STRIDER

LYING IN WAIT

Uncovering Hidden Threats in Open Source Software Through a New Contributor-Centric Risk Model

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Open source software (OSS) has become the backbone of modern digital infrastructure, underpinning critical systems in both the private and public sectors. However, as OSS adoption by business and government entities has accelerated, so too has its exploitation by state-sponsored cyber threat actors.

This report explores how adversarial nation-states, like the People's Republic of China (PRC), Russia, and North Korea, are infiltrating OSS ecosystems to advance their respective national interests and objectives.

Drawing on proprietary open-source intelligence collection and analysis, this report presents evidence that OSS platforms, such as GitHub, are infiltrated by malign cyber threat actors, including advanced persistent threat (APT) groups. These actors can discreetly embed themselves within development communities, contributing code that is influencing critical software supply chains.

This report introduces a contributor-centric risk model for open source software—an emerging approach to software supply chain security that shifts the focus from solely examining what the code does to also understanding who is behind it. By analyzing contributor behavior, affiliations, and activity patterns across open source platforms, Strider's latest tool—Open Source Software Search—helps organizations uncover hidden risks that traditional vulnerability scans completely miss. With deeper visibility into the contributors writing and maintaining open source code, organizations can make more informed decisions about the software they choose to trust.

INTRODUCTION

Open source software (OSS) forms the foundation of today's digital infrastructure, powering everything from enterprise applications to critical government systems. With most enterprise applications and codebases relying on OSS components, global dependency on community-driven code is both unprecedented and expanding.

> **This widespread adoption, however, has outpaced the evolution of corresponding security practices. The inherent transparency, decentralized governance, and volunteer-driven nature that define the OSS ethos now expose the ecosystem to new forms of manipulation, particularly by highly trained, well-resourced advanced persistent threat (APT) groups enabled by adversarial governments.**

Historically, the OSS community operated on a foundation of mutual trust, good-faith collaboration, and open exchange. But the realities of our geopolitical situation require new approaches to protect that open environment. State-sponsored cyber threat groups, like APT41 (PRC), Lazarus Group (North Korea), and Cozy Bear (Russia), have exploited open source platforms such as GitHub to further their governments' strategic objectives. These actors have become active contributors who subvert the openness of these platforms to infiltrate the software supply chain, steal sensitive data, and enable long-term cyber-espionage campaigns.

Unlike financially motivated cybercriminals, APTs are state-directed, well-resourced, and ideologically aligned with their government's geopolitical goals. Their presence in OSS ecosystems demonstrates the nature of our new geopolitical reality—one where corporations are on the frontlines and the vectors for injecting system-wide risk into our societies. Through subtle code contributions, the insertion of backdoors, and the exploitation of trusted software components, these malign actors are embedding persistent threats into software pipelines that are used by corporations, developers, and governments alike. GitHub, the world's largest host of source code, has become a primary target and tool in this new paradigm.

Several high-profile incidents in recent years illustrate this trend. These incidents underscore the critical need for organizations to implement robust security measures, including regular code reviews, continuous software dependency monitoring, timely patch management, and increased collaboration between insider threat and information technology leaders in both the private and public sectors to share threat intelligence and best practices.

2024

PYPI SUPPLY CHAIN ATTACK

A supply chain attack targeted the *Python Package Index* (PyPI), a central repository for Python developers. Attackers uploaded malicious packages containing "JarkaStealer," malware designed to exfiltrate sensitive information from infected systems, that were disguised as legitimate tools and promoted through social engineering tactics (including AI chatbots offering assistance). Japanese cybersecurity officials attributed this attack to the Lazarus Group (North Korea).

XZ UTILS BACKDOOR INCIDENT

Beginning in November 2021, an individual operating under the alias “Jia Tan” (also known as “JiaT75”) contributed to *XZ Utils*—a widely used open source data compression software—and gradually built trust within the community. In 2024, Jia Tan inserted a malicious backdoor into the software after maintaining a high level of operational security for a lengthy period and gaining co-maintainer status. The identity of Jia Tan, and the nation-state group behind this attack, have yet to be identified.

