precision
CYBERTECHNOLOGIES & DIGITAL SOLUTIONS LTD

CYBER DIGITAL WORLD

NEWSLETTER

Volume: 50 OCTOBER 2025

Dr. Ronald Walcott
Managing Director

INTRODUCTION

In today's hyper-connected digital landscape, an organization's security is only as strong as its weakest link, and increasingly, that link lies within the supply chain. From software vendors to third-party service providers, each partnership introduces potential entry points for attackers seeking to exploit trusted relationships. Recent high profile breaches, such as the SolarWinds compromise and the MOVEit vulnerability, have exposed how deeply supply chain attacks can infiltrate global networks, impacting thousands of organizations at once.

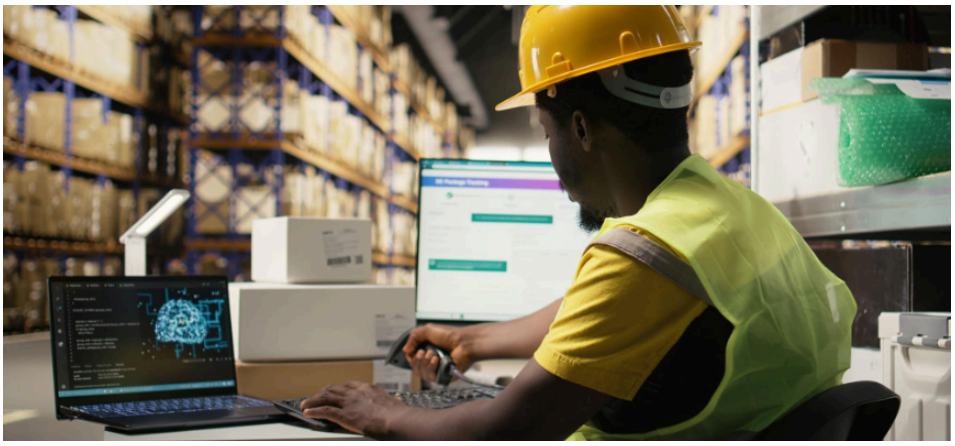
In this edition of Precision Cyber's newsletter, we explore the evolving tactics threat actors use to target supply chains, uncover key lessons from real-world incidents, and share actionable strategies to strengthen resilience across every layer of your vendor ecosystem. Whether you're managing IT procurement, vendor risk, or cybersecurity operations, these insights will help you identify hidden vulnerabilities, implement zero-trust principles, and ensure that trust in your supply chain is earned not assumed.

HOW TO IDENTIFY HIDDEN VULNERABILITIES IN THE SUPPLY CHAIN.

Identifying hidden vulnerabilities in the supply chain begins with building a complete visibility map of all your suppliers, subcontractors, and software or hardware vendors inclusive of the ones that sit only one or two tiers beyond your direct engagements. Many organizations stop at the first-tier suppliers, but attackers often exploit weaknesses in lesser-scrutinized second- or third-tier vendors. A comprehensive audit should capture not just the vendor's name and contract value, but the types of access they have (network, cloud, physical), their patching/maintenance practices, their history of incidents, and whether they themselves depend on further vendors. You should also assess components such as firmware, outsourced operational technology modules, and embedded software libraries, which is one classic weak link in many supply-chains. By profiling and scoring each vendor on their risk exposure, you can prioritize audits, require security commitments (e.g., SLAs, certifications, continuous monitoring) and insert contractual clauses to mitigate risk.

In the Caribbean context, there is an example that underscores how such hidden vulnerabilities play out. In 2022, a major regional conglomerate in Trinidad & Tobago, was subject to a data breach in which the hacker group allegedly exfiltrated over 700,000 files (including staff salaries and passport copies) after exploiting vulnerabilities in systems connected to the supply chain of the organization. While the initial target was the conglomerate, the weakness was reportedly in a vendor-supplied system or external link rather than the main network perimeter, illustrating how third-party systems can become entry points. From this lesson, organiza-

CONTINUED ON PAGE 2



IN THIS ISSUE:

tions should emphasize vendor due diligence (security posture reviews), require evidence of strong controls (segmentation, least privilege, frequent backups), and monitor vendor activity (logs, anomalous behaviour) to offset the risk of hidden supply chain vulnerabilities.

