28-Aug-2023

Supply Chain Risk: **Gaining Trust and Certainty Through Transparency**

Dmitry Raidman
CTO & Co-Founder
@dmraid
dmitry@cybeats.com
dmitry@security-architecture.org

CYBEATS | Software Made Certain

3 Facts About Cybeats

Cybeats is a **Canadian**, Toronto-based **supply chain security** and transparency company

We are a public company listed on the **CSE** as **CYBT.CN**

SBOM Studio considered to be one of the **top** enterprise **SBOM management** solutions

Agenda for the session

I. Examples Software Supply Chain Attacks

II. What happens when we blindly trust?

III. Transparency is necessity not an option

IV. How BOMs can help us in our journey?

V. SBOM Consumers vs Producers and why quality matters?

VI. SBOM vs VEX?

Real Life Examples

*December 13, **2020***

Solarwinds - Software supply chain attack are here to stay.

Supply chain attacks, when attackers turned harmless and trusted software into a weapon, with intent to acquire the ability of infecting anyone who uses it.

https://www.wired.com/story/solarwinds-hack-supply-chain-threats-improvements/

Real Life Examples

*November 24, **2021***

The Log4J Vulnerability Will Haunt the Internet for Years

Attackers will still look for creative new ways to discover and continue exploiting as many vulnerable systems as possible. The scariest part of the Log4Shell, though, is how many organizations won't even realize that they have systems at risk.

https://www.wired.com/story/log4j-log4shell/

Real Life Examples

*March 23, **2023***

Hackers compromise 3CX desktop app in a supply chain attack

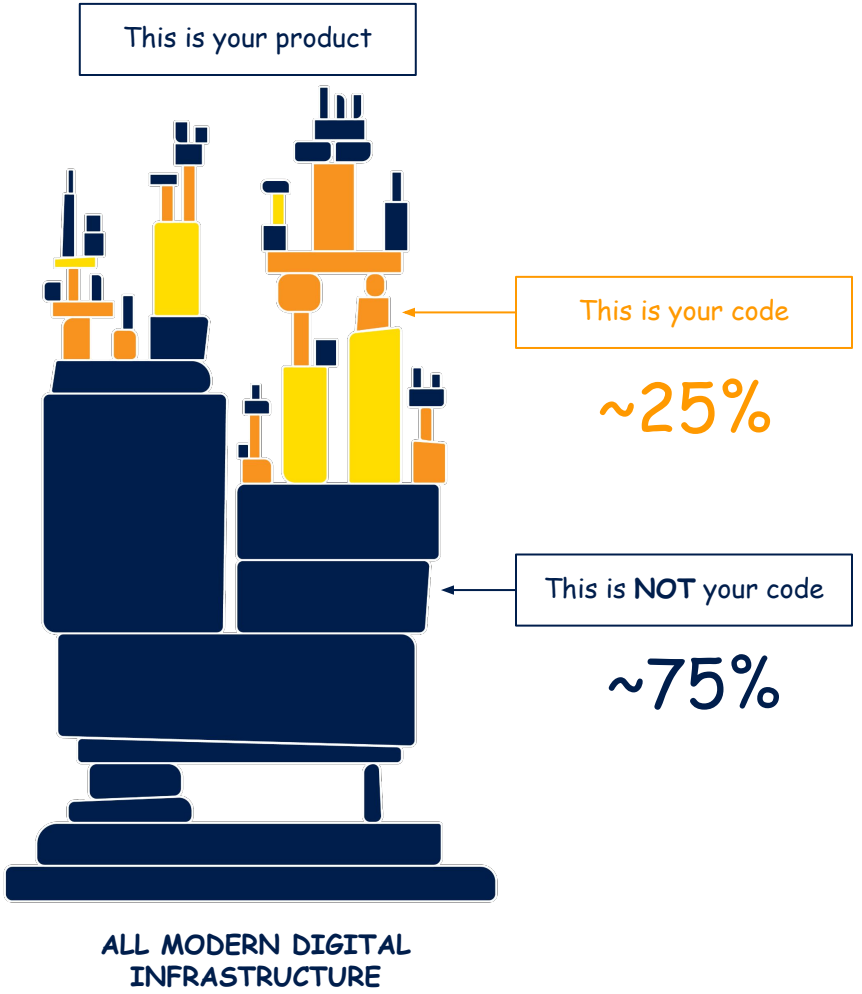
A digitally signed and trojanized version of the 3CX Voice Over Internet Protocol (VOIP) desktop client is reportedly being used to target the company's customers in an ongoing supply chain attack.

