Executive Viewpoint: Supply Chain Attacks

The SolarWinds supply chain attack exploited a trusted enterprise tool to infect upwards of 18,000 companies worldwide—resulting in damages that may not be fully understood for years to come. This will not be the last supply chain attack. We spoke with Zscaler's Chief Information Security Officer & VP Security Research, Deepen Desai, to learn how to protect your organization against supply chain attacks.

Deepen Desai

CHIEF INFORMATION SECURITY OFFICER & VP SECURITY RESEARCH

Deepen Desai, Chief Information Security Officer & VP Security Research at Zscaler, is responsible for global security research operations and working with product teams to ensure that the Zscaler platform and services are secure. Deepen has been a cybersecurity leader for 15 years, with seven of those years at Dell SonicWALL.

ENGAGE WITH ZSCALER THREATLABZ FOR SUPPORT

Get expert help from our world-class threat research team to help you understand your risk, assess impact, and improve your security posture.

zscaler™

Q: How are supply chain attacks different from a data breach?

Supply chain attacks exploit legitimate tools that are already trusted within your ecosystem to gain access to your network—injecting malware and backdoors into software patches and updates. These attacks can infect hundreds or thousands of companies at once without discovery.

Q: What technology safeguards are necessary for robust protection?

- **Zero trust architecture and policy:** Reducing the attack surface and limiting lateral movement through a zero trust architecture is a critical safeguard. This isolation must restrict internet access – if a third-party app needs access for software updates, for example, it should only be able to access the relevant software update servers.
- **Strong C2 prevention:** Your security stack must block access to all known command and control (C2) servers on all ports and must inspect all encrypted and unencrypted traffic and authenticate each new request in order to detect and stop abnormal activity.
- **Identify and stop unknown malware.** Behavioral analysis (sandbox) and advanced analytics that leverage machine learning are crucial to detecting unknown malware and abnormal behaviors. If a threat actor tries to move laterally and deploy additional tools on the network, these capabilities can detect these tactics and payloads before they cause additional harm.
- **DLP to prevent potential data theft.** Data loss prevention (DLP) tools provide in-line inspection of all outgoing traffic to ensure that sensitive data is not leaked or exfiltrated. DLP also ensures a security team can control the data leaving the network.

Q: How will supply chain attacks evolve in the future?

We'll start to see multi-tier supply chain attacks as adversaries become more advanced: they could breach one software vendor to gain access to their customers' networks. Some of those customers could also be software companies, and adversaries will attempt to infect those companies' software updates to reach even more organizations.

Q: How does Zscaler differentiate itself for supply chain attack protection?

Zscaler's Zero Trust Exchange is a cloud-native platform that redefines what is possible for zero trust. Instead of granting users access to a subset of the company's data and systems (as is the case with traditional network segmentation), Zscaler connects individual users and applications directly to the resources that they need, inspecting and authenticating each individual connection at a speed and scale that no other security vendor can match. With Zscaler's unique proxy-based architecture, adversaries can't hide in encrypted traffic without being detected—and if they ever do breach a component, they can't move freely through the network or communicate with C2 servers or payloads. All of this means unmatched protection against supply chain attacks. ■

CSO FROM IDG

SPONSORED CONTENT