SOFTETHER VPN EXPLOITATION BY PRC-ALIGNED APTS

PRC-aligned APT groups utilized *SoftEther VPN*, an open source, multi-platform VPN software, to maintain access to victims' networks. *SoftEther*'s ability to use HTTPS for establishing VPN tunnels allowed the attackers to bypass firewalls and blend into legitimate traffic, complicating detection and mitigation efforts.

2023

PLUSHDAEMON APT ATTACK ON SOUTH KOREAN VPN PROVIDER

A previously undocumented PRC-aligned APT group, dubbed “PlushDaemon,” conducted a supply chain attack targeting a South Korean VPN provider. The attackers deployed a sophisticated backdoor named “SlowStepper,” utilizing a multi-stage DNS command-and-control protocol to facilitate espionage activities.

2021

LOG4SHELL VULNERABILITY EXPLOITATION

The discovery of the *Log4Shell* vulnerability in the widely used open source logging framework *Log4j* exposed numerous organizations to potential exploitation. The attackers leveraged this vulnerability to execute arbitrary code, leading to data breaches and system compromises across various sectors. Cybersecurity firms and government agencies observed that APT groups from the PRC, Iran, North Korea, and Turkey actively leveraged this vulnerability to infiltrate networks and conduct various malicious activities.

Cybersecurity experts estimate that the *Log4Shell* cost organizations more than $90,000 in incident response support per incident, with total industry-wide costs reaching into the billions. One U.S. federal agency dedicated more than 33,000 staff hours to its response.

More than half of corporate security teams spent weeks or longer remediating the issue, working nights and weekends. Two years after the initial exploitation, 72% of organizations were still detecting active exploitation events.

IMPACT ON ORGANIZATIONS

The exploitation of OSS ecosystems by cyber threat actors has profound implications for organizations:

WIDESPREAD EXPOSURE

Given the pervasive integration of OSS in enterprise applications, a single vulnerability can have cascading effects across multiple industries and sectors.

SUPPLY CHAIN COMPROMISE

By targeting widely used open source components or repositories, attackers can infiltrate the software supply chain, leading to the distribution of malicious code to numerous unsuspecting organizations.

OPERATIONAL DISRUPTION

Successful exploitation can result in significant operational disruptions, data breaches, unauthorized access to sensitive information, and reputational damage, undermining organizational integrity and trust.

RESOURCE DRAIN

Organizations are compelled to allocate substantial effort to identify, mitigate, and remediate vulnerabilities, diverting resources from core business functions and innovation.

TACTICS, TECHNIQUES, AND PROCEDURES

Malign cyber threat actors are motivated and well-resourced adversaries who employ various tactics, techniques, and procedures (TTPs) to leverage OSS-sharing platforms to advance their national strategic objectives. **These TTPs are sophisticated and intentionally designed to obfuscate malicious actors and their activities within victimized networks.**

Introducing Exploits into Contributed Code

Threat actors have been observed capitalizing on OSS platforms to target developer workstations by compromising publicly available code through the implementation of a malicious backdoor disguised as a troubleshooting tool that lets attackers maintain persistence. Once inside the target environment, threat actors can wield relevant TTPs to access sensitive and proprietary information.

One observed technique, known as "persistence," involves intruders maintaining access to a compromised system in pursuit of long-term strategic goals. In one case, a company affiliated with PRC state-owned enterprise Shanghai Zhenhua Heavy Industry Co., Ltd. (ZPMC) drew scrutiny after it was exposed installing unauthorized cellular modems to the cranes it supplies to U.S. ports. Modems can serve as a discreet and deniable means for threat actors to linger within systems and exfiltrate critical data over extended periods of time. A U.S. government report in September 2024 identified ZPMC as a national cybersecurity threat.

