REVERSINGLABS

SOLUTION BRIEF

ReversingLabs secure.software

Rising risk of revenue-impacting software supply chain security attacks

Software supply chain security attacks are devastating because a single release containing malicious changes can simultaneously affect a considerable number of companies. There are also long-term ramifications for software publishers that unwittingly distributed malicious changes to their releases and updates. The 2021 Ponemon-IBM research[1] indicates that almost half of the breach costs occur after the first 12 months and 38% of total breach costs are from lost business stemming from loss of customer trust and business reputation.

Recent survey of more than 300 global IT and security professionals[2], indicates that 37 percent have a way to detect software tampering across their software supply chain (i.e. open source, third-party, and proprietary software and their dependencies). Of those that can detect software tampering, just seven percent do it at each phase of the software development lifecycle – which means that malicious changes are invisible to most software publishers. When taken together with the ever increasing frequency of software releases and updates, this lack of visibility significantly increases the likelihood of software supply chain security incidents that ultimately impact software revenue.

How it works

SUBMIT & ANALYZE
Rapidly analyze large release packages, containers, open source libraries, and third-party software for threats

REVIEW & FIX
Find the important stuff, and remediate the big risks buried deep within layers of software dependencies

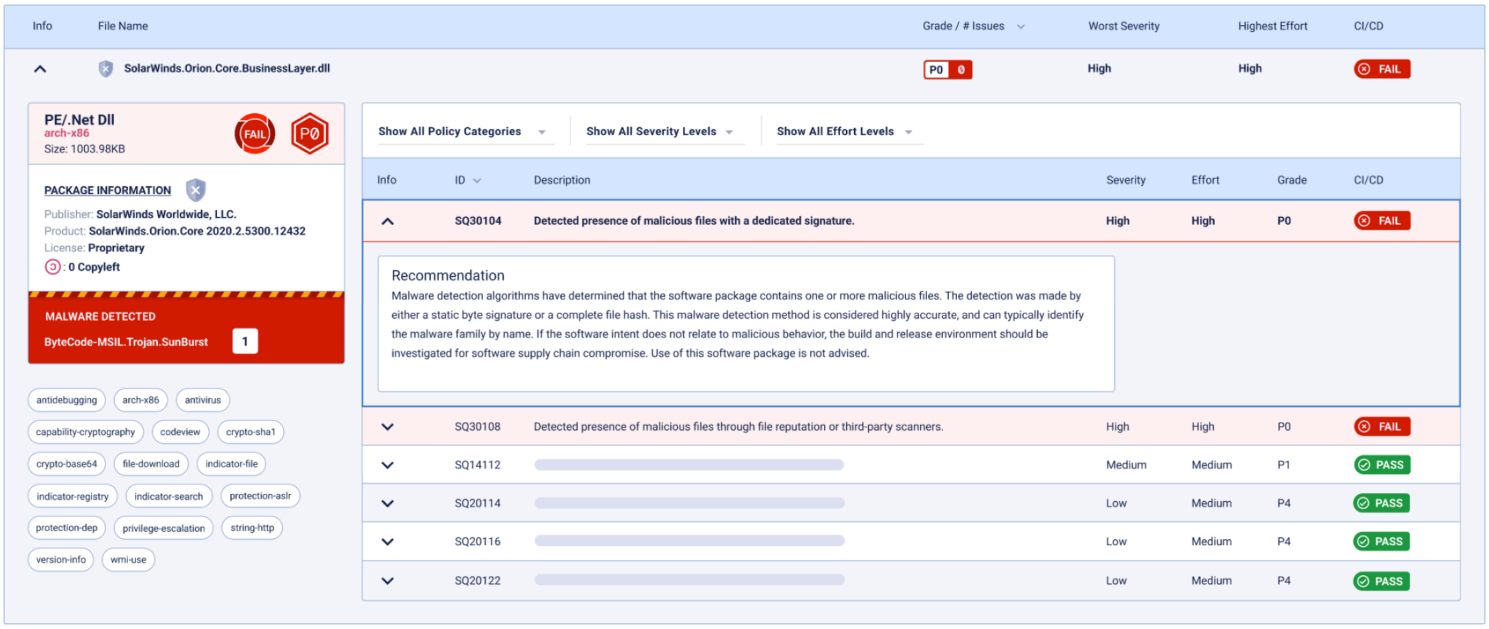
VERIFY & RELEASE
Confidently confirm security quality and keep customers loving your awesome code.

Analyze Software For Supply Chain Security Threats

ReversingLabs secure.software provides software supply chain security protection for CI/CD workflows, containers, and release packages. It is the only integrated platform that detects when high-risk threats, exposures, and software tampering (i.e. unauthorized changes with malicious intent) take place across the software development cycle and at the speed needed to keep release cycles on time. The platform enables CTOs to understand when malicious changes to their software could threaten customers' deployments and ensure remediations required to keep customers' trust intact are implemented.

