



## Technology Sector **Deep Dive**

# **Dark Web- Powered Supply Chain Attacks**



# Contents

---

- Overview ..... 4**
- How the Dark Web Facilitates Supply Chain Attacks ..... 6**
  - The Dark Web as a Gateway to Supply Chain Attacks ..... 6
  - Dark Web Data Trophies of Supply Chain Attacks ..... 7
  - Chain Attacks Against the Tech Industry on the Dark Web ..... 10
  - Recent Notable Supply Chain Attacks Against the Tech Sector ..... 10
  - GitHub Actions Supply Chain Attack. .... 11
  - Oracle Cloud Supply Chain Breach and Initial Denial. .... 12
  - The xrpl.js Supply Chain Breach ..... 14
- Security Recommendations for Technology Companies ..... 16**
- References ..... 19**

# Overview

---

**The technology industry, known for its fast-paced innovation and growth, serves as the pillar of development and automation for businesses of all sectors. Since all sectors depend on the tech industry, either directly or indirectly, for efficiency, connectivity, and productivity, it has become a prime target for cybercriminal activity that's constantly under enemy siege.**

---

The Trustwave SpiderLabs team created this report to highlight how the dark web enables threat actors' attacks against technology companies, not just by providing the necessary tools to go about doing them but also by creating a platform to monetize and promote their illicit activities.

Tech companies rely on a web of interconnected technologies — networks, infrastructures, applications, services, environments, repositories, libraries, and tools — to drive digital transformation and adapt to different industries' fast-changing shifts and demands. However, this interconnectedness is the very thing that threat actors are constantly scrutinizing and have used to conduct successful attacks.

Cybercriminals are on the prowl for weak links, vulnerability, misconfiguration, or credentials that will allow them to launch insidious attacks that lead to financial and reputational harm.

For threat actors, targeting the technology industry's supply chain is highly appealing because it can unlock other organizations' and end users' critical data, making one attack against a tech company lead to multiple victims that they can make money from on the dark web. The dark web, after all, serves as a hidden refuge for threat actors to learn new tools and techniques, obtain stolen credentials, and even sell stolen data to fellow cybercriminals for the right price.

This report is made in support of the 2025 Trustwave Risk Radar Report for the Technology Sector, a comprehensive report that tackles the major cybercriminal tactics and trends affecting the technology industry today.

# How the Dark Web Facilitates Supply Chain Attacks

---

The dark web has evolved into a key facilitator of supply chain attacks targeting the Technology sector. Cybercriminals are no longer isolated actors, but part of organized ecosystems where access credentials, zero-day exploits, and malicious code updates are traded like commodities. Within underground forums and encrypted channels, threat actors openly discuss, develop, and sell access to technology companies, offering everything from compromised developer accounts to malicious software. This underground economy enables attackers to scale operations, evade detection, and exploit trusted technology providers as gateways to far-reaching intrusions. Understanding how these activities unfold on the dark web is essential to anticipating and defending against modern supply chain attacks.

## The Dark Web as a Gateway to Supply Chain Attacks

Within the dark web's bustling marketplaces and forums, the sale of unauthorized access has evolved into a lucrative and well-organized trade. While stolen user credentials, phishing kits, and credential stealer logs remain common commodities, a more sophisticated tier of offerings has emerged: direct access to sensitive systems and data belonging to technology companies.

This data often advertises not just basic login credentials, but privileged access to core systems, APIs, and sometimes administrative portals that can act as entry points for devastating supply chain attacks.