Extracting Organizations' Leaked Information

PRC APT Silk Typhoon has been observed leveraging leaked corporate passwords on public repositories to gain quiet entry into organizations' internal networks.

Co-Opting OSS Platform Collaboration Features

Since 2022, a PRC-based cyber threat actor has been manipulating GitHub's legitimate collaboration features by uploading code to a repository, then creating a pull request or issuing a comment containing a Python-based back door. This creates a stealthy reverse shell, allowing remote access to compromised systems, which leads to mass data exfiltration of sensitive data.

Mining for Publicly Available Exploits

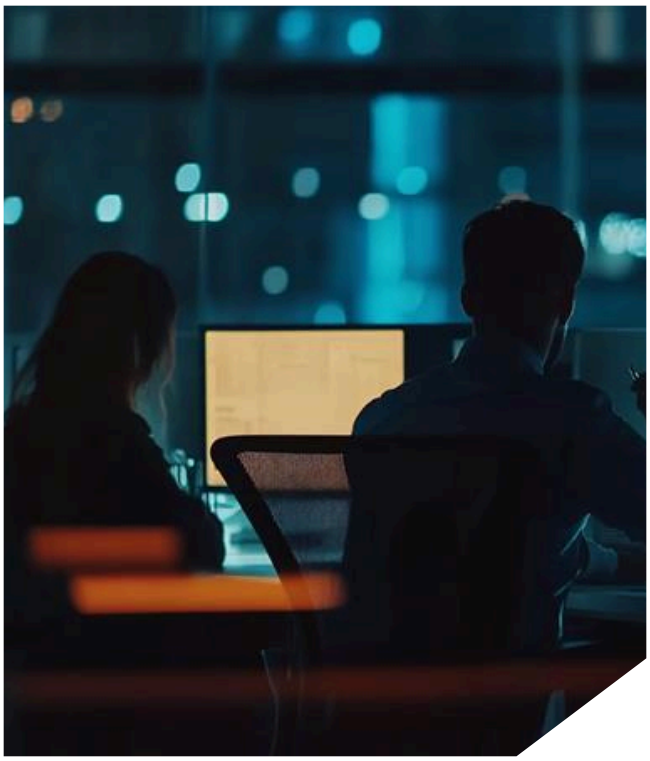
PRC-based APT groups have been observed mining GitHub for publicly available exploits such as zero-days and proof-of-concept exploits and vulnerabilities disclosed by state-linked researchers and entities.

Weaponizing OSS Platform Features

APTs, including PRC-based groups, have previously launched a distributed denial of service (DDoS) attack to disrupt OSS development on GitHub utilizing a combination of attack vectors. The attack featured a technique involving "man-on-the-side" injection whereby hijacked HTTP connections redirected unsuspecting web users to GitHub—disrupting service to specific pages for GitHub users—without exploiting a GitHub feature.

INDIVIDUALS BEHIND THE CODE

Traditional approaches to software security focus on code, but the individuals behind the code also deserve attention. **Strider used its new Open Source Software Search tool to analyze open source contributors and uncover affiliations to known entities of concern.**



CASE STUDY 1:
Risky contributors to *openvino-genai*—the code making it possible to run generative AI models on consumer-grade devices

With more than 100 contributors, the *openvino-genai* repository sits at the heart of modern AI inference workflows. OpenVINO's toolkit has been downloaded more than one million times, demonstrating growing popularity. Strider's analysis found that more than 21% of its contributors were flagged with non-zero risk scores, including several tied to high-risk ecosystems.

Strider rates contributors on a scale of one (low) to four (high) in terms of risk due to connections with high-risk entities. Two contributors, in particular, stood out:

- **as-suvorov**, with a risk score of four, has made 55 commits (changes made to a project's files), remaining active as recently as May 2025.
  - as-suvorov serves as a "maintainer," his 18 code reviews indicate he is a gatekeeper who decides what code from other contributors gets included in the final product. He also has infrastructure control, which means his work on the project's build, test, and release automation gives him the ability to change how the software is assembled and distributed. With this level of access, as-suvorov is able to influence not just the source code, but the integrity of the entire build and release pipeline.

