacks from state-backed APTs. During 2023 the world saw how the Ukrainian war translated into cyber operations for disinformation, espionage, and sabotage. Iranian-backed Emmentet Pasargad's regional-targeted espionage and [hack-and-leak](#) and Log4Shell operations². China is rising as a global CyberPower. And do not forget the persistent resource abuse for crypto mining & cryptocurrency theft campaigns from North Korea.

It is too early for a clear assessment of the impact of the recent conflict between Hamas and Israel, but some reports document [DDoS attacks from both sides](#), while others [link Hamas with Iranian threat activity](#). The Iranian-linked APT Agrius (a.k.a. "Agonizing Serpens"), known for its destructive wipers, mainly targets Israeli organizations across multiple industries and countries. Agrius's [activity during 2023](#)³ targeted the education and technology sectors in Israel.

Cybercrime is getting more sophisticated. A good example is the evolution of China as a cyber power:



Source: Charting China's Climb as a Leading Global Cyber Power, in Recorded Future by Insikt Group.

An example (reported by ESET) of an SSC attack by a Chinese APT known as Evasive Panda: Chinese members of an international NGO, were [targeted by malicious updates](#) of popular Chinese chat apps (Tencent QQ and

WeChat), including a backdoor known as MgBot, possibly by compromising the update servers for delivering the backdoor only to the intended targets.

²Iranian-backed APTs are targeting opposition groups and organizations perceived as affiliated or supporting, often using destructive ransomware, and disguised as hacktivism.

³Interestingly enough, a web server vulnerability was exploited to drop a webshell (variant of ASPXSpy) that was encoded in the base64 payload of a fake PEM certificate file!

The impact

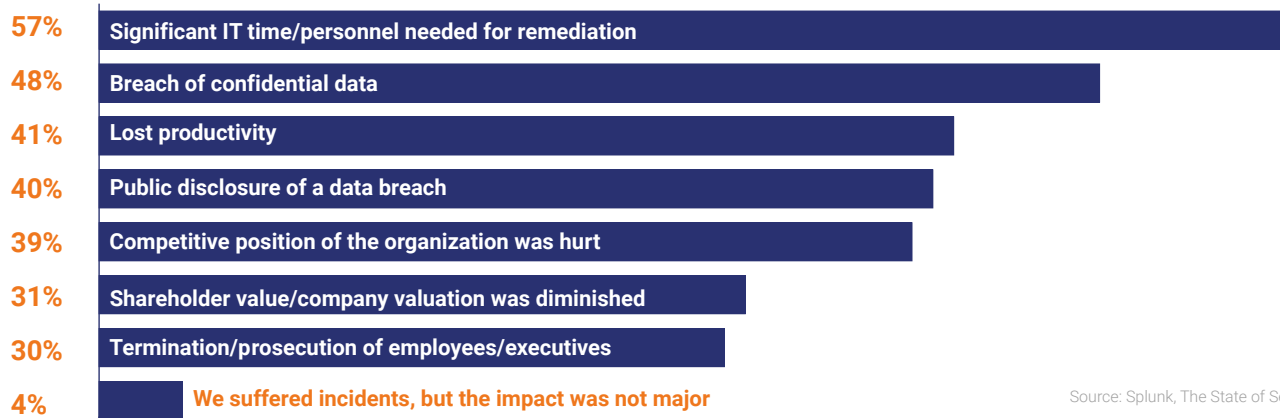
When looking at the impact of general cyberattacks⁴, **the digital impact** (damaged or unavailable systems, corrupted data files, exfiltration of data, and malicious intrusion) is by far the most prevalent, followed by **financial loss** (due to the loss of important material or ransom paid) and **social impact** (effect on the general public or impact on society due to disrupting services or leakage of private information) composing the most of the impact—source: ENISA Threat Landscape 2023.

Splunk’s survey in [The State of Security 2023](#) may give some insights into the impact valuation by the affected parties. Considerable time and resources expended to

clean up the mess is the most reported impact but with significant numbers for competitive position damage, stock price affected, or embarrassment due to public disclosure. Only 4% of respondents say they experienced no significant consequences.

Please note that **46% of respondents mention having suffered SSC attacks**, as many as other common threats like ransomware or DoS. Other surveys, like [this](#) from Capterra, give **61% of companies impacted by an SSC attack in the last 12 months before May 2023**. What most data tells us is that this class of attacks is affecting the software industry.

Effects of Incidents Over the Past Two Years



Source: Splunk, The State of Security 2023.

Many respondents reported that incidents had harmful effects on their company, such as damage to competitiveness, stock price decline, or public embarrassment. Only a small percentage (4%) experienced incidents without significant consequences.

Incidents Experienced in the Past Two Years



Source: Splunk, The State of Security 2023.

Regarding attack types, “supply chain attacks” (impacting 46% globally) refer to successful incidents using that approach. If defined as “discovering and addressing unexploited vulnerabilities in third-party software,” the percentage would be much higher.

⁴Unfortunately, information related to the impact of cyberattacks is often not available or made public. This may change with regulations like EU NIS2 in the future.



Summary of the most relevant attacks

War in Ukraine was a significant driver for cyberattacks, some using the SSC vector. And though 2022 was probably the worst year up to now for attacks targeting identity providers and password managers (with Okta, LastPass, and Entrust among the targets), during 2023 we saw recurrent activity with phishing kits to extract credentials or bypass 2FA.

The following are a few paradigmatic attacks that occurred in 2023.

PyTorch nightly InfoStealer



At the end of 2022, a malicious version of PyTorch's Torchtriton was uploaded into the nightly build server. It was an info stealer. Please note that PyTorch is a popular framework for machine learning. Although quickly identified and removed, it was downloaded [2,386 times](#): many developer machines to care for!