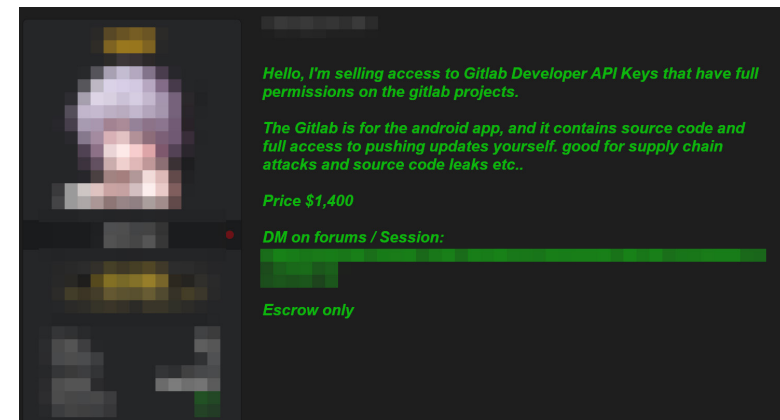


Figure 1. A recovered advertisement from a dark web forum offering access potentially usable in a supply chain attack, dated April 12, 2025.

Actors operating in these spaces are increasingly transparent about the value such access holds. They market access to developer environments, software build systems, cloud infrastructure, and remote management interfaces, highlighting how these can be leveraged to pivot into the supply chains of other organizations. The data may specify access to source code repositories, internal APIs, or privileged VPN credentials, all of which can enable the injection of backdoors, unauthorized updates, or widespread data exfiltration. As seen in Figure 1, threat actors are advertising access to GitLab Developer API Keys for USD \$1,400.

What sets these offerings apart is the emphasis on supply chain leverage. Sellers often boast about the potential for buyers to use these accesses to compromise downstream clients, distribute malware through software updates, or intercept sensitive communications passing through targeted platforms. The explicit mention of these tactics not only underscores the evolving sophistication of threat actors but also drives up the perceived value of such listings, as buyers recognize the potential for wide-ranging exploitation beyond the initial breach.

### Dark Web Data Trophies of Supply Chain Attacks

Trustwave SpiderLab’s ongoing dark web monitoring and targeted investigations reveals a stark reality: supply chain attacks against technology companies are yielding concrete, valuable data trophies that are actively traded in underground forums.

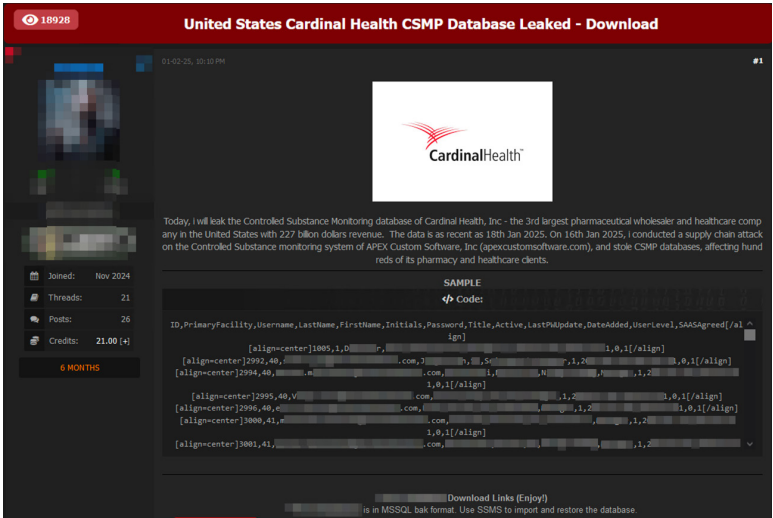
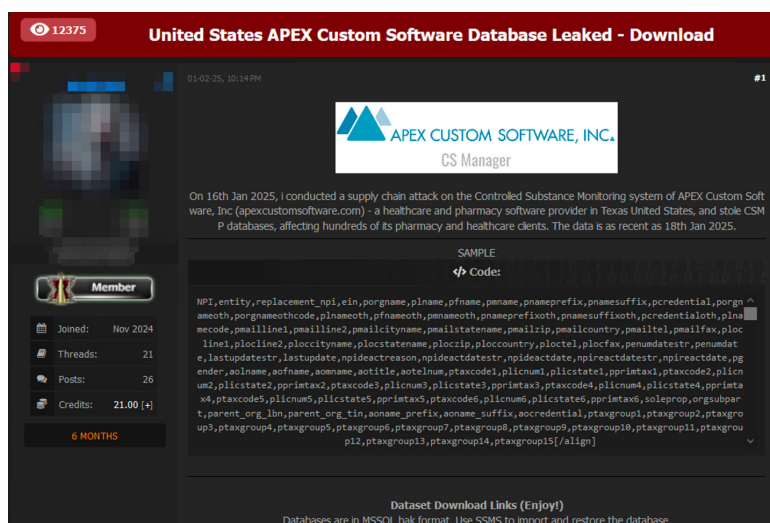