600,000 companies worldwide and 12 million daily users

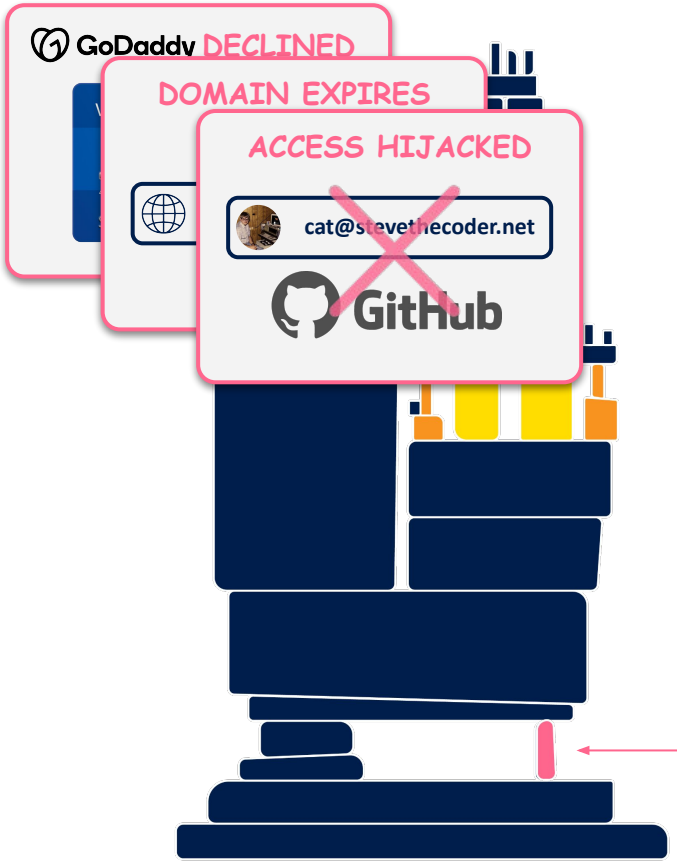
https://www.bleepingcomputer.com/news/security/hackers-compromise-3cx-desktop-app-in-a-supply-chain-attack/

You are as secure as the weakest link of your supply chain

Over **90%** of Commercial Applications Contain **Outdated** or **Abandoned** Open Source Software Components