CircleCI incident

The year started with an [incident in the CI/CD CircleCI product](#) (reported on January 4th). A malware deployed in a CI/CD engineer's laptop allowed the bad actors to steal a valid, 2FA-backed SSO session (using session cookie theft), which allowed impersonation as the targeted employee in production systems. As the engineer had the rights to generate access tokens, the bad actors exfiltrated data from production databases and stores, including customer environment variables, tokens, and keys. Although the data was encrypted at rest, the attackers managed to extract decryption keys from a running process. The incident response led to a shutdown of the targeted employee, production access to most employees, rebuilt production servers, revocation of all project and personal API tokens, and all tokens on behalf of customers (bitbucket, AWS, GitHub OAuth). The clean-up was complex and the impact was large, as it needed [full rotation for customer secrets](#) stored in CircleCI.

It is interesting to read the procedure that CircleCI followed for containment, recovery, disclosure, support for customers, and lessons learned. In particular, access to production should be strictly controlled.

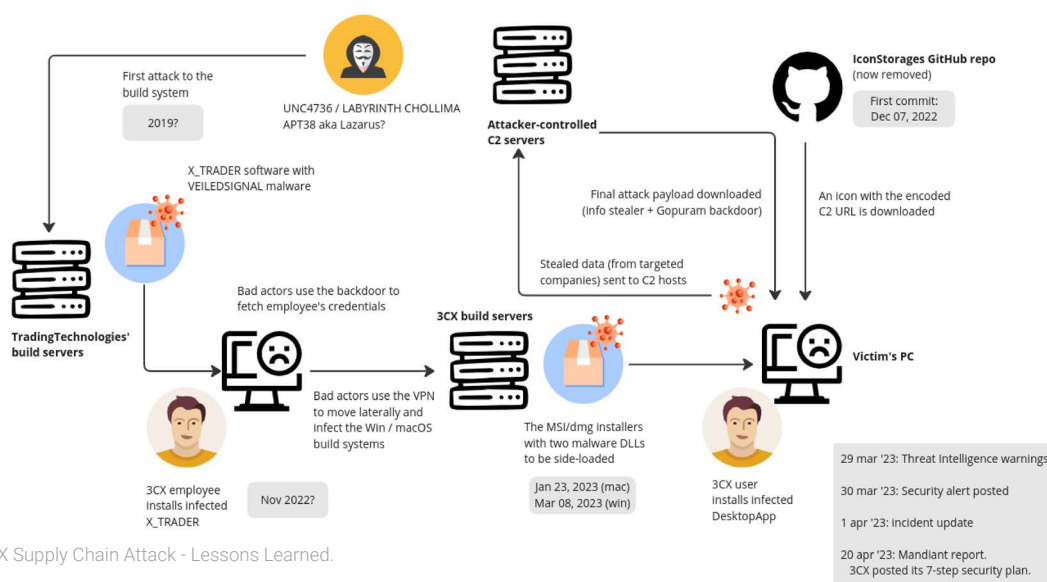
A similar incident was reported on New Year's Eve by Slack, showing that [Slack employee tokens were stolen to download private code repositories](#).



Summary of the most relevant attacks

3CX multi-step attack

By the end of March 3CX, a well-known company providing VoIP and Unified Communications products, was [attacked in a sophisticated software supply chain attack](#), which managed to inject malware into their desktop software. The malware aims at stealing information, but it also drops a backdoor. This seems to be the first case of a multistep supply chain attack: a 3CX employee installed trading software which was the subject of an attack, then injected a backdoor in the employee's computer. The bad actors stole the employee's corporate credentials and used the corporate VPN to access 3CX's macOS and Windows build systems. [Read the 3CX Supply Chain Attack: Lessons Learned post for full details.](#)



MOVEit Transfer data breach

In May 2023, the MOVEit Transfer tool from Progress Software was [abused by exploiting a zero-day SQL injection vulnerability](#)⁵ by the TA505 APT, which used the CL0P Ransomware-as-a-Service for ransom on exfiltrated information. A web shell named LEMURLOOT was installed. Even though the vendor quickly published a patch, this was probably the biggest data leak of 2023. Although not explicitly a supply chain attack, this reminds us that software tools installed on customers' premises could be unintentional trojan horses for cybercriminals.

⁵Who said that SQL Injection was over?



Summary of the most relevant attacks

PyPI temporal suspension of new users/projects

PyPI administrators decided on May 20th to suspend the registration of new users and project names. As the [Incident Report reported](#), "The volume of malicious users and malicious projects being created on the index in the past week has outpaced our ability to respond to it in a timely fashion, especially with multiple PyPI administrators on leave."

The suspension was lifted on the following day, but this shows the avalanche of (mostly typosquatting) attacks done on public package registries this year, and the struggle of key software infrastructures to keep up with the influx of malicious activity.

NPM Manifest Confusion

On June 27th Darcy Clarke, previous staff engineering manager for the npm CLI, posted about [a massive bug at the heart of npm](#), coined as "manifest confusion".

The manifest file displays information describing the artifact archive attributes such as bundled scripts, licenses, and other dependencies. The problem is when the manifest JSON is submitted independently from the attached tarball which hosts the package's `package.json`, using the API. As these two pieces of information are never cross-validated by npm, and many tools use the manifest JSON instead of the `package.json` in the tarball (which turns out to be the "source of truth"), this opens the door for malicious behavior: cache poisoning, installation of unknown/unlisted dependencies, execution of unknown/unlisted scripts, or a downgrade attack.

```
1 {
2   "name": "express",
3   "version": "3.0.0",
4   "main": "index.js",
5   "scripts": {
6     "install": "touch ./bad-pkg-write && echo '\\bad pkg exec!'",
7   },
8   "license": "ISC",
9   "dependencies": {
10    "sleepover": "*"
11  }
12 }
```

Source: VLT. Darcy Clarke

The proof: This package tarball has a different license, and has one dependency and one install script!