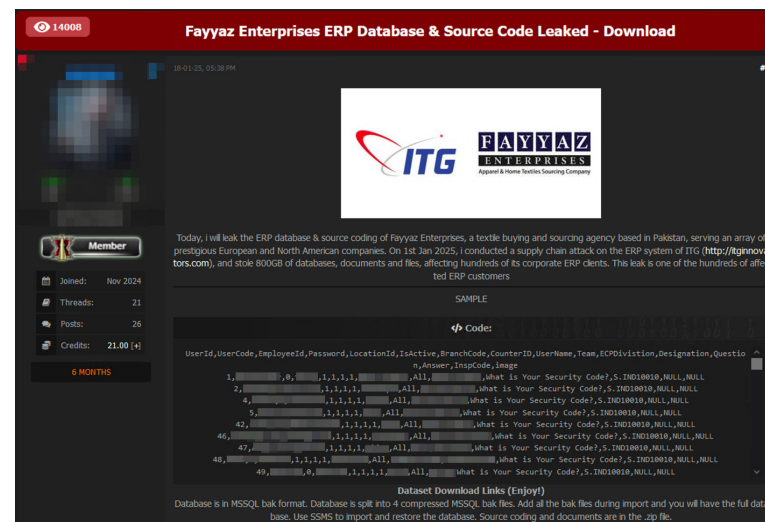
Figure 2. A threat actor is offering a healthcare facility database claimed to be obtained through a supply chain attack.

These are not just credentials or random logs; they are specific data sets, accesses, and compromised assets resulting from successful breaches of software providers and IT service vendors.



**Figure 3. A threat actor is offering a database from an initially targeted technology company, which claimed to have served as the entry point for a supply chain attack.**

In these cases, threat actors have exploited vulnerabilities in a single technology company, be it a software developer, a cloud platform, or a managed service provider, and then used that breach as a steppingstone to compromise multiple downstream clients.



**Figure 4. A threat actor is offering a database of a company belonging in the textile industry. The leaked data was obtained via a supply chain attack against a technology company that provides enterprise resource planning (ERP) software services to the Pakistan-based company.**

When these assets fall into the wrong hands, the impact extends far beyond the initially compromised provider. For end users of the affected second-layer companies, those relying on the compromised technology vendor, the consequences can be severe. These end users often experience disruptions in service availability, unauthorized access to their sensitive data, and potential manipulation of core processes managed by the vendor.

Compromised software updates or stolen API credentials can be used to inject malware into customer environments, intercept data streams, or hijack account access, leading to breaches that appear as isolated incidents but trace back to a single upstream supply chain attack.



**Figure 5. A threat actor is offering one of hundreds of leaked databases obtained from a supply chain attack that started from a technology sector company.**

The trust placed in a vendor’s technology becomes a vulnerability that adversaries exploit. End users may not immediately realize they have been compromised, as attackers often leverage legitimate channels and credentials to maintain stealthy access. This can result in prolonged exposure to data breaches, financial fraud, and operational disruptions, compounded by the difficulty in identifying the true source of the compromise. We’ve seen this recently in March when customer data was stolen from a popular cloud vendor.<sup>1</sup> We are often only as secure as the companies we partner with.

Ultimately, supply chain attacks that begin with a technology provider have cascading effects that place end users of second-layer companies at significant risk. These attacks can undermine digital trust, erode customer confidence, and create regulatory and financial repercussions for organizations caught in the downstream blast radius of an upstream compromise.