Application architects can complement existing application security investments, which are good at finding vulnerabilities across the development lifecycle, but cannot detect modern software supply chain attacks. ReversingLabs secure.software digs deep into the many layers of software, components, and dependencies, regardless of toolchain choices or the size of builds, releases, or containers being analyzed. It detects unauthorized software changes, malware or backdoors, and exposed secrets that can be used in software supply chain attacks. The platform empowers teams to implement and automate new workflows, toolchain integrations, software assessments, approval policies, and remediation validation to prevent threats from reaching production environments without impacting developer productivity.

DevSecOps teams can confidently release software by utilizing the platform's actionable developer-ready remediation prioritization to remove high risk threats and exposed secrets without impacting speed of release. The platform also minimizes developers' effort required for other security-related tasks, such as auditing secure development practices, providing data for corporate compliance or vendor risk management teams, and creating software bills of materials (SBOM) with automated report generation.



Info	File Name	Grade / # Issues	Worst Severity	Highest Effort	CI/CD
^	SolarWinds.Orion.Core.BusinessLayer.dll	P0 0	High	High	FAIL

PE/.Net Dll
arch-x86
Size: 1003.98KB
FAIL P0

PACKAGE INFORMATION

Publisher: SolarWinds Worldwide, LLC.
Product: SolarWinds.Orion.Core 2020.2.5300.12432
License: Proprietary
: 0 Copyleft

MALWARE DETECTED
ByteCode-MSIL.Trojan.SunBurst 1

antidebugging, arch-x86, antivirus, capability-cryptography, codeview, crypto-sha1, crypto-base64, file-download, indicator-file, indicator-registry, indicator-search, protection-aslr, protection-dep, privilege-escalation, string-http, version-info, wmi-use

Show All Policy Categories | Show All Severity Levels | Show All Effort Levels

Info	ID	Description	Severity	Effort	Grade	CI/CD
^	SQ30104	Detected presence of malicious files with a dedicated signature.	High	High	P0	FAIL

Recommendation
Malware detection algorithms have determined that the software package contains one or more malicious files. The detection was made by either a static byte signature or a complete file hash. This malware detection method is considered highly accurate, and can typically identify the malware family by name. If the software intent does not relate to malicious behavior, the build and release environment should be investigated for software supply chain compromise. Use of this software package is not advised.

Info	ID	Description	Severity	Effort	Grade	CI/CD
v	SQ30108	Detected presence of malicious files through file reputation or third-party scanners.	High	High	P0	FAIL
v	SQ14112		Medium	Medium	P1	PASS
v	SQ20114		Low	Medium	P4	PASS
v	SQ20116		Low	Medium	P4	PASS
v	SQ20122		Low	Medium	P4	PASS

Figure1: Sunburst attack identified by malware analysis and suspicious behavior changes[3]

Secure Software Releases

Challenge: Prevent Software Supply Chain Threats From Reaching Production

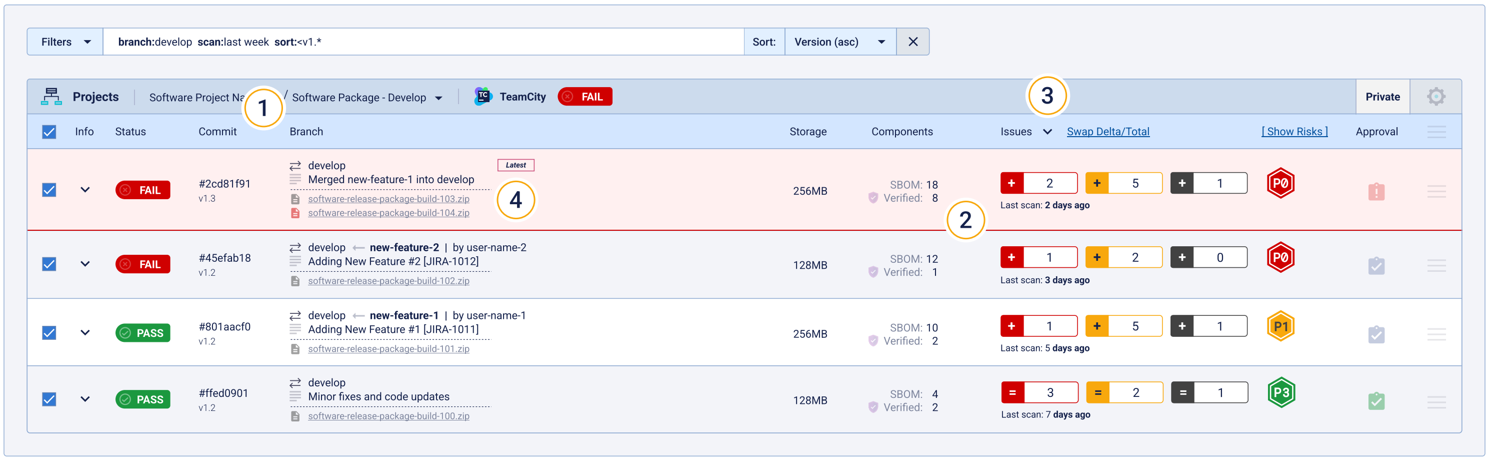
- Software supply chain threats and attacks have outpaced current detection tooling
- Software release packages and containers can be too big, with too many layers of dependencies to scan effectively
- Scanning without reporting the discovered components (e.g. SBOM) creates a false sense of security