WHY IT IS IMPORTANT TO EVALUATE SUPPLY CHAIN.

It is essential for companies to evaluate who they decide to partner with. Here are three key reasons why conducting thorough evaluations of your supply chain is critically important each re-enforced with a real-world example from the Caribbean region:

1. **Risk propagation through third-parties leads to widespread impact.** When a supplier or partner in your chain is compromised, it can ripple through to your organization even if you believe your own systems are secure. For example, the region-wide cyber-attack on Massy Group in Trinidad & Tobago in 2022 (where hundreds of thousands of files including staff passports, internal audits and customer information were publicly leaked) shows how a breach in one link devastated broader operations. By evaluating your supply-chain you can identify which vendors have high access privileges, what systems they depend on, and how their failure might affect you.
2. **Operational & logistical vulnerabilities can undermine business continuity and competitiveness.** The Caribbean supply chain faces physical, geopolitical and infrastructure constraints that amplify risk. For example, according to reporting in Barbados: delays at major regional trans-shipment hubs (such as those in Trinidad and Jamaica) caused significant shipment back-logs and disrupted retailers' holiday stocking plans. If you evaluate your supply chain you are better placed to identify fragile logistics nodes (ports, transshipment hubs, shipping dependencies), plan contingencies (alternative routes, buffer stock), and thereby maintain continuity when disruptions occur.
3. **Regulatory, reputational and financial fallout from unmanaged partner risk.** When a supplier suffers a breach, your organization may suffer reputational damage or regulatory scrutiny even if you weren't directly breached. The case of the telecom provider who reportedly had sensitive customer data (including national ID numbers) exposed in a ransomware incident – shows how downstream consequences from vendor or supply-chain failures matter. By evaluating the security posture of your supply-chain partners (and requiring due diligence, audits, SLAs) you mitigate the risk of being dragged into someone else's failure.

IMPLEMENTING ZERO TRUST PRINCIPLES

Implementing **Zero Trust principles** is essential in today's cybersecurity landscape, where perimeter-based defenses are no longer sufficient. Traditional models assumed that once a user or device was inside the network, it could be trusted, but modern attacks routinely exploit this assumption through credential theft, insider threats, or compromised vendor accounts. Zero Trust operates on the principle of "never trust, always verify," requiring continuous authentication and authorization for every access request, regardless of the user's location or network position. By validating identity, device health, and context before granting access, organizations can dramatically reduce the risk of lateral movement by attackers and contain potential breaches more effectively.

Beyond just security, Zero Trust supports resilience and compliance by enforcing granular access controls and detailed visibility across systems. This model ensures that only the right people have the right access to the right resources at the right time limiting the blast radius of any incident. For example, if a partner organization's account or a supplier's access token is compromised, Zero Trust segmentation prevents attackers from moving deeper into critical assets such as financial systems or sensitive data stores. As hybrid work, cloud adoption, and third-party integrations expand, implementing Zero Trust is no longer optional it's a strategic necessity for maintaining data integrity, operational continuity, and stakeholder trust in a borderless digital ecosystem.

UPCOMING EVENTS

CYBERSECURITY SUMMIT: TORONTO FINANCIAL SERVICES
October 23, 2025

FRAUD PREVENTION SUMMIT: NEW YORK
November 5, 2025

CYBERSECURITY SUMMIT: NEW YORK FINANCIAL SERVICES
November 6, 2025

Frequently Asked Questions:

WHAT IS ZERO TRUST?