## Chain Attacks Against the Tech Industry on the Dark Web

The dark web has evolved into a key facilitator of supply chain attacks targeting the Technology sector. Cybercriminals are no longer isolated actors, but part of organized ecosystems where access credentials, zero-day exploits, and malicious code updates are traded like commodities. Within underground forums and encrypted channels, threat actors openly discuss, develop, and sell access to technology companies, offering everything from compromised developer accounts to malicious software. This underground economy enables attackers to scale operations, evade detection, and exploit trusted technology providers as gateways to far-reaching intrusions. Understanding how these activities unfold on the dark web is essential to anticipating and defending against modern supply chain attacks.

## Recent Notable Supply Chain Attacks Against the Tech Sector

The cybersecurity landscape in 2024 and 2025 has been marked by an alarming rise in supply chain attacks against the technology sector. These attacks leverage the sector's deep interconnectivity, exploiting dependencies in open-source libraries, Continuous Integration/Continuous Delivery (CI/CD) pipelines, cloud infrastructure, and third-party services. As we know, a single compromise can now impact thousands of organizations and millions of users almost instantly.

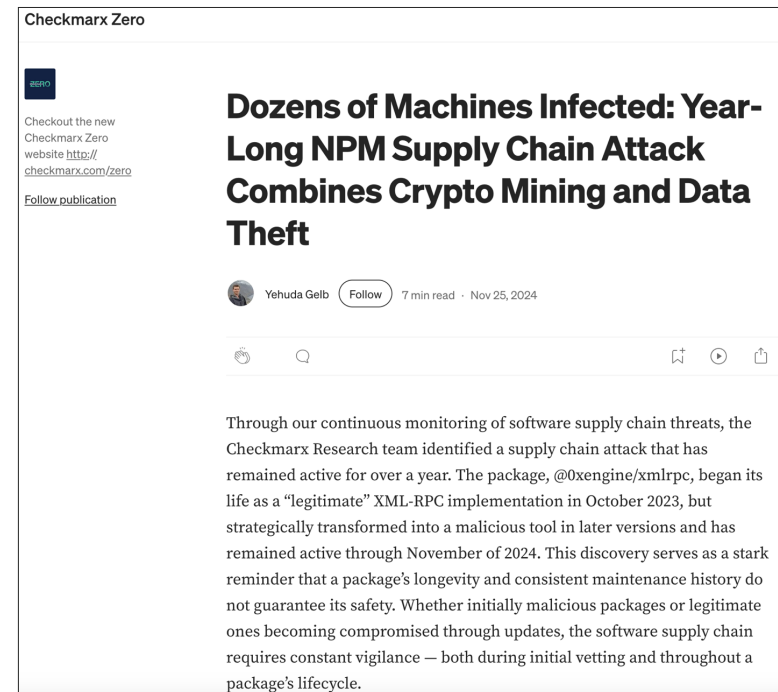


Figure 6. Supply chain attack spotted in the news.

Recent incidents, (all of which are discussed in depth below) such as the xrpl.js npm breach, the GitHub Actions workflow compromise, and the Oracle Cloud credential exposure, highlight a clear shift in malicious actor tactics. Attackers increasingly target trusted vendors and shared components, embedding malicious code into essential tools and services that propagate far beyond the initial breach point. These attacks often unfold quietly, with the impact only becoming clear after sensitive data has been exfiltrated or backdoors have been discovered in widely used libraries.

The consequences are far-reaching. Technology companies, once seen as guardians of digital innovation, now face reputational damage, regulatory scrutiny, and operational disruptions from these breaches. Worse, a supply chain attack can cascade into connected sectors such as healthcare, finance, and government, compounding risks and creating systemic vulnerabilities.

### GitHub Actions Supply Chain Attack

In March 2025, a sophisticated supply chain attack exploited the interconnected nature of GitHub Actions, affecting numerous repositories and highlighting vulnerabilities in CI/CD pipelines.



Figure 7. An article about the GitHub Action supply chain attack.

The attack began with the compromise of the *reviewdog/action-setup@v1* GitHub Action. Attackers injected malicious code into this action, which was then propagated to dependent actions, notably *tj-actions/eslint-changed-files* and subsequently *tj-actions/changed-files*. This chain of dependencies allowed the malicious payload to spread widely, affecting over 23,000 repositories that utilized these actions.

