Obtainium.ai
ENGINEERED INTELLIGENCE. REAL IMPACT.

Supply Chain Attacks: What Small Businesses Need to Know

Obtainium.ai LLC

Engineered Intelligence. Real Impact.

When the Tools You Trust Become the Threat

Most small business owners think about cybersecurity in terms of phishing emails, weak passwords, or someone breaking into their website. But one of the fastest-growing and most dangerous threats today works differently — it hides inside the software tools your business already uses and trusts.

In early April 2026, security researchers confirmed that attackers — later linked to North Korean state-sponsored hackers — had compromised four widely-used software packages: **Axios**, **LiteLLM**, **Trivy**, and **Telnyx**. These tools are used by millions of organizations worldwide, including in financial services, retail, legal, insurance, and education.

The Axios compromise alone affected more than **100 million weekly downloads** across multiple release versions — all within a three-hour window. Once installed, the malicious code quietly harvested passwords, API keys, and cloud credentials from the systems running it. Within hours of those credentials being stolen, attackers were already inside victim cloud environments, looking around and pulling out data.

This is what a **supply chain attack** looks like. And it's something every business that uses software — which is every business — needs to understand.

What Is a Software Supply Chain Attack?

The term "supply chain" in security mirrors the concept in business. Just as a contaminated ingredient can affect every product made from it, a compromised software component can affect every system that runs it.

Here's the basic pattern:

1. **An attacker targets a popular open-source or commercial software package** — something used by thousands of businesses.
2. **They inject malicious code** — either by compromising the developer's account, sneaking a harmful update past reviewers, or creating a near-identical package with a misleading name.
3. **Businesses download and install the package** as part of a normal update or new project setup — without any warning.
4. **The malicious code runs silently** on the business's systems, stealing credentials, keys, or data.

5. **Attackers use what they steal** to break into cloud accounts, steal more data, or install ransomware.

What makes this so effective is that the software appears legitimate. It came from a trusted source. Your security tools may not flag it because, technically, you installed it yourself.

> *Supply chain attacks exploit the implicit trust we place in software we download — making them among the hardest threats to detect and defend against.*

Why This Matters Even If You Don't Write Code

You might be thinking: "We don't use any of those tools. We're not a tech company." But the connection runs deeper than you might expect.

Almost every modern business relies on software that is, in turn, built on dozens or hundreds of other software components. Your accounting platform, your email marketing tool, your scheduling app, your CRM — all of them are likely built using open-source packages like Axios. When those packages are compromised, the risk flows downstream to every business using any product built on top of them.

Here are some of the sectors hit hardest by the 2026 supply chain attacks:

- **Financial services** — accounting tools, payment processors, banking integrations
- **Retail** — e-commerce platforms, inventory systems, point-of-sale software
- **Legal** — document management, client portals, contract automation
- **Insurance** — policy management systems, claims platforms
- **Education** — learning management systems, student data platforms

If your business operates in any of these sectors, your vendors almost certainly use software components that could be affected by supply chain compromises.

What Attackers Do Once They're In

Understanding what happens after an attack helps you see why these events are so damaging — and so urgent.

When attackers compromised the packages described above, they stole **hundreds of thousands of secrets** — including:

- **Cloud access credentials** (keys that unlock your business's files, databases, and infrastructure)
- **API keys** (which control integrations between your apps and third-party services)
- **Passwords and session tokens** (which can be used to log in as you)

Researchers from Wiz, a cloud security firm, observed that stolen credentials were being validated and used within hours of the attack. Here's the typical sequence:

Stage 1: Credential Harvesting

The malicious package runs silently, collecting any credentials or keys it finds on the system. This takes seconds.

Stage 2: Rapid Validation

Attackers test the stolen credentials automatically — checking which ones still work. This happens in bulk, often within minutes.

Stage 3: Cloud Environment Exploration

Once valid credentials are confirmed, attackers log into cloud accounts and quietly map out what's there: storage buckets, databases, customer records, financial data, email archives.

Stage 4: Data Exfiltration or Ransomware

Attackers either steal the data quietly (for sale, espionage, or extortion) or deploy ransomware that encrypts your files and demands payment for their return. The attackers behind these specific incidents have ties to a ransomware group called **Vect** and are developing their own ransomware program called **CipherForce**.

The window between infection and impact is measured in hours — not weeks. Businesses that don't have detection tools in place often don't know they've been breached until it's far too late.