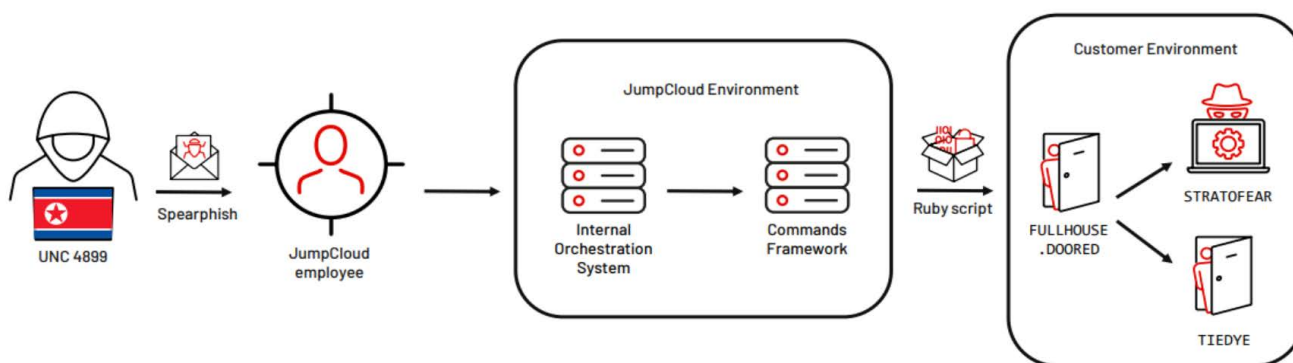


Summary of the most relevant attacks

JumpCloud attack

In late June, a spear phishing campaign by a north-korean group was targeting JumpCloud, a zero-trust directory platform service used for identity and access management. A JumpCloud employee was the foothold for gaining access to deploy a malicious lightweight Ruby script in JumpCloud's Commands Framework. The script, a simple dropper, downloaded a well-known second-stage payload, FULLHOUSE.DOORED, a backdoor, and later deployed other tools like the modular backdoor STRATOFEAR. Mandiant published full details of this [targeted supply chain attack](#).

The incident was notified in [this post](#), and details on the incident were reported via a later [post in the JumpCloud blog](#).



Source: Mandiant, "North Korea Leverages SaaS Provider in a Targeted Supply Chain Attack"

VMConnect campaign

Hiding into apparently useful new packages or typo squats, 24 malicious packages were uploaded to Python's public registry PyPI. Some mimicking Python wrapper modules for VMware vSphere (hence the VMConnect name given to the campaign), in a concerted effort to deceive developers, by implementing the entire functionality of the mimicked modules, with linked GitHub projects that omit the malicious functionality found in the release package. Contrary to common malicious packages, the attackers (linked to the North Korean Lazarus group APT) made many efforts to conceal the packages as legit. This was [reported by ReversingLabs](#) on August 3rd.

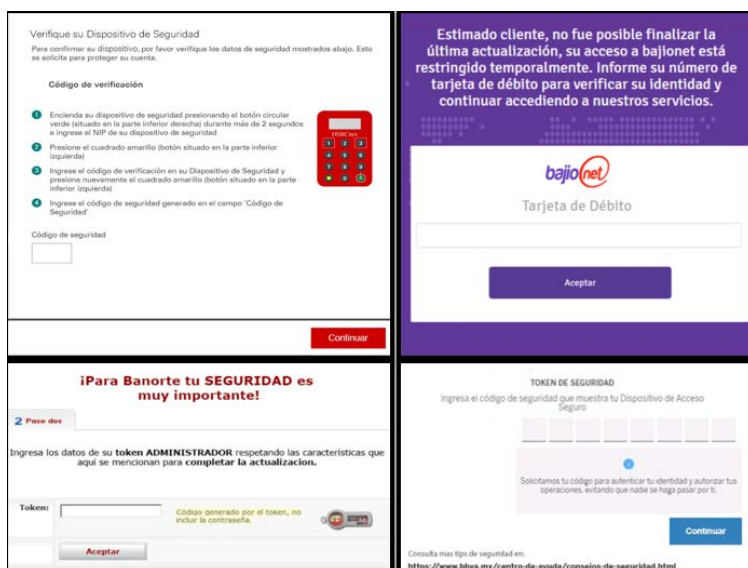


Summary of the most relevant attacks

BBTok Banking Hijacks

Though not exactly an SSC attack, for an example of an adversary (named BBTok) targeting the banking industry in the LATAM region, let's examine the [BBTok trojan attacks](#). More than 40 banks in Mexico and Brazil were the subjects of this campaign. The victim is lured by phishing emails to click on a malicious link that installs via fileless (living-off-the-land) techniques the BBTok malware.

The malware, among other things, can create a dynamic fake interface for capturing the 2FA code to their bank accounts or into entering their card number. As a side note, the cybercriminal gang is cautious: all banking activities are only executed upon direct command from the C2 server.



Source: CheckPoint Research, "Behind the Scenes of BBTok".

Ukrainian War-related Attacks

[According to the NSA](#), Russian APTs targeted Ukrainian and European (non-software) supply chains to disrupt the flow of humanitarian goods and weapons into Ukraine. Attacks focused first on disruption, but in the second half of 2022, they shifted to intelligence-collection operations. Two concrete examples are the purely destructive [Prestige ransomware campaign](#) (and later RansomBoggs) against organizations in the transportation industries, and a modified version of the [GoMet backdoor](#) destined for a software development company whose software is used in state organizations within Ukraine.

Another worrisome example is the distribution of [trojanized installers of the Windows 10](#) operating system distributed via Torrent sites: The installers use the Ukrainian language pack and are designed to target Ukrainian users to conduct reconnaissance and data theft. Based on reports, the victims were 'handpicked' and included Ukrainian government organizations. In another twist, there is news that [Ukrainian radio stations were hacked](#) to spread misinformation about President Zelensky.



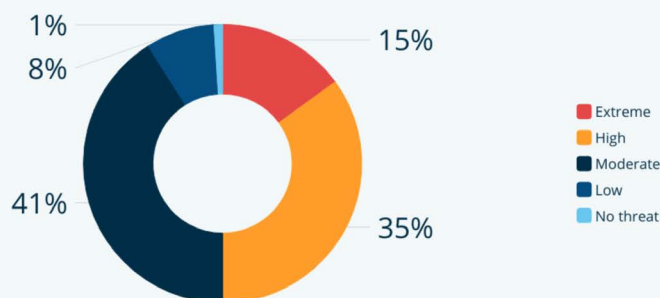
Maturity: Adoption of security frameworks and practices

The gap between perceived risk and reality

Most humans have a cognitive bias (the Dunning-Kruger effect) that makes them overestimate their knowledge or ability in a specific area. Risk assessment is another task we humans perform poorly. So when asked, security professionals probably think their organizations are better prepared against threats than the actual security measures in place would indicate.

