Scanning for Counterfeits and Insertion of Malicious Code
NIST SP 800-161

NIST SP 800-161 revised 1/11/2024 states:

"Organizations are concerned about the risks associated with products and services that may potentially contain malicious functionality, are counterfeit, or are vulnerable due to poor manufacturing and development practices within the supply chain. These risks are associated with an enterprise's decreased visibility into and understanding of how the technology they acquire is developed, integrated, and deployed or the processes, procedures, standards, and practices used to ensure the security, resilience, reliability, safety, integrity, and quality of the products and services."[1]

"The insertion of malicious code and counterfeits are two primary examples of cybersecurity risks throughout the supply chain."[2] SR-11 directs a "minimum" scan for counterfeits.[3]

Supply Chain Risk is amplified by the fact that software vendors do not know what is in their code. SI-3 specifically states that "Because the majority of code operated in federal systems is not developed by the Federal Government, malicious code threats often originate from the supply chain."[4] This applies to any organization using third-party software.

Unknown Cyber, an In-Q-Tel portfolio company, controls for supply chain and third-party software risk through continuous scanning at C-SCRM Baseline, Flow Down, or Levels 2 & 3.

Unknown Cyber's Software Scan scans software binary code at the function level using a method orthogonal to traditional static and dynamic solutions. This allows automated code assurance at scale so organizations can in minutes scan for counterfeits, and insertion of malicious code that has entered the supply chain. Software Scan saves thousands of hours of expert time through automation. This allows risk managers to automatically identify what is not found by other solutions, automating inventory reviews and updates from baseline configurations (i.e., re-baselining) to establish traceability and provenance. Software Scan automates the analysis needed to know when code contains malicious functionality, is counterfeit, or is exploitable due to poor manufacturing. (Software Scan demonstrates novel detections with our detection of Solar Winds exploit code, trojanized DLLs, counterfeit or stolen software, and attack methods that remain undetectable to AV, Sandbox, and other behavior-based solutions.

Software Scan assures against Software Supply Chain Risk helping organizations trust their legacy code base, assure open-source and unsupported code, and conduct audits and assessments of software products that lack the provision of source code. Software Scan provides the control needed for situations where malicious code cannot be detected as discussed in NIST SP 800-53, REV. 5

[1] NIST.SP.800-161r1-upd1, 2024, p. i
[2] NIST.SP.800-161r1-upd1, 2024, p. 154
[3] NIST.SP.800-161r1-upd1, 2024, p. 161-162
[4] NIST.SP.800-161r1-upd1, 2024, p. 155

Contact Us:
info@UnknownCyber.com
www.UnknownCyber.com

"In situations where malicious code cannot be detected... (other controls are needed) to ensure that software does not perform functions other than the functions intended."[5] Automated scanning for these risks is the only scalable solution. Organizations using Software Scan reduce both cost and risk with automation.

In addition to being able to conduct an automated scan to identify counterfeits and malicious functionality that enters supply chains due to decreased visibility into third-party software, Software Scan helps organizations achieve the security requirements for [FIPS200] as follows.

[FIPS200] "Organizations must at a minimum:"

- Identify system flaws in a timely manner.[6]
- Provide protection from malicious code. [6]
- Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.[6] (Software Scan can be used as an internal or external audit tool.)
- Establish and maintain baseline configurations and inventories of software.[7]
- Ensure that third-party providers employ adequate security measures.[8]

SR-11 in provides new guidance for Supply Chain Risk Management to expand upon the controls in SP 800-53, Rev. 5. Section 3 requires Anti-Counterfeit Scanning and states "Enterprises should conduct anti-counterfeit scanning for critical components, at a minimum."[9]

This is a key capability that Software Scan offers that cannot be obtained through other automated solutions. Software Scan will search through the code for counterfeit components using automated scanning from Baseline. The usefulness of this method can be demonstrated in Software Scan's recent identification of a counterfeit trojanized DLL. NIST SP 800-161 further emphasizes that detecting counterfeits may require significant resources. Using Software Scan to automate scanning as required in the SR-11 control will reduce cost by eliminating time consuming manual workflows for compliance or audits. This while also meeting [FIPS200] requirements for timeliness, protection from malicious code, continuous monitoring of baseline and inventory, and assurance that third-party providers employ adequate security measures.

NIST SP 800-161 goes on to state that Enterprises should integrate C-SCRM controls to include:

- Activities to assess the verification of suppliers' claims of conformance to security[10]
- Product/ component integrity[10]
- Detection of counterfeits or malware (e.g., Trojans) using inspection for genuine components, including manual inspection techniques.[10]

Bottom line, Software Scan provides cost savings, time savings and reduces risk by providing the ability to conduct scans of entire binaries to satisfy the minimum C-SCRM requirements of NIST SP 800-161 and NIST SP 800-53, thereby assuring against unanticipated changes or the introduction of counterfeit, malicious, exploitable, or unaccounted for code. Software Scan empowers organizations that are concerned about unmitigated risks in their software, or vendors' software with a solution to scan for hidden malicious functionality, and counterfeits that have entered their supply chain. With Software Scan organizations have and automated option to conduct due-diligence into code for which they have limited visibility.

[5] NIST SP 800-53, REV. 5, 2020, p. 335
[6] NIST.SP.800-161r1-upd1, 2024, p. 153
[7] NIST.SP.800-161r1-upd1, 2024, p. 87
[8] NIST.SP.800-161r1-upd1, 2024, p. 136
[9] NIST.SP.800-161r1-upd1, 2024, p. 162
[10] NIST.SP.800-161r1-upd1, 2024, p. 84

Contact Us:
info@UnknownCyber.com
www.UnknownCyber.com

Below you see real world results of Unknown Cyber's automated analysis of binary code. This document shows the trojanization of supply chain responsible for the insertion of a Salt Typhoon manufactured variant of attributed Snappybee Malware. Salt Typhoon is the CCP threat actor responsible for the recent attack which compromised telecoms and classified wiretaps. Unknown Cyber's automated analysis of software tracked the evolution of updates from baseline to the point Salt Typhoon counterfeited an update using their Snappybee trojanized binary. Unknown Cyber immediately found this trojanization through code comparison at scale. Please note the fidelity which Unknown Cyber has in identifying this single function inside the counterfeit update responsible for trojanization. You can see the evolution of the open-source Sandboxie Software through licensed versions which ultimately culminates in the trojanization of IO Bit Software. Identification of the insertion of this malicious code can easily be seen by Unknown Cyber's ability to observe the statistical similarity of the code updates. The .999 similarity score you see hi-lighted is representative of the IO Bit Software being 99.9% the same as the trojanized IO Bit Snappybee malware variant. The one added function (.01%) of inserted code is responsible for a series of subsequently executed fileless malware deployed in memory. These we also have unique capability to detect. I don't want to get too far into the details of extended capabilities for fileless malware detection because just the ability to identify the insertion of malicious code and counterfeits down to a single function through similarity of binary is a novel technical breakthrough in it's own right. This innovation stands on its own as a scalable way to deliver inspection of software for unknown malicious code and vulnerabilities in supply chain with accuracy and scale not resident in other solutions.