The malicious code was designed to exfiltrate sensitive information by dumping CI/CD secrets into workflow logs. These logs, often publicly accessible, contain environment variables and authentication tokens, posing significant security risks to the affected projects.

Coinbase's open-source project, agentkit, was among the initial targets. Attackers attempted to exploit its CI/CD pipeline by leveraging compromised actions. Although Coinbase detected and mitigated the threat promptly, preventing any significant damage, the incident underscored the potential risks associated with third-party dependencies in software development workflows.

This attack sequence has been documented under CVE-2025-30066 and CVE-2025-30154, emphasizing the importance of securing CI/CD pipelines and the dependencies they rely upon.

The incident serves as a stark reminder of the cascading effects a single compromised component can have within the software supply chain, stressing the need for vigilant monitoring and stringent security practices in development environments.

## Oracle Cloud Supply Chain Breach and Initial Denial

In March 2025, a significant cybersecurity incident emerged involving Oracle Cloud's infrastructure. A threat actor, operating under the alias "rose87168," claimed responsibility for exfiltrating approximately six million records from Oracle SSO and LDAP systems. The stolen data reportedly included JKS files, encrypted SSO passwords, key files, and Enterprise Manager JPS keys, potentially impacting over 140,000 Oracle Cloud tenants worldwide.

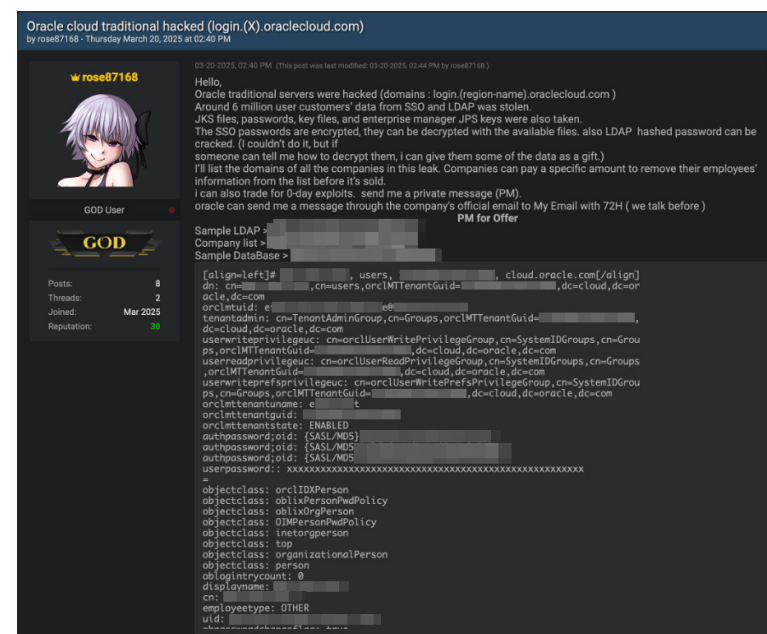


Figure 8. The threat actor's initial post claiming a successful breach into Oracle Cloud.

The attacker alleged that the breach was facilitated by exploiting a vulnerability in Oracle Cloud's login endpoint, specifically targeting servers at *login.(region-name).oraclecloud.com*. This claim suggested a supply chain compromise, where unauthorized access to Oracle's authentication infrastructure could have cascading effects on numerous client organizations.

Initially, Oracle publicly denied any breach of its cloud infrastructure, asserting that its systems remained secure. However, as independent cybersecurity researchers and firms like CloudSEK presented supporting evidence, including samples of the exfiltrated data and details of the alleged vulnerability, pressure mounted on Oracle to address the claims more transparently.

Subsequently, Oracle began notifying affected customers, clarifying that while Oracle Cloud Infrastructure had not been compromised, certain legacy systems had experienced unauthorized access. This nuanced acknowledgment highlighted the complexities inherent in large-scale cloud environments, where legacy components can introduce unforeseen vulnerabilities.