As usual with surveys, everything depends on who is surveyed. In a [survey](#) by Capterra, half of the surveyed professionals are highly concerned.

Half of IT professionals say the software supply chain threat is **extreme** or **high**



Source: Capterra's 2023 Software Supply Chain Survey
Q: What level of threat do you believe software supply chain attacks pose to your company?
n: 271



On the opposite side, we observed during 2023 that many organizations do not even know what an SSC attack means, showing fairly basic knowledge of the attacking techniques, the goals for this class of attacks, or the weaknesses that bad actors exploit. Vulnerability handling seems to be the highest concern for many organizations regarding software security, with marginal effort and resources in other parts.

Most security professionals are aware of some of the issues, like dependency typosquatting, secret leaks, or unsafe configurations in IaC templates. However, there is yet a lack of knowledge on CI/CD pipeline vulnerabilities, build runtime security,

detection of anomalies in software infrastructure, or the different attack patterns followed by malicious dependencies. When asked about the tools and processes in place, we found some lack of coverage against many of these threats.



Maturity: Adoption of security frameworks and practices

Do we know what we are doing?

A common claim in the industry is that the labor shortage in cybersec remains a serious problem. Lack of resources leads to being forced to take responsibilities not ready to cope with, burnout, and failed initiatives. Handling a growing pile of vulnerabilities, despite noise reduction, triage, and prioritization⁶, takes most of the time for security-related activities in DevOps teams.

Limited knowledge of SSC Security is the root cause for existing software infrastructures to have a large risk of being successfully attacked in the future. Having personnel with expertise in the field is probably the first goal security officers would embrace.

Are we doing the thing?

The gap between perceived and actual adoption of practices. When you ask any IT security professional how they see the adoption of software security practices in their organizations, and then ask specific questions about concrete practices in place, this overconfidence mismatch stands out. A reality check is necessary, Xygeni found signs of overconfidence, a gap between perceived security in DevOps-related security teams, and reality according to facts. More than two-thirds of organizations expressed confidence that their software does not depend on known vulnerabilities, but 10% reported security breaches due to open-source vulnerabilities in the past year (2022).

Are we doing the right thing?

The CyberSecurity Industry is famous for recommending standards and best practices that are both costly to implement and with a negligible effect on risk reduction. So questions arise: Are there tangible benefits from implementing standard/guideline X? Which practices show the biggest impact on security outcomes? Given the scarce resources my organization can devote to the Sec in DevSecOps, how can I optimize risk reduction without being entombed by an avalanche of best practices and noisy positives from tools?

Operationally, an important part of cybersecurity is about countering subversion, espionage, and sabotage -activities where the defender must be just as adept as the attacker. Many users report that **insider threats** are a big concern⁷ and the source of past incidents, but many do not follow a specific framework for targeting this threat, like the CISA's [Insider Threat Mitigation Guide](#).

⁶Application Security Posture Management (ASPM) is the buzzword that looks for an answer to this problem.
⁷Insider Threat concerns vary widely across sectors and geographical regions.

Maturity: Adoption of security frameworks and practices

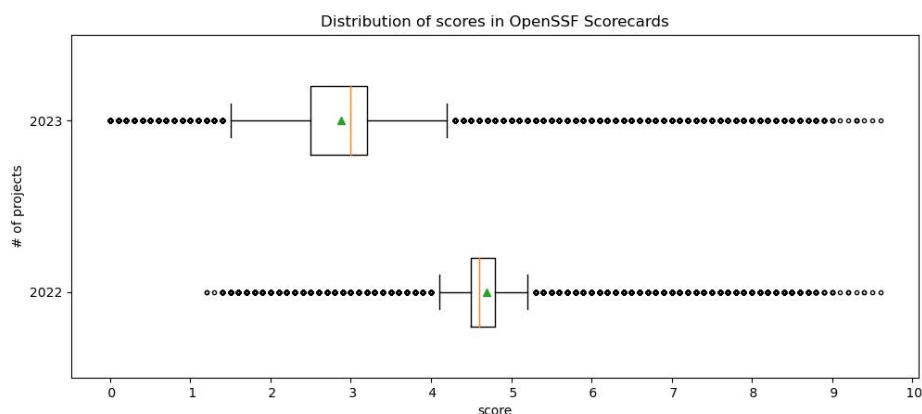
Adoption of security practices in OSS: The OpenSSF Scorecard case

If I put a set of practices in use on my software projects, for example, the [OpenSSF ScoreCard⁸](#), will I improve in risk reduction and lower vulnerability scores? Unfortunately, there are few studies on the topic. (Human) resources are always scarce, and to make informed decisions we need input data.

During 2023 some researchers worked in this area. For example, the study [Do OpenSSF Scorecard Practices Contribute to Fewer Vulnerabilities?](#) presented the unexpected result that **packages with higher security scores had more vulnerabilities!** A possible explanation of the increase in reported vulnerability count while increasing in security score could be that the selected packages are used frequently by other OSS packages. Since more clients utilize these packages, there is a higher likelihood that the package will be tested or attacked, and there will be more reported vulnerabilities.

The study highlights 4 practices ('Maintained', 'Code Review', 'Branch Protection', and 'Security Policy') as the most important that practitioners can adopt to improve package security outcomes by minimizing vulnerabilities.

If we look at the OpenSSF ScoreCard⁹ score and how it changed in the last year, we see another surprising fact: in general, **the score decreased significantly, from a median of 4.6 to a median of 3.** And while many popular projects have high scores above 9 which was kept from last year, which is good news, **75% of the OSS projects have a score below 3.2**, a worrisome value.



