BUSINESS BRIEF

REVERSINGLABS

Software Supply Chain Security for the SOC

Introduction

Threat actors rely on stealth to launch successful attacks. They persist in developing sophisticated attacks designed to evade detection. Security leaders continue to experience malware delivered through email, malicious domains and software vulnerabilities like Log4j. In the continuously evolving threat landscape, we are seeing explosive growth in a new attack vector - Software Supply Chain attacks.

What's driving this? Software Supply Chain attacks provide a more efficient and stealthier means for cybercriminals and nation-state adversaries to gain access to thousands of targets.

Security leaders are realizing that Software Supply Chain threats are not going away and will continue to evolve in sophistications.

289%

growth in supply chain threat to open-source repositories (NPM, PiPy...)

ReversingLabs

70%

of SBOMs for software developed for internal open-source code

TAG Cyber

45%

of organizations will experience a software supply chain attack by 2025

Gartner

59%

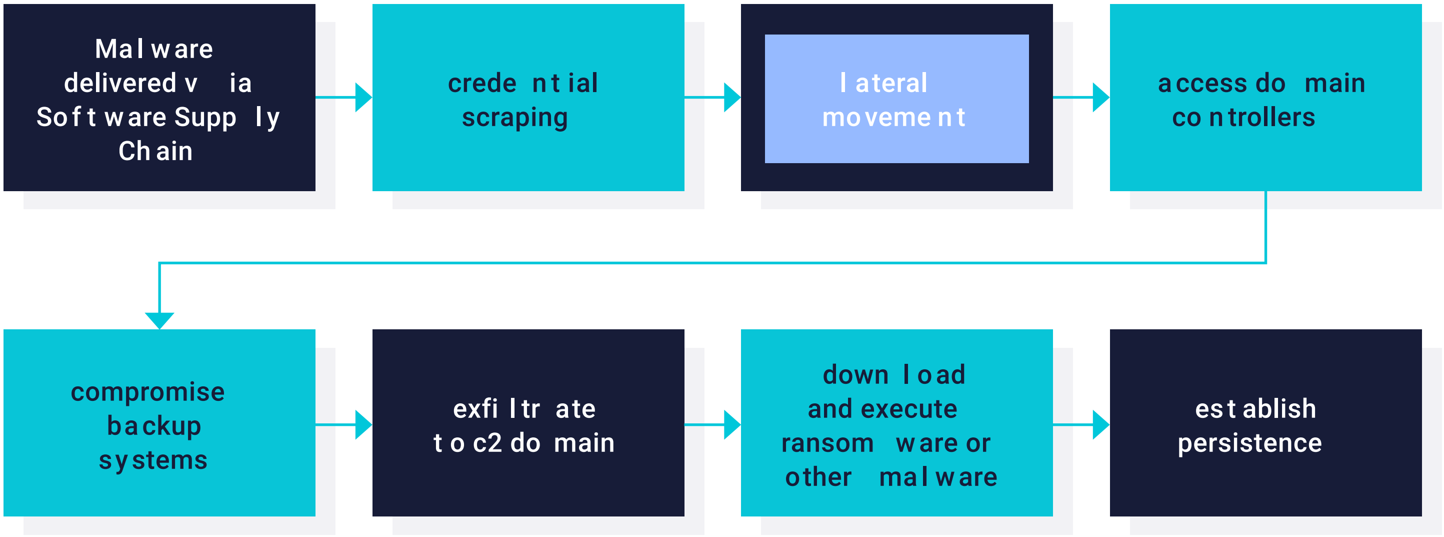
of organizations that suffered a software supply chain attack did not have a response strategy

PurpleSec

Software Supply Chain Attacks Evade Existing Security Tools

Software Supply Chain attacks pose a new set of challenges for security teams. Commercial software provides malware authors with larger and more complex packages to hide their malicious code from existing security tools:

- The files are several gigabytes in size.
- They have tens of thousands of executable components
- They contain hundreds of thousands of files.
- They take a long time to analyze


Malware delivered via Software Supply Chain
credential scraping
lateral movement
access domain controllers
compromise backup systems
exfiltrate to c2 domain
download and execute ransomware or other malware
establish persistence

Attacker Tactics, Techniques and Processes

Following the initial compromise, the damage done by Software Supply Chain attacks quickly piles up against security teams. Once in, threat actors scrape credentials and move laterally across the network.

They often target two key components of your IT infrastructure. By escalating privileges, they gain control over domain controllers providing access to all resources on the network. And they compromise back-up systems, impacting recovery of infected systems.

At this point in the attack, attackers know the devices on your network, their credentials, and installed software which they post on the deep and dark web for use by other adversaries. Most attacks involve dropping multiple malware packages, including Ransomware and highly destructive Disk Wiping.

Lastly, once is not enough to threat actors. They apply various methods, such as altering registry or startup folders, to establish persistence to repeatedly attack their victims.

To combat these advanced Software Supply Chain threats, security leaders need to look at new TTPs and technologies to respond early in an attack and to remediate the entire attack life cycle. ReversingLabs customers come to us for an advance malware analysis solution that:

- Delivers deep visibility to accurately convict malicious code hiding in large and complex software
- Works in concert with other security tools to effectively contain and remediate the attack
- Provides early warning into emerging threat to proactively prepare response strategies
- Seamlessly integrates with existing SOC workflows

ReversingLabs Software Supply Chain Security for the SOC

ReversingLabs combines the most advanced malware analysis engine with a highly scalable architecture and the largest commercial repository of goodware and malware to protect your organization from Software Supply Chain, Ransomware and other file-based attacks.

How We Solve the Problem

Recursive Binary Analysis

Delivers unmatched visibility into malware and their behaviors. Superior file decomposition:

- Exposes malicious code hiding in deep layers of complex software.
- Indicator and metadata extraction reveals the full life cycle of an attack

Scalable, High-Volume Processing

Clustered architecture incrementally scales to process:

- Large software files that exceed the capacity of other solutions
- Very large quantity of files quickly without disrupting IT operations

Curated File-Threat Intelligence

Largest commercial repository of goodware and malware.

- Pre-processed by RL Recursive Binary analysis.
- Delivers detailed intelligence to proactively identify and prevent emerging threats.

Baselining File Security

Fast and easy snapshot of all files in your environment

- SBOM for a complete inventory of all files. Important for compliance with gov't regulations and Executive Orders
- Deep scan of all files for fast classification, Goodware or Malware, on-prem and cloud

Purpose Built SOC Portal

Intuitive dashboards deliver common source of the truth for more efficient and effective response to malware threats

- Deep visibility to eradicate the full life cycle of and attack
- Improved communication and coordination for faster and more accurate decisions

Delivering Outcomes That Matter Most

- ✓ Reduced business risk from Software Supply Chain, Ransomware, and other malicious packages
- ✓ Reduced reliance on hard to find and retain malware analysis expertise.
- ✓ Enriched SOC operations to improve detection and response efficacy
- ✓ Proactively prevents new and emerging threats.
- ✓ Increased detection capabilities and value of other security tools.

Get Started!

REQUEST A DEMO

www.reversinglabs.com

About ReversingLabs

ReversingLabs, the leader in software supply chain security, offers the only holistic software supply chain solution that secures third-party software and open source components and identifies active threats. ReversingLabs provides protection against malware and tampering in pre and active production. For more information or to schedule a demo, contact us today.

REVERSINGLABS

Worldwide Sales : +1.617.250.7518
sales@reversinglabs.com