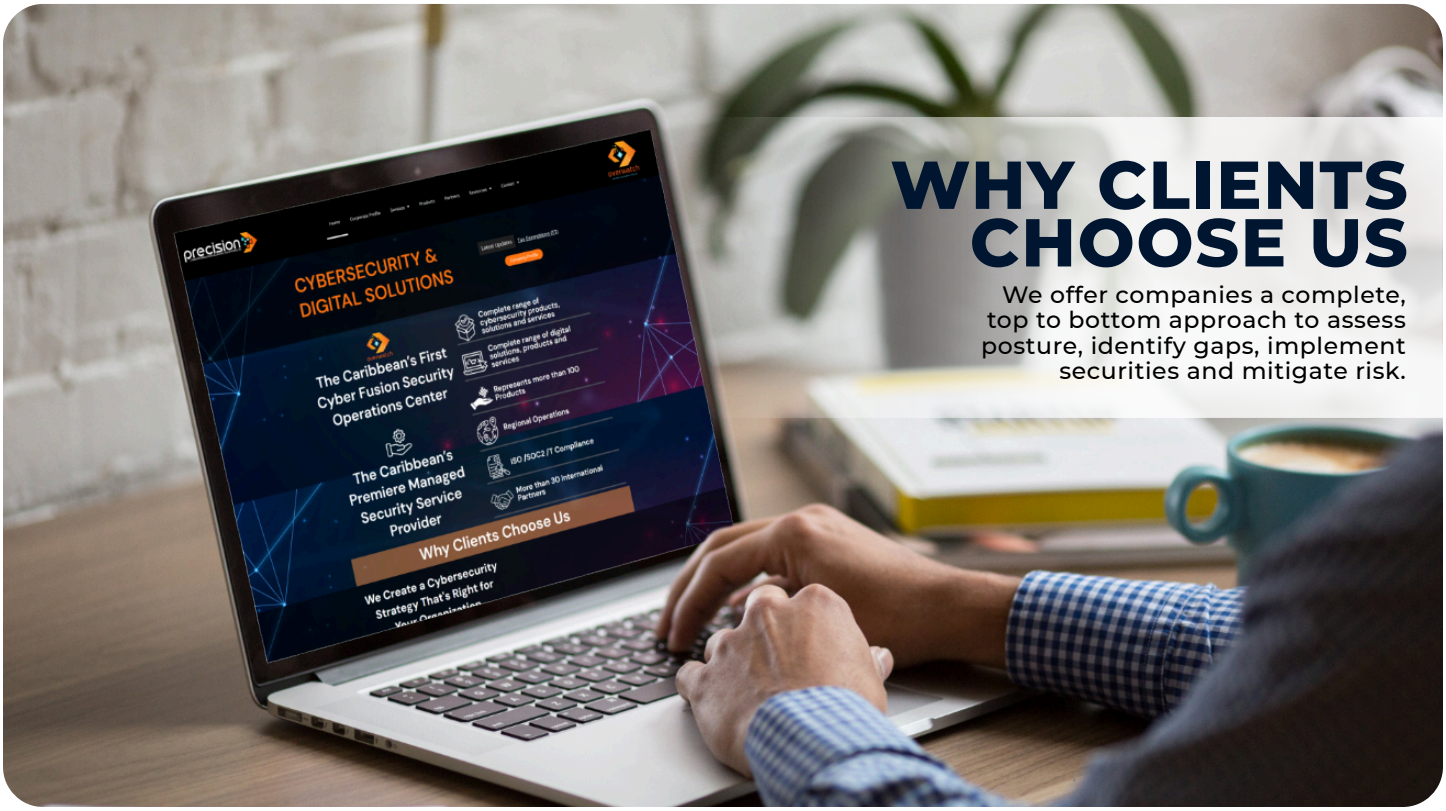
Zero Trust is a modern cybersecurity framework built on the idea that no user, device, or application should ever be automatically trusted—even if they're already inside the organization's network. Instead of assuming that everything within the network perimeter is safe, Zero Trust continuously verifies every access request as though it comes from an open, untrusted environment.

WHAT CAN WE DO TO IMPROVE SUPPLY CHAIN SECURITY IN THE CARIBBEAN?

To strengthen supply chain security in the Caribbean, organizations must adopt a proactive, region-wide approach that combines strong vendor risk management, regional collaboration, and local capacity building. This includes enforcing cybersecurity standards and audits for suppliers, sharing threat intelligence through CARICOM and other regional networks, and investing in training programs to build local cybersecurity expertise. Additionally, adopting modern tools such as continuous monitoring, blockchain for supply-chain transparency, and Zero Trust frameworks can help detect vulnerabilities early and limit damage. Together, these efforts will enhance resilience, protect critical infrastructure, and build greater trust across the Caribbean's interconnected digital economy.