In response to the incident, the Cybersecurity and Infrastructure Security Agency (CISA) issued guidance to organizations, emphasizing the risks associated with credential exposure and recommending immediate actions to mitigate potential impacts.

This case underscores the critical importance of transparent communication during cybersecurity incidents and the need for organizations to continuously assess and secure all components of their infrastructure, including legacy systems, to prevent supply chain attacks.

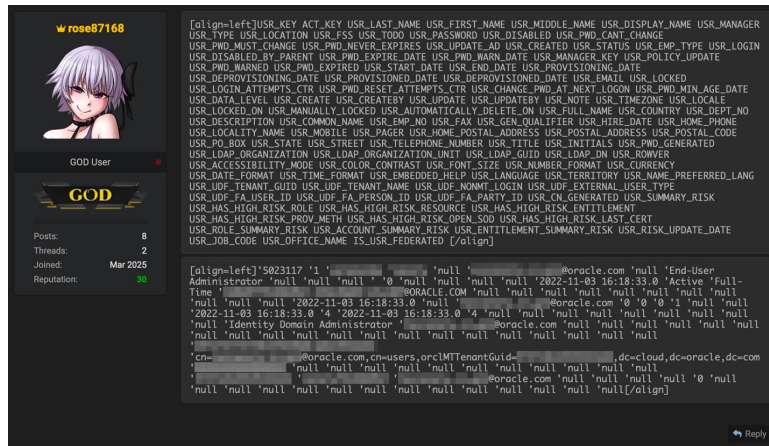


Figure 9. The threat actor provides more data to prove its claims on a dark web post.

## The xrpl.js Supply Chain Breach

In April 2025, a sophisticated supply chain attack rocked the open-source community, targeting the widely used xrpl.js JavaScript library, a core component for developers interacting with the XRP Ledger. This attack was traced to a compromise of a Ripple developer's npm account, which allowed attackers to publish malicious versions of xrpl.js, specifically versions 2.14.2, 4.2.1, 4.2.2, 4.2.3, and 4.2.4. These versions contained a stealthy backdoor function named `checkValidityOfSeed`, embedded directly into the `/src/index.js` file of the compromised packages.

The malicious `checkValidityOfSeed` function was designed to exfiltrate wallet seeds and private keys to an attacker-controlled domain (`0x9c[.]xyz`). The data was transmitted through HTTP POST requests disguised as innocuous ad referral traffic, making detection challenging in routine network monitoring. This backdoor targeted users who interacted with the XRP Ledger via the affected library, posing a severe risk of fund theft and unauthorized access.



Figure 10. Xrpl.js supply chain attack flowchart.

Interestingly, the injected malicious code was absent from the public GitHub repository, indicating the compromise occurred solely within the npm registry. This points to a highly targeted supply chain attack focused on package distribution, exploiting the trust developers place in npm as a source of dependencies. The compromise went unnoticed until April 22, 2025, when security researchers<sup>2</sup> identified the anomaly and immediately notified Ripple.

Ripple responded by deprecating the compromised versions and swiftly releasing patched versions, 4.2.5 and 2.14.3, removing the backdoor and restoring the integrity of the library. The vulnerability has been cataloged as CVE-2025-32965<sup>3</sup>, receiving a critical severity rating of 9.3 due to its potential for widespread impact. Developers using the affected versions were urged to upgrade immediately and rotate any exposed credentials or wallet seeds.

This incident highlighted persistent vulnerabilities in open-source software supply chains, particularly in package management ecosystems like npm. It underscores the importance of implementing robust access controls for developer accounts, continuous monitoring for unusual code changes, and adopting automated dependency scanning tools to detect potential backdoors in critical libraries.

# Security Recommendations for Technology Companies

---

To mitigate the increasing risks and prevent future cyberattacks, organizations belonging in the tech industry must take a proactive approach to cybersecurity by implementing the following best practices:

## **Strengthen Access Controls and Authentication**

- Implement multi-factor authentication (MFA) for all user accounts, especially VPNs, RDP access, and administrative systems.
- Use zero-trust security models to restrict access based on identity verification and least privilege principles.
- Conduct regular cybersecurity audits of third-party vendors, including software providers and suppliers.
- Implement vendor access controls and monitor third-party API connections for suspicious activity.