- **sbalandi**, with a risk score of four, has made 42 commits, with their latest contribution in June 2025.
  - sbalandi also serves as a maintainer; her 36 code reviews make her one of the primary gatekeeps for the project. Her focus on the core "engine" and the Python API gives her control over the software's most critical features and how they are presented to most users.

Strider's proprietary intelligence platform surfaced real-world affiliations between these contributors and high-risk entities, connections that are invisible through public GitHub metadata alone.

as-suvorov, identified as “Suvorov,”[1] was formerly employed as a full-stack developer at MFI Soft, a Russian software company controlled by Citadel Group (a Russian technology company linked to oligarch Alisher Usmanov), that occupies 60-80 percent of the Russian System for Operative Investigative Activities (SORM) production market. Both MFI Soft and Citadel were sanctioned by the U.S. in 2023 for operating in Russia’s technology sector. MFI Soft has also conducted a significant amount of work on behalf of the Federal Protective Service's (FSO) Special Communications Service, a cryptologic intelligence agency responsible for the collection and analysis of foreign communications and signals intelligence.

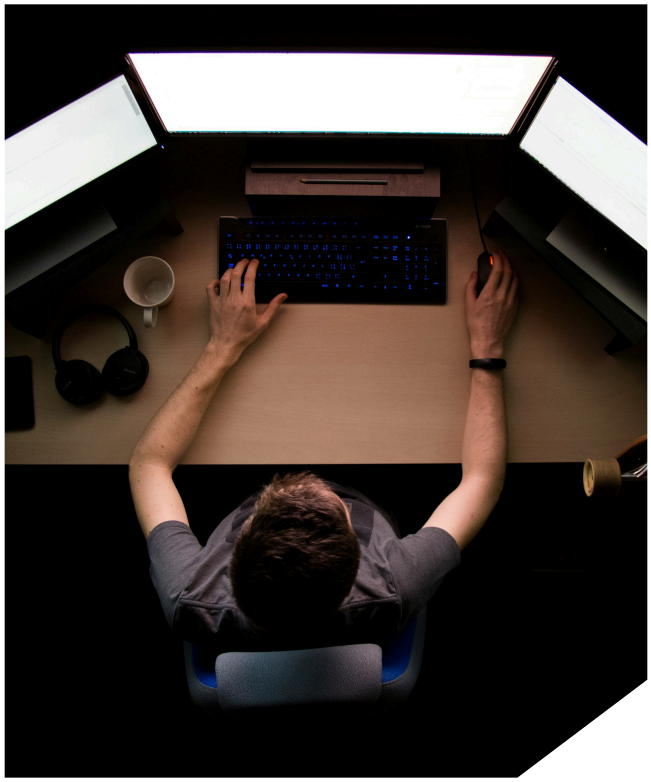
Suvorov also worked as a senior engineer at PJSC GAZ, a Russian vehicle manufacturer sanctioned by the U.S. in 2018 for supplying the Russian Armed Forces. He also received his undergraduate and graduate degree in physics from Lobachevsky State University of Nizhni Novgorod (NNGU), a national research university that conducts R&D for the Russian Ministry of Defense and Russian state-owned weapons manufacturer Almaz-Antey.

sbalandi, identified as “Balandina,”[2] formerly worked for Positive Technologies, a Russian information technology firm that was sanctioned by the U.S. in 2021 for facilitating malicious cyber operations and supporting Russian government cyber actors. Positive Technologies has also been accused of organizing recruitment events for the Federal Security Service (FSB) and the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU). Balandina also received her undergraduate and graduate degrees from NNGU.