You are as secure as the weakest link of your supply chain

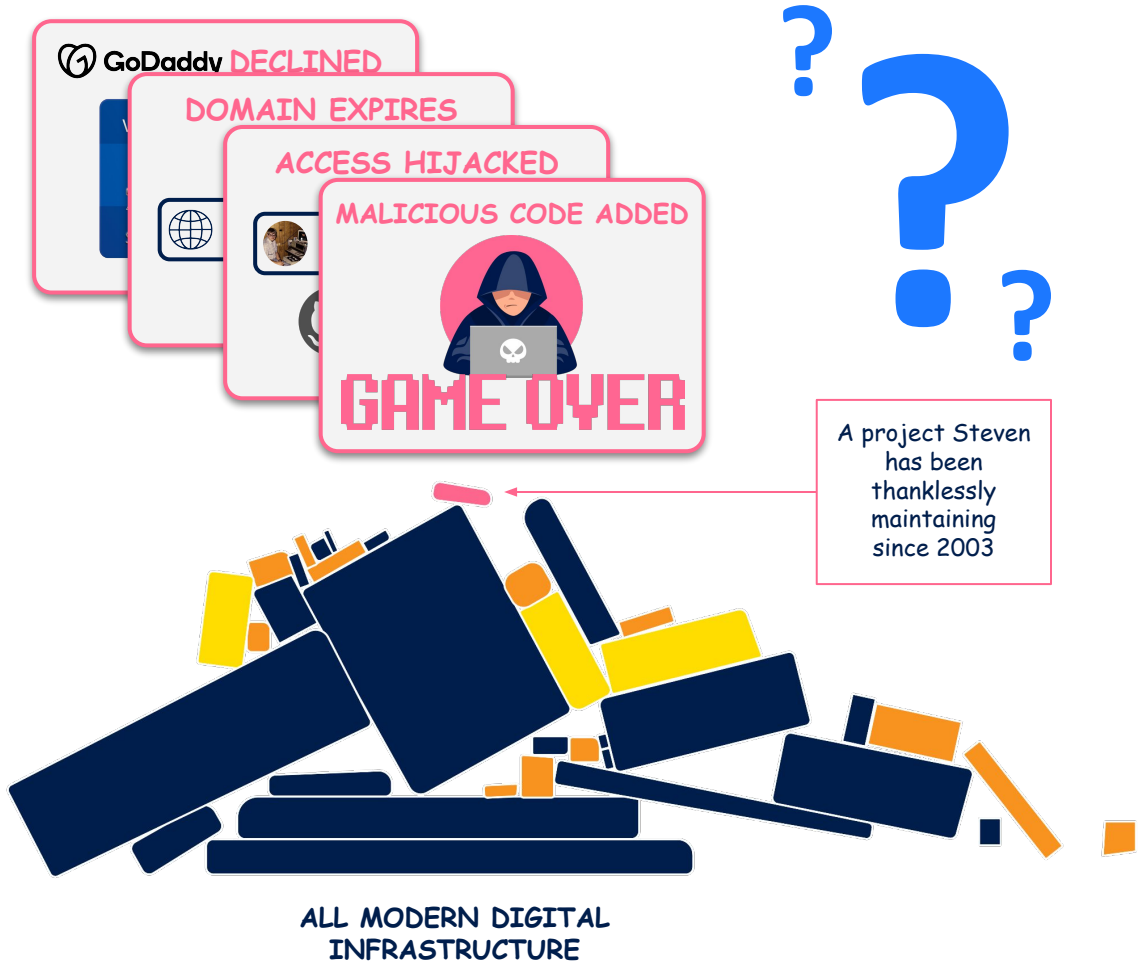


Steven
Callback Cat

- Nebraska
- cats and open source
- ♥ GitHub

A project Steven has been thanklessly maintaining since 2003

You are as secure as the weakest link of your supply chain



Zero Trust in Product **Hardware** Supply Chain **HBOM**

- Electronic components specs, provenance and docs
- Environmental factors
- Trade and tariffs restrictions compliance
- Firmware manipulation
- Hardware based attacks, Spectre Meltdown
- Lifecycle management, discontinued parts
- Market availability

Your Telecom Infrastructure or Mobile Device Product

Zero Trust in Product **Software** Supply Chain **SBOM**

- Dependency reputation, popularity, supply chain intelligence
- Is there newer version how far you are behind?
- Do you carry any OSS license risks?
- Can you get answers in seconds not in weeks?
- Known Exploited Vulnerabilities by CISA/EPSS?
- Software End of Life, End of Support events?
- Anomalous activity in one of your dependencies OSS repos?

Your Telecom Infrastructure or Mobile Device Product

Zero Trust assessment of your **Supply Chain**?

- Are you aware of all software or hardware vulnerabilities?
- Are you aware of Outdated or Abandoned dependencies?
- When was the last time it was assessed for all your products?
- Can you collect and observe all the data in one place?
- Can you trust vulnerable SW or HW?
- What would be the effort to perform it continuously?

Your Telecom Infrastructure or Mobile Device Product

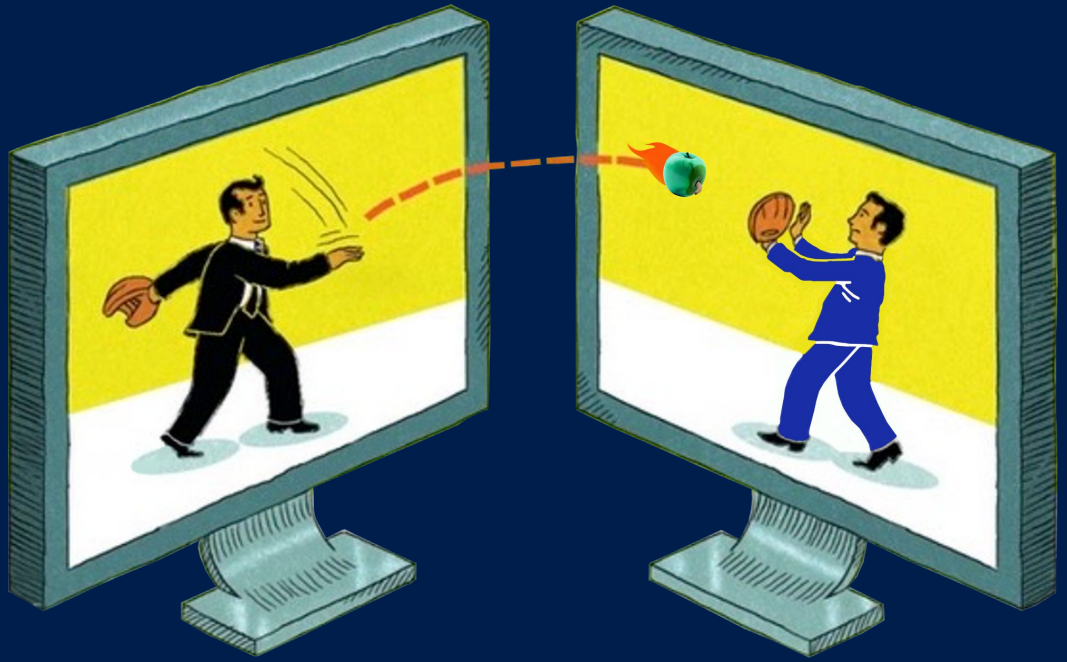
How to improve your **Supply Chain** culture?