## **Understand Your Supplier Concentration**

- Check your critical suppliers' infrastructure or backend, ensuring that your backup suppliers don't use the same infrastructure as your primary.

## **Have An Exit Planning Strategy**

- Make sure that your supplier contract reflects the disabling of credentials, return of data, use and ownership of IP, and switchover to alternative suppliers, among other critical tasks.

## **Monitor Databases and Log Activities**

- Closely monitor databases and regularly log key activities such as user activity or actions taken on a database.
- Monitor file and folder activities.

### **Monitor the Dark Web for Leaked Data**

- Use threat intelligence tools to track stolen credentials and business-critical information, and ransomware discussions on dark web forums.
- Work with cybersecurity firms and law enforcement agencies to recover stolen data and disrupt cybercriminal operations.

### **Check, Test, and Monitor Third-Party Suppliers**

- Conduct a thorough check of a potential supplier prior to obtaining their services. Make sure that due diligence questionnaire responses are carefully reviewed.
- Make sure that certifications are verified. Do not just accept responses at face value.
- Conduct tests over systems developed by third parties.
- Let all suppliers go through a one-size-fits-all procedure no matter the level of risk. Perform triage and grading. Identified low-risk suppliers can be subject to less stringent requirements to ensure efficiency.

### **Develop a Robust Incident Response and Recovery Plan**

- Establish a dedicated cybersecurity team capable of responding to breaches, ransomware infections, and insider threats.
- Test disaster recovery plans regularly to ensure quick restoration of services in the event of an attack.

### **Increase Staff Cyber Awareness and Training**

- Conduct regular phishing simulations and security awareness training for technology employees.
- Establish incident response protocols so that staff can quickly respond to ransomware, phishing, and social engineering attempts.

The dark web has evolved into a critical enabler of supply chain attacks targeting technology companies. It provides threat actors not only with the tools and services necessary to execute these breaches but also with a marketplace to monetize their successes. From credentials and developer accounts to entire software update systems and management consoles, compromised assets are packaged and sold on a variety of dark web platforms.

These activities illustrate a shift in cybercrime strategy: Attackers are no longer solely focused on direct intrusion but increasingly seek to exploit the trust and interconnectedness that defines modern technology supply chains. The result is a growing ecosystem of secondary victims — end users and organizations that unknowingly inherit the consequences of a breach upstream.

Moreover, the explicit marketing of supply chain attack capabilities on underground platforms signals a growing confidence among threat actors. By highlighting how access to a single provider can unlock entire ecosystems, sellers are driving up the perceived value of their illicit offerings while signaling the systemic risks these breaches create.

For technology companies, this landscape demands heightened vigilance, more robust access controls, and proactive supply chain security measures. Defending against these evolving threats requires a shift from reactive responses to preemptive strategies, including dark web monitoring, dependency analysis, and rigorous security protocols at every stage of software and service delivery.

As cybercriminals refine their techniques and underground markets become more sophisticated, the need for collaborative defense and comprehensive supply chain resilience has never been more urgent.

# References

---

- 1. Kazymirskyi, Nikita, and Karl Sigler. "Trustwave SpiderLabs Threat Review: Alleged Oracle Compromise."**  
*Trustwave*, 25 Mar. 2025,  
<https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/trustwave-spiderlabs-threat-review-alleged-oracle-compromise/>.  
Accessed 25 June 2025.
- 2. Eriksen, Charlie. "XRP Supply Chain Attack: Official NPM Package Infected with Crypto Stealing Backdoor."**  
*Aikido*, 6 June 2025,  
<https://www.aikido.dev/blog/xrp-supplychain-attack-official-npm-package-infected-with-crypto-stealing-backdoor>.  
Accessed 25 June 2025.
- 3. National Institute of Standards and Technology . "CVE-2025-32965."**  
*NVD*, 22 April 2025,  
<https://nvd.nist.gov/vuln/detail/CVE-2025-32965>.  
Accessed 25 June 2025.