Due to the high adoption of the Scorecard in the open-source community, the analysis of facts for OpenSSF results deserves a future post from Xygeni.

⁸ The OpenSSF Scorecard project computes automated scores of 18 security practices, aimed to help developers make better decisions about security when consuming open source projects

⁹ Xygeni is working on a more comprehensive analysis of the 2023 data for the Scorecard project.



Maturity: Adoption of security frameworks and practices

Are we doing the thing right?

1. Open source security and dependency handling.

As most security professionals understand that this is the most frequent avenue for SSC attacks, initial attempts to improve on SSCS often start here. Some well-known techniques are Version pinning¹⁰, registering an organization's scope in public repositories, checking in malicious packages blacklists, or better using a whitelist of vetted, allowed package versions. SCA tools traditionally considered vulnerabilities, but are starting to pay attention to the large number of malicious packages pushed this year. Internal package registries offer whitelisting allowed package versions and the possibility to block or put in quarantine versions that might have critical vulnerabilities or malware. Provenance checking will be a logical next step.

2. Change control.

Controlling changes in source code, build files, IaC templates, CI/CD pipelines, dependencies descriptors, image manifests and other critical assets is not new, and most organizations think that they are doing it when asked. Do not assume anything without backing data! Commit signing, code reviews, branch protection rules, PR approvals, code tampering checks, etc. are standard techniques for change control, and many organizations started to check that they are indeed active everywhere. But beware of the dog! Basic measures, like branch protection rules, are not as common as you may think: [According to GitHub](#), the proportion of top 1000 public projects with branch protection raised from 40% in 2020 to a mere **60%** in 2023 ...which is far from ideal.

3. Mandatory Multi-Factor Authentication (MFA)

Mandatory Multi-Factor Authentication (MFA) was established this year in popular SCM and CI/CD systems, like [GitHub](#)¹¹. Others, like GitHub, keep it as an open issue, with MFA optional. Rather, organizations are increasingly integrating SCM and CI/CD platforms into single sign-on with their IdP, and enforcing MFA at the IdP side, without needing direct enforcement from the tool vendor.

4. Avoiding secret leaks.

A secret leak is [one step forward to the disaster](#): many software supply chain incidents started with the unintentional leak of an important credential. Many organizations started this year to scan for secrets in their code repositories. Secret leak prevention seems to be a trivial feat, but the real world is complex.

5. Inventory.

The application sprawl and loss of governance a well-known issues. With the software infrastructure, the same happens. Many security professionals reported to be building or showed their interest in building, an inventory of assets in the software infrastructure. Such inventory includes assets like build & deploy pipelines, systems and tools, and code repositories, linked to users and their permissions, with enough detail to provide key information for risk assessment and impact analysis. Remember: to be useful, the inventory needs to be continuously updated.

¹⁰ Version pinning and frequent updates for security patches look contradictory, but they do not. You should update vulnerable versions with fixed ones for known vulnerabilities, but without letting malicious versions be installed automatically.

¹¹ GitHub first enrolled all maintainers in the top-100 packages on the npm registry, then the top-500, then the "high impact" packages, to end with all code contributors to github.com by the end of 2023.



Evolution of Standards and Regulations

Regulatory frameworks in the software supply chain play a vital role by setting standards that the organizations in the chain must adhere to¹². These regulations help ensure that technology and processes meet an established level of data protection, privacy, and overall security. Established by regulatory or industry bodies, compliance regulations are sets of **goals, rules, standards, and guidelines** to ensure that the software along the chain has an acceptable risk, maintains the trust of the stakeholders and agents involved, and protects privacy and intellectual property.

The regulatory framework for the SSC is under construction. With highly different intensities across regions, it seems that the US has the most mature framework, with the European Union lagging. Other regions, like Asia and the Pacific, and relevant countries to the software industry like Japan, Canada, Australia, India, and Germany have advanced their SSC regulation in the past years. Meanwhile, industrial giants like China have a regulation corpus shrouded in mystery.

How have standards and regulations evolved over the years, in different regions?

US and America



In March 2023 the [National Cybersecurity Strategy \(NCS\)](#) was published. The NCS addresses key areas in the form of five strategic pillars, like critical infrastructure (pillar one). It mentions SBOM alignment with Executive Order 14028 launched after the SolarWinds attack. The most groundbreaking part is its Strategic Objective 3.3 “Shift Liability for Insecure Software Products and Services”. Organizations unable to demonstrate that security is inherently integrated into their software design will face increased responsibilities and liabilities, with the load put on the “most capable of taking action” agent: “We must begin to shift liability onto those entities that fail

to take reasonable precautions to secure their software while recognizing that even the most advanced software security programs cannot prevent all vulnerabilities. Companies that make software must have the freedom to innovate, but they must also be held liable when they fail to live up to the duty of care they owe consumers, businesses, or critical infrastructure providers. Responsibility must be placed on the stakeholders most capable of taking action to prevent bad outcomes, not on the end-users that often bear the consequences of insecure software nor on the open-source developer of a component that is integrated into a commercial product. (...).”

¹² Many costly organizational practices are motivated by pure compliance with regulatory frameworks that apply for the organization’s sector. Compliance is a necessary evil, and a central concern for most CISOs.



Evolution of Standards and Regulations

[The NCS Implementation Plan](#) was released in July, with the intent of putting a greater burden on cybersecurity by major organizations, and the promotion of investments. The document includes 68 initiatives each with the responsible agency and contributing entities, and expected completion date. Many of the initiatives aim at SSCS. Undoubtedly the NCS will have a significant impact on many organizations worldwide.

The NIST [Secure Software Development Framework](#) or **SSDF** (NIST SP 800-218) has undergone a major transformation since its inception in 2017. Though the current 1.1 revision was unveiled in February 2022, many **SSDF compliance deadlines** for government suppliers set by CISA had passed during 2023. At the moment, SSDF compliance is mandatory for companies that wish to sell to U.S. government entities, but it is recommended for organizations to move toward SSDF compliance, as the framework may be adopted worldwide in software development.