Solution: Perform Critical Checks On Final Release Packages As A Last Line Of Defense

- Find & stop tampering, malware and other supply chain attacks by pinpointing unexpected or suspicious behaviors within any software component (See Figure)
- Find and eliminate exposed secrets (e.g. credentials, private keys and access tokens) that can be used in future CI/CD attacks
- Verify that appropriate vulnerability mitigations are correctly implemented
- Validate that critical remediations are completed by comparing subsequent release package
- Analyzes the entire release package, regardless of:
  - Layers and layers of dependencies
  - Size of package or container
  - Toolchain or file compression choices

Benefits

- Reduced loss of customer trust and long term revenue
- Closes security testing gap while maintaining development velocity
- Increased confidence in secure software releases
- Minimized release delays by prioritizing critical deployment threats for remediation



Filters ▾ | **branch:**develop **scan:**last week **sort:**<v1.* | Sort: Version (asc) ▾ | ✕

Projects | Software Project Na… / Software Package - Develop ▾ | TeamCity FAIL | Private

☑	Info	Status	Commit	Branch	Storage	Components	Issues ⌄ Swap Delta/Total	[Show Risks]	Approval
☑	⌄	FAIL	#2cd81f91 v1.3	develop Merged new-feature-1 into develop *Latest* software-release-package-build-103.zip software-release-package-build-104.zip	256MB	SBOM: 18 Verified: 8	+ 2 + 5 + 1 Last scan: **2 days ago**	P0	!
☑	⌄	FAIL	#45efab18 v1.2	develop ⟵ **new-feature-2** | by user-name-2 Adding New Feature #2 [JIRA-1012] software-release-package-build-102.zip	128MB	SBOM: 12 Verified: 1	+ 1 + 2 + 0 Last scan: **3 days ago**	P0	✓
☑	⌄	PASS	#801aacf0 v1.2	develop ⟵ **new-feature-1** | by user-name-1 Adding New Feature #1 [JIRA-1011] software-release-package-build-101.zip	256MB	SBOM: 10 Verified: 2	+ 1 + 5 + 1 Last scan: 5 **days ago**	P1	✓
☑	⌄	PASS	#ffed0901 v1.2	develop Minor fixes and code updates software-release-package-build-100.zip	128MB	SBOM: 4 Verified: 2	= 3 = 2 = 1 Last scan: 7 **days ago**	P3	✓

Secure CI/CD Workflows

Challenge: Software Supply Chain Attacks Happen At Each Stage

- Sophisticated attacks on CI/CD workflows and systems are difficult to detect
- Well hidden changes that mimic developer coding style very hard to spot during manual code reviews

Solution: Shift Left To Detect Software Tampering At DevSecOps Speed

1. Find & stop tampering, malware and other supply chain attacks by pinpointing unexpected or suspicious behaviors within any software component (See Figure)
2. Choose more secure components by tracking changes in security quality as new components are added
3. Tracks approval status against customizable build failure conditions, to enable developers to address problems before code review submission
4. Check for build system compromise by automating "reproducible build" workflows,comparisons, and reporting

Benefits: Halt attacks earlier and more effectively

- Increased security quality while maintaining developer productivity
- Faster discovery of supply chain attacks, i.e. when build tampering occurs rather than when customer breaches are reported
- Enables DevSecOps platform and culture
- Improved automation of supply chain security guardrails earlier in the CI/CD
- Decreased remediation times as issues are detected earlier in the software lifecycle

2022 GLOBEE AWARDS GOLD WINNER
CYBER SECURITY GLOBAL EXCELLENCE

CYBER SECURITY EXCELLENCE AWARDS
★ WINNER ★
2022

2021 WINNER
SC awards

BLACK UNICORN AWARDS
WINNER

SILVER
2020 STEVIE WINNER
AMERICAN BUSINESS AWARDS

Additional Resources:

Experience our interactive reports

Learn more

Sample Software Supply Chain Security Reports

CHECK OUT OUR INTERACTIVE REPORTS THAT HELP YOU TO HALT ATTACKS AND IMPROVE SECURITY QUALITY

Are We Flying Blind?

A survey of >300 software development companies reveals deep concerns about the inability to deliver secure software

Download Report

ЯEVERSINGLABS

Flying Blind: Software Firms Struggle To Detect Supply Chain Hacks

ReversingLabs supports many languages and repository packages to deliver software supply chain protection for CI/CD workflows, containers and release packages.

See us in action

Get a personalized demo to see how we protect your development lifecycle from software supply chain threats

REQUEST A DEMO

Sources:

[1] 2021 Ponemon IBM Cost of a Data Breach Report https://www.ibm.com/security/data-breach

[2] Flying Blind: Software Firms Struggle to Detect Supply Chain Hacks https://www.reversinglabs.com/reports/flying-blind-software-firms-struggle-to-detect-supply-chain-hacks

[3] https://blog.reversinglabs.com/blog/sunburst-the-next-level-of-stealth

Worldwide Sale:
+1.617.250.7518
sales@reversinglabs.com