IS IT MORE IMPORTANT FOR BUSINESSES TO EVALUATE THEIR SUPPLIERS VS REGULAR INDIVIDUALS?

Yes, it is generally more important for businesses to evaluate their suppliers than for regular individuals, because organizations rely on a complex web of third-party vendors, service providers, and technology partners that can directly impact their operations, data security, and reputation. A single weak link in a company's supply chain can expose sensitive information, disrupt services, or even lead to large-scale breaches affecting thousands of customers, as seen in incidents like the Massy Group cyberattack in Trinidad & Tobago. While individuals should still practice good digital hygiene, businesses face greater risk due to the interconnected nature of their supply chains making supplier evaluation a critical component of organizational resilience, regulatory compliance, and long-term trust.



WHY CLIENTS CHOOSE US

We offer companies a complete, top to bottom approach to assess posture, identify gaps, implement securities and mitigate risk.

Headline News

Self-Spreading 'GlassWorm' Infects VS Code Extensions in Widespread Supply Chain Attack

Cybersecurity researchers have discovered a self-propagating worm that spreads via Visual Studio Code (VS Code) extensions on the Open VSX Registry and the Microsoft Extension Marketplace, underscoring how developers have become a prime target for attacks.

The sophisticated threat, codenamed GlassWorm by Koi Security, is the second such supply chain attack to hit the DevOps space within a span of a month after the Shai-Hulud worm that targeted the npm ecosystem in mid-September 2025.

What makes the attack stand out is the use of the Solana blockchain for command-and-control (C2), making the infrastructure resilient to takedown efforts. It also uses Google Calendar as a C2 fallback mechanism.

Another novel aspect is that the GlassWorm campaign relies on "invisible Unicode characters that make malicious code literally disappear from code editors," Idan Dardikman said in a technical report. "The attacker used Unicode variation selectors – special characters that are part of the Unicode specification but don't produce any visual output."

The end goal of the attack is to harvest npm, Open VSX, GitHub, and Git credentials, drain funds from 49 different cryptocurrency wallet extensions, deploy SOCKS proxy servers to turn developer machines into conduits for criminal activities, install hidden VNC (HVNC) servers for remote access, and weaponize the stolen credentials to compromise additional packages and extensions for further propagation.

The names of the infected extensions, 13 of them on Open VSX and one on the Microsoft Extension Marketplace, are listed below. These extensions have been downloaded about 35,800 times. The first wave of infections took place on October 17, 2025. It's currently not known how these extensions were hijacked

The malicious code concealed within the extensions is designed to search for transactions associated with an attacker-controlled wallet on the Solana blockchain, and if found, it proceeds to extract a Base64-encoded string from the memo field that decodes to the C2 server ("217.69.3[.]218" or "199.247.10[.]166") used for retrieving the next-stage payload.

The payload is an information stealer that captures credentials, authentication tokens, and cryptocurrency wallet data, and reaches out to a Google Calendar event to parse another Base64-encoded string and contact the same server to obtain a payload codenamed Zombi. The data is exfiltrated to a remote endpoint ("140.82.52[.]31:80") managed by the threat actor.

Written in JavaScript, the Zombi module essentially turns a GlassWorm infection into a full-fledged compromise by dropping a SOCKS proxy, WebRTC modules for peer-to-peer communication, BitTorrent's Distributed Hash Table (DHT) for decentralized command distribution, and HVNC for remote control.

The problem is compounded by the fact that VS Code extensions are configured to auto-update, allowing the threat actors to push the malicious code automatically without requiring any user interaction.

"This isn't a one-off supply chain attack," Dardikman said. "It's a worm designed to spread through the developer ecosystem like wildfire."

"Attackers have figured out how to make supply chain malware self-sustaining. They're not just compromising individual packages anymore – they're building worms that can spread autonomously through the entire software development ecosystem."

The development comes as the use of blockchain for staging malicious payloads has witnessed a surge due to its pseudonymity and flexibility, with even threat actors from North Korea leveraging the technique to orchestrate their espionage and financially motivated campaigns.

Source: databreachtoday.com