In April 2023, the [Secure Software Self-Attestation Common Form](#), was released for comments. This self-attestation form identifies the minimum secure software

development requirements a software producer must meet, and attest to meeting, before their software may be used by US Federal agencies. Software producers attest via this form that the software they produce was developed in conformity with specified secure software development practices, aligned with the NIST SSDF practices and tasks.

In September 2023 CISA announced its [Open Source Software Security Roadmap](#), which lists strategic goals and objectives for enhancing the security of open source software, with a focus on US federal agencies. Many objectives are under construction in the industry: to develop a framework for OSS risk prioritization (O2.2), to foster security education for open source developers (O4.2), to publish guidance on OSS Security Usage BPs (O4.3), or to foster OSS vulnerability disclosure and response (O4.4).

The US Securities and Exchange Commission (SEC) made effective on Sept 5, 2023, the "[Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure](#)" rule. It raises the bar for enterprise cybersecurity with new disclosure and management rules. It touches SSC incidentally.

European Union (EU)



The main regulation related to SSC is the [NIS2 Directive](#)¹³, which entered into force in early 2023, with member states required to transpose it into national law before October 2024. Most organizations operating in member states have specific requirements, with businesses identified by the Member States as operators of essential services in

the above sectors required to take appropriate security measures and notify relevant national authorities of serious incidents. Key digital service providers, such as search engines, cloud computing services, and online marketplaces, have to comply with the security and notification requirements under the Directive.

¹³ is "Directive on measures for a high common level of cybersecurity across the Union".



Evolution of Standards and Regulations

NIS2 indicates that those covered should consider the vulnerabilities specific to each direct supplier and service provider and the overall quality of their suppliers and service providers' cybersecurity products and practices, including their secure development procedures. In particular, the obligation to assess/predict how a given product will be developed is an organizational challenge for entities that do not have sufficient resources. Another obligation under the NIS2 Directive is the need to take into account the results of coordinated security risk assessments of critical supply chains.

For sure EU financial entities and their IT providers have worked this year on the [Digital Operational Resilience Act](#) (DORA), which will enter into force in January 2025.

A milestone this year was the [EU Cyber Resilience Act \(CRA\)](#), drafted in 2022: On 30th Nov 2023 the EU members finally reached a political agreement on the CRA, but the technical details are in progress¹⁴.

CRA introduces mandatory cybersecurity requirements for hardware and software products, mainly focusing on the manufacturers, ensuring that they are designated and manufactured with security in mind. These requirements cover aspects such as security by design, secure development processes, vulnerability management, and patch management.

A lifecycle approach is emphasized, where manufacturers remain responsible for the security of their products across their entire lifespan, including obligations for security updates, communication of incidents, and collaboration with cybersec authorities. Additionally, promotes transparency and accountability by requiring manufacturers to provide clear cybersec information about their products (which points without a doubt to things like SBOM and software attestations). A certification scheme will be mandatory for high-risk products in critical infrastructures.

In 2024 we will watch how the technical rules of the CRA are developed.

Other regions and countries



Some standards and guidelines need less consensus than other regulations, so they can be agreed upon by a large set of agencies worldwide. An example is the joint guide [Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software](#) ("Secure By Design" for short), which was published in April and updated in October. This product was led by CISA but joined

the FBI, NSA, and cybersecurity authorities of Australia, Canada, UK, Germany, Netherlands, New Zealand, Czech Republic, Israel, Singapore, South Korea, Norway, CSIRT Americas, and Japan. This is good news as an example of global collaboration and as a confirmation of the trend that the burden of software security should not rely solely on the user but mainly on the manufacturers.

¹⁴ The CRA, at least, recognized a fact: "The current EU legal framework does not address the cybersecurity of non-embedded software"

Evolution of Standards and Regulations

A note on Spain: Spain mainly operates under the EU regulatory corpus and specifically the [application of the EU NIS2](#) directive. The Electronic Administration is regulated by the Esquema Nacional de Seguridad (ENS), amended in 2022, and the scope of the ENS concerning NIS2 should be defined. With no specific local regulation for the SSC, it is expected to transpose the directives from the EU during 2024, notably NIS2 and possibly the CRA.

In summary, **regulation is under construction**, with some common ideas despite the regional differences:

1. The need for defined processes to address cybersecurity incidents and to communicate them to a central operator.

2. That software manufacturers should be accountable for their products and keep most of the burden for software security.
3. The gradual assimilation of the *secure-by-design* and *secure-by-default* principles on software.

Though specific to AI and not directly related to SSC, on October 30, 2023, the White House published an [Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence](#). The EU was pioneering the “trustworthy AI” with the AI Act announced in April 2021 (but which needed more than two years and a half to reach a political agreement). This leads us to how AI burst into the software supply chain security landscape.



The emergence of AI



Artificial Intelligence (AI) and Machine Learning (ML) can be seen as disruptors and buzzwords simultaneously. They refer to technologies being actively developed long before the debut of ChatGPT in Nov 2022, which moved AI from industry and academia to mass media (no pun intended). That event alone put AI in the headlines, opening for some pundits the Age of AI. At least we all can agree that the growth of Generative

AI in 2023 was explosive.

After many warnings, lawsuits, and supposed breakthroughs towards Artificial General Intelligence, Biden signed the aforementioned executive order. There is a lot to digest here. But AI might be used for the good and the bad. Terms like “reliability” and “explainability” are now under the umbrella of [Trustworthy AI](#).



The emergence of AI

The AI wave attracted many security vendors during 2023 to add some “AI touch” to their products. Nonetheless, AI is set to play a critical role in the future of software supply chain security. Some potential applications for AI and ML in SSC could include:

AI-Enabled Threat Intelligence

As the threat landscape evolves, organizations will increasingly rely on AI to detect and respond to potential security threats. AI-enabled threat detection systems can analyze large amounts of data in real-time, identifying potential vulnerabilities and risks before they can be exploited. This will help organizations to protect their software supply chains and prevent cyber attacks.