NIST SSDF 1.1

NIST SP 800-161

- Create SBOMs and HBOMs for your products
- Receive SBOMs and HBOMs from your vendors
- Gain SBOM management capabilities (ability to asses, validate and import the SBOMs at scale)
- Continuously monitor software and hardware components described in the BOMs
- Gain capabilities to query the BOMs data in one place
- Be proactive on the risks with alerting SIEM and monitoring establish response processes
- Assess risks, utilize VEX and invest in risk mitigation where it makes sense

SBOM Producers vs Consumers



Producers

Consumers

Vulnerabilities

7	Critical
33	High
23	Medium
2	Low
65	Total
✓	No license policy violations

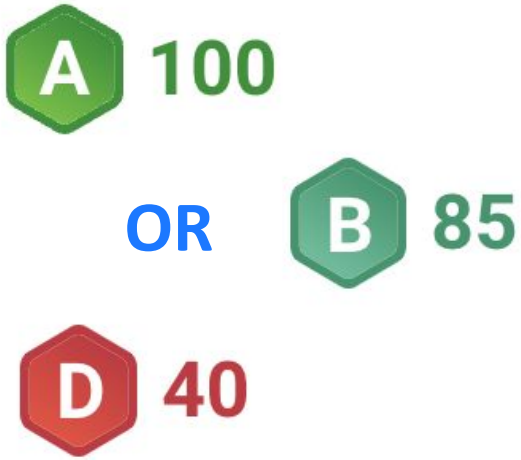
SBOM Producers

- Care about reputation of their organization and products. Have many releases of firmware or software for the same products sometimes between tens to hundreds a year.
- Focusing on protection of their products, customers. Need to be ahead of their customers when it comes to zero day risks.
- Have hundreds to thousands of product with multiple versions some of them are 10 years old and considered to be legacy products but still used by customers.
- Have various compliance framework and certifications FCC, IEC 62443, SSDF, FDA, UL.
- Usually falls under the responsibility of the CPSO and the Product Security team.
- In most of the cases the SBOM Producers are also consumers.

SBOM Consumers

- Care about the risk for their Organization from supply chain products. Multiple different SBOMs HBOMs.
- Focusing on protection of their crown jewels, customers, employees and assets that in many cases data.
- Have variety tens of thousands software or hardware based products on their networks from multiple vendors.
- Following different set of compliance frameworks Zero Trust.
- Have to pass audits on annual basis and comply PCI-DSS, SOC2, ISO 27001, NERC-CIP.
- Usually falls under the responsibility of the CISO and the IT team.

SBOM Future - Quality Matters



Common SBOM Quality Issues

- Invalid SBOMs
- Circular Dependencies
- Missing data in root component or no root component defined
- Missing software identification (cpe, purl, hashes)
- Missing software versions (will lead to false positives)
- No relationships between entities (flat SBOM)
- Missing low level software components (packages, libraries)
- No assembly tool is specified

Questions?

Thank You!

Dmitry Raidman
CTO & Co-Founder
@dmraid
dmitry@cybeats.com
dmitry@security-architecture.org

CYBEATS | Software Made Certain

MFA

SBOM Types

Design SBOM

Describes the intended design for a new software artifact

Source SBOM

Generated from source files, and included dependencies

Build SBOM

Generated as part of the building process of the software to create a releasable artifact

Analyzed SBOM

Generated through analysis of artifacts (e.g., executables, packages, containers, and virtual machine images). Heuristics based analysis.