How to Reduce Your Exposure: Practical Steps

You don't need to become a cybersecurity expert to meaningfully reduce your risk. Here are

the most impactful steps a small business can take:

1. Know What Software Your Business Uses

Create a simple list — a software inventory — of every tool, platform, and application your business runs. Include the software your vendors use on your behalf if possible. You can't protect what you don't know exists.

- Start with your most sensitive systems: anything that touches customer data, financial information, or employee records.
- Ask your IT provider or managed service vendor: "Do we have a current inventory of all software in use?"

2. Stay Current on Updates — But Verify Before You Apply

Keeping software updated is generally good security hygiene. But supply chain attacks exploit the update process itself. Here's the nuance:

- **For critical systems**, don't blindly auto-update. Wait 24–48 hours after a major release and check whether any security advisories have been issued.
- **Monitor your vendors' security bulletins.** Legitimate vendors will notify you if a package they use has been compromised.
- **For lower-risk tools**, automatic updates remain appropriate and beneficial.

3. Use Multi-Factor Authentication (MFA) Everywhere

This is the single highest-return security action for small businesses. Even if an attacker steals a password or API key, **MFA requires a second verification step** (typically a code from your phone) before they can log in.

- Enable MFA on your email, cloud storage, banking, accounting tools, and CRM.
- Use an authenticator app (like Google Authenticator or Authy) rather than SMS codes, which can be intercepted.
- For cloud services like AWS, Google Cloud, or Azure: MFA on the root/admin account is non-negotiable.

4. Rotate Credentials Regularly — and After Any Incident

API keys, passwords, and access tokens that never expire are a major risk. Stolen credentials are only useful if they still work.

- Set a quarterly reminder to rotate API keys for your most sensitive integrations.
-

Change passwords immediately if any tool you use announces a security breach.

- If you hear about a supply chain attack affecting a tool you use, rotate all credentials on systems where that tool ran — don't wait to find out if you were affected.

5. Limit What Your Software Can Access

This is called the **principle of least privilege**. Every tool, every user, and every integration should have access to only what it absolutely needs — nothing more.

- Review which apps have access to your Google Drive, Microsoft 365, or cloud storage. Revoke access for anything you no longer use.
- When setting up new software, don't grant administrator access by default. Start with the minimum required.
- Ask your IT provider to review permissions on your cloud environment at least once a year.

6. Have an Incident Response Plan

Speed matters enormously in breach response. Businesses that respond within the first few hours limit their losses dramatically. Businesses that take days to notice often face complete data loss or extended downtime.

A basic incident response plan includes:

- Who to call first (IT provider, cybersecurity firm, legal counsel)
- How to isolate affected systems quickly (disconnect from the internet, revoke credentials)
- How to notify affected customers if required by law
- A checklist of steps to preserve evidence for any insurance claim or investigation

> *You don't need a sophisticated security operation. You need a plan written down, shared with key people, and reviewed once a year.*

The Bigger Picture: Nation-State Threats Targeting Small Businesses

It might seem improbable that North Korean government-sponsored hackers would be

interested in your small business. But the scale of supply chain attacks means that small businesses become collateral damage in campaigns aimed at much larger targets.

Attackers who compromise a software package used by 100 million downloads per week are not targeting specific victims. They are casting the widest possible net and then sorting through what they catch. A small business with valid cloud credentials is just as valuable to them as a large enterprise — sometimes more so, because smaller businesses tend to have weaker defenses.

The combination of nation-state attackers, organized cybercrime groups, and ransomware-as-a-service platforms means the threat landscape has professionalized significantly. These are not lone hackers. They are coordinated organizations with tools, playbooks, and financial incentives.

Being small is no longer a form of protection.

What to Do Right Now

If this article has raised your concern level, that's appropriate — and actionable. Here are three things you can do this week:

1. **Audit your MFA status.** Log into your five most critical business tools and confirm multi-factor authentication is enabled. If it isn't, enable it today.
2. **Ask your IT provider one question:** "Do we have monitoring in place that would alert us if our credentials were used from an unusual location or at an unusual time?" If the answer is no, ask what it would take to get there.
3. **Review your software subscriptions.** Cancel or revoke access for any tool you no longer actively use. Every active credential is a potential entry point.

Supply chain attacks are a real and growing threat. But they are not inevitable. Basic hygiene, applied consistently, puts your business in a far stronger position than the majority of small businesses that remain unprotected.

Sources: Help Net Security reporting on the April 2026 Axios/LiteLLM/Trivy/Telnyx compromises; Wiz incident response team findings; Google Threat Intelligence (Mandiant) attribution of UNC1069 activity.