Risk Assessment for SSC Actors

AI can evaluate the security posture of partners in the supply chain, assessing their overall risk profile, vulnerabilities and weaknesses, and compliance with security standards. By analyzing their security practices, policies, and incident history, AI models can provide organizations with insights into potential security gaps within their supply chains, allowing organizations to make informed decisions about their supplier relationships, and ensuring that their supply chains are resilient to external threats.

Anomaly Detection in Code Repositories

AI algorithms can systematically comb through massive codebases. The ability to recognize patterns and anomalies, even in intricate code structures, may identify suspicious segments that could harbor malicious code injections or vulnerabilities.

Vulnerability Assessment and Prioritization

Organizations need to fight the too-many-vulnerabilities syndrome. ML models, trained on extensive vulnerability data, can accurately assess the severity of identified security flaws. Each raw vulnerability is put into context, considering factors such as the affected software components, the likelihood of exploitation and if the vulnerabilities are exploited in the wild (“exploitability”), if the vulnerable parts of third-party components are used (“reachability”),

and the potential damage caused. By prioritizing these vulnerabilities based on their contextualized risk level, teams can focus on the most critical threats, ensuring that resources are used effectively.

secret leak is one step forward to the disaster: many software supply chain incidents started with the unintentional leak of an important credential. Many organizations started this year to scan for secrets in their code repositories. Secret leak prevention seems to be a trivial feat, but the real world is complex.

Predictive Analytics

Predictive Analytics for SSC Risk Management. Integrating AI into predictive analytics will allow organizations to identify and mitigate potential risks in their software supply chains before they occur. By analyzing historical data and trends, predictive analytics can help organizations forecast potential risks and take proactive measures to prevent them.

Intelligent Remediation

Security flaws, especially reported vulnerabilities, are outpacing remediation efforts, overwhelming developers. Simple dependency version bump remediation was a first but insufficient step towards assisted remediation. Future AI-powered remediation tools will help DevOps teams quickly resolve potential security issues in software supply chains.

Compliance Reporting¹⁸

Integrating automation and AI will also make it easier for organizations to maintain compliance with regulatory requirements. By automating the reporting process, companies can ensure they meet all necessary compliance requirements with less manual effort.

¹⁵ Compliance Reporting is the process of presenting information to auditors that show that a company or organization is adhering to relevant regulations..



The emergence of AI

Code Review Automation

Code review is a key technique in modern software. But manually checking for security flaws, vulnerabilities, weaknesses and malicious code in large codebases is not effective anymore. AI will improve the code review process, probably by focusing human reviewers on areas that require closer scrutiny. This guidance has already started at SAST tools that added AI to the existing rule-based scans, to limit false positives and to direct developers to the root cause for a group of security flaws.

SBOM / Attestation Assessment

Generating SBOM (including security-related information like vulnerabilities and exploitability) or software attestations like SLSA Provenance is the easy part, which current

tools do reasonably well. Using it for validation of the corresponding software on the software consumer's side is more difficult. The mechanical part (integrity and origin validation of signatures and digests for software artifacts) could be well resolved, but assessing the risk and security posture of the software, as well as deciding to deploy it, require abilities that only a well-trained human or AI algorithm could have.

Phishing Attack Detection

Remind that developers and DevOps teams are the first target for SSC attacks for intrusion into the software pipelines. Spear phishing is a common attack technique for that goal. AI-powered tools can analyze email content, user interactions, and network behavior, identifying anomalies and suspicious patterns that are indicative of phishing attempts, which could be blocked.

On the bad side, actors started weaponizing AI during 2023, and here are some alarming examples:

AI-powered reconnaissance

Pen-testing tools (used for the bad) can scrape websites, social media platforms, forums, and other online sources to extract relevant data. With the ability to recognize natural language in user comments, attackers may extract actionable intelligence from textual sources. Tools like [GTP_Vuln-analyzer](#), capable of doing network vulnerability analysis, DNS enumeration, and also subdomain enumeration, will expand from the proof-of-concept stage.

Highly personalized Spear Phishing

Repurposed AI models like [WormGPT](#) are now seen in the wild. They help with target selection and then analyze email, personal preferences, and social media messages to craft customized phishing messages, increasing the likelihood of tricking recipients into revealing sensitive information through multi-factor authentication. Generating convincing phishing emails is the first step. Highly convincing fake audios for vishing and even deepfake videos will certainly be seen more often for targeted phishing attacks.

Crafting attacks with the help of LLMs

Many LLMs like ChatGPT have limitations on 'inappropriate' content and do not respond to intrusive prompts. But in dark web forums, there are tutorials to jailbreak the LLM. The post [How AI tools drive effective penetration testing](#) by CQR is an example. Generative AI can generate new malware variants or generate exploit code for a vulnerability as well. FalconFeeds.io reported in July 2023 that in hacker forums, for-sale tools like [XXXGPT](#) or [Wolf GPT](#) were announced.

CAPTCHA bypassing

According to this [report by Arkose Labs](#), certain Cybercrime-as-a-Service (CaaS) offerings provide "Solver Services" to help fraudsters bypass CAPTCHAs. As some generative AI tools are now multimodal (named [LMM](#) for that reason), they can integrate text (for translation and language modeling), image (for object detection and image classification), or audio (for speech recognition). Many traditional CAPTCHA schemes may be vulnerable to the new solver services provided by advanced bad bots.

As with any software, AI tools are also targets for SSC attacks. A [cache deception attack](#) against ChatGPT due to a bug in the `redis-py` open source library for the Redis cache database, with a [critical account takeover](#) vulnerability found later. Data poisoning for training data is another concern for GenAI models.



The Future: What We Expect for 2024



Looking ahead, the threat of supply chain attacks is expected to continue to increase in the coming years.

How many organizations will experience an attack?

Analysts like Gartner predict that by 2025, [45% of organizations worldwide](#) will have experienced attacks on their software supply chain, a 3x increase from 2021. Many analysts raise this figure even higher, as in surveys like Capterra's [61% of the subjects reported being attacked](#) in the last year.