To quantify the broader implications of risky contributors, Strider traced how the *openvino-genai* package propagates through the software ecosystem, tracking up to three degrees of dependency. *openvino-genai* appears in 62 downstream projects, including: *llama_index, gradio*, and *huggingface/transformers.* Among these, two are in the top 450 GitHub repositories.

[1] *Editor’s note: The contributor’s full name has been partially obfuscated to just their surname (“Suvorov”) throughout this case study.*

[2] *Editor’s note: The contributor’s full name has been partially obfuscated to just their surname (“Balandina”) throughout this case study.*



CASE STUDY 2:
One individual’s Contribution to the PRC’s Cyber Strategy

Strider analyzed the Python *treelib* package in GitHub. *Treelib* helps coders quickly and easily navigate “tree data structures”—or connected information, like file systems, menus, or family trees.

All commonly accepted metrics show *treelib* is a well-established and widely accepted code contribution. As of June 2025, GitHub’s *treelib* repository had accumulated more than 830 stars (approvals from users) and 185 forks (copies that users can modify without changing the original). According to PyPI Stats, *treelib* has been downloaded more than 878,000 times in the month leading up to the publishing of this report, indicating substantial usage and interest.

Using OSS Search, Strider identified GitHub’s *treelib* repository owner as “Chen.”[3] Chen has made 154 contributions to the *treelib* package. He also incubated the *awesome-public-datasets* project on GitHub.

[3] *Editor’s note: The contributor’s full name has been partially obfuscated to just their surname (“Chen”) throughout this case study.*

Strider found that Chen has been working as a technical expert at Alibaba Cloud since 2022. Alibaba Cloud is a PRC cloud computing company that cooperates with various state-affiliated defense conglomerates and reports code vulnerabilities to a government database that is shared with PRC intelligence services. Chen is simultaneously listed as a researcher at Baiyulan Open AI, a PRC state-backed research organization "committed to interconnecting with well-known open source communities [and] gathering the wisdom of developers at home and abroad."

Chen received his PhD in Behavior Informatics from Shanghai Jiao Tong University (SJTU). SJTU is a PRC university that maintains research ties with the People's Liberation Army and state-owned defense industry conglomerates, such as the China Shipbuilding Industry Corporation and the China Aerospace Science and Technology Corporation. While at SJTU, Chen specialized in mobile data mining, participating in research related to technical methods for public surveillance at a key PRC state laboratory. His research also received funding from several PRC risk entities, including Huawei Technologies.

This case illustrates a broader theme established throughout this report: The greatest risk in open source software is not always the code itself—it can be the people behind it. Integrating any open source tool means placing trust in its contributors. As demonstrated here, even widely used and well-regarded repositories can be maintained by individuals with affiliations to entities tied to state-sponsored activity. When those individuals control the update pipeline, they also hold the potential to introduce subtle vulnerabilities or malicious functionality—often without detection. Organizations must recognize that software trust is not just technical, but human.

striderintel.com

CONCLUSION

Compromised open source code contributions enable hostile nation-states to attack supply chains, launch ransomware, and cripple critical infrastructure.

Software Bills of Materials (or SBOMs) give organizations visibility of what is inside the software products they use. However, to truly recognize who is using code repositories to launch potential attacks, software makers and users must also have visibility on who is behind the codes they are utilizing.

This contributor-focused approach complements traditional endpoint security measures, offering early warning insights into structural and human-layer risks that may otherwise go undetected. By mapping these risks into the open source software supply chain, Strider helps organizations see beyond the code and into the contributors behind it.

Strider analyzes open source repositories to help safeguard software ecosystems by tracing contributor activity, monitoring updates to widely used libraries, and identifying affiliations with state-sponsored threat actors across thousands of organizations. This contributor-level intelligence empowers organizations to make informed decisions about the software they adopt before trust is misplaced.

By illuminating the human layer of open source software, Strider enables a more complete understanding of risk, which is essential for securing the technologies that power modern innovation.

For sourcing information or more insight into information detailed in this report and Strider's tools, reach out to our team via email at info@striderintel.com.