Threats are wider and deeper. Organized criminal groups¹⁶ will engage in cybercrime, notably cyber-enabled crime, like cyber extortion, online banking scams, and fraudulent gambling. Such criminal groups may leverage more mature Cybercrime-as-a-Service offerings, with less fear of police and law enforcement than traditional cybercriminals. Additional instances of AI-powered tools will be tailored for advanced phishing and vishing, bypassing controls like CAPTCHA or 2FA. We will watch more attacks targeting CI/CD systems to distribute ransomware and data theft trojans using popular software.

More transparency on Incident details. Many incidents that were not disclosed will have to be, due to current regulations. The details on how the attackers breached the software infrastructure will be more transparent, so the industry may gather more “lessons learned” and have

better insights on how to protect themselves. Wishful thinking?

Limits on insurance coverage. Cyber Risk Insurance may begin including excesses and other limits on coverage for SSC attacks, in line with previously introduced limitations on other incidents like ransomware. This will be a sign that attacking the SSC is getting mainstream.

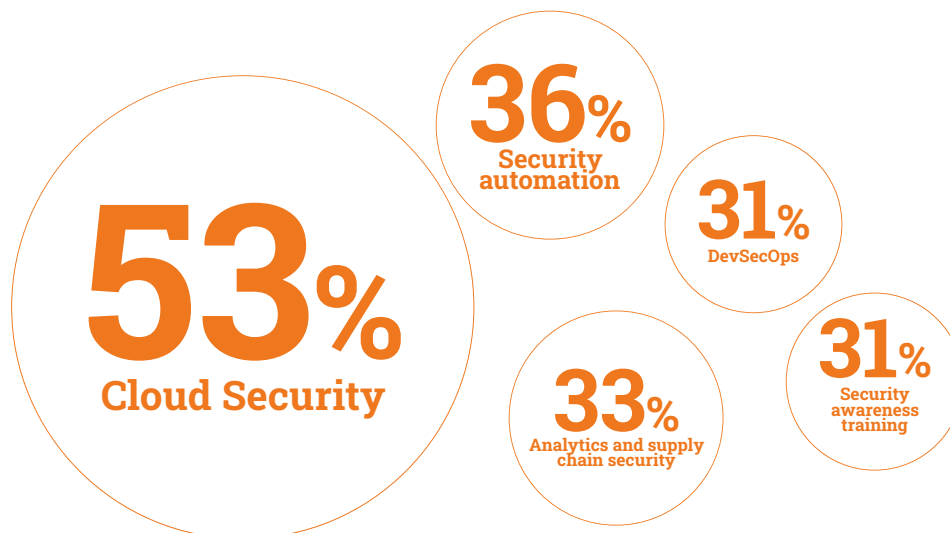
Changes in SBOM and Software Attestations. SBOM is a sort of soft inventory translating the physical bill-of-materials to software, but to be operational, many gaps need to be closed: continuous generation (on each software delivery), storage & distribution, security context, searching and summaries, policy enabling for automation...

NIST is currently developing guidelines for SBOMs, which could become a requirement for software vendors. SBOM (and software attestations) will begin to include more security context, like VEX. Infrastructure like container images and package registries could become the preferred stores, as the SBOM/attestation could be co-located with (or even embedded into) the software product they reference. Automation will increasingly use SBOM and attestations for enhanced controdelivery/deployment according to security policies.

¹⁶We are not talking here about APTs, but of Camorra, 'Ndrangheta, chinese triads, etc.

Evolution of Standards and Regulations

SSCS enters the plan. [Splunk's 2023 survey](#) gives us clues about top security initiatives:



One out of three security officers mentioned the security of the software supply chain as one of the three top priorities. This is in sharp contrast with previous years' data.

Technological advancements. Aligned with the *security-by-design* and *security-by-default* trend, technological advancements and increased awareness of security risks may mitigate some of these threats. Adopting zero-trust architectures could help limit the impact of supply chain attacks, by restricting access to sensitive data and resources. The integration of automation and artificial intelligence (AI) is set to play a critical role in the future of software supply chain security.

BTW, I was showing my daughter the [famous scene from Amadeus movie where Mozart supposedly dismounts Salieri's Little March](#), then to my surprise the link to the Xygeni video appeared ...)



References

Other Summary Reports

- CrowdStrike - [Global Threat Report 2023](#)
- ENISA - [Threat Landscape 2023](#)
- GitHub - [The state of the Octoverse 2023](#)
- Snyk - [2023 Software Supply Chain Attack Report](#)
- Sonatype - [9th Annual State of the SSC](#)
- Splunk - [The State of Security 2023](#)

The Attack Landscape

- [Charting China's Climb as a Leading Global Cyber Power](#), in Recorded Future by Insikt Group
- BBTok 2023 attack: [Behind the Scenes of BBTok: Analyzing a Banker's Server Side Components](#), by CheckPoint Research.
- JumpCloud attack: [North Korea Leverages SaaS Provider in a Targeted Supply Chain Attack](#), by Mandiant, Jul 24, 2023.
- [Q1 2023 Evolution of Software Supply Chain Security Report](#), by Phylum.
- [Vishing Statistics 2023](#), by Keepnet Labs.

Standards and Regulations

- CISA - [Open Source Software Security Roadmap](#)
- CISA - [Secure Software Self-Attestation Common Form](#)
- CISA - [Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software](#)
- EU - [Cyber Resilience Act](#)
- EU - [Digital Operational Resilience Act](#)
- EU - [NIS2 Directive](#)
- NIST - [Secure Software Development Framework](#)
- US SEC - [Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure](#)
- White House - [Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence](#)
- White House - [National Cybersecurity Strategy](#)
- White House - [NCS Implementation Plan](#)





Software Supply Chain Security Retrospect: Shaping a Safer 2024

by Luis Rodríguez,
CTO & co-Founder of Xygeni

Contact

Get in touch today!

 www.xygeni.io

 <https://www.linkedin.com/company/xygeni>

 <https://twitter.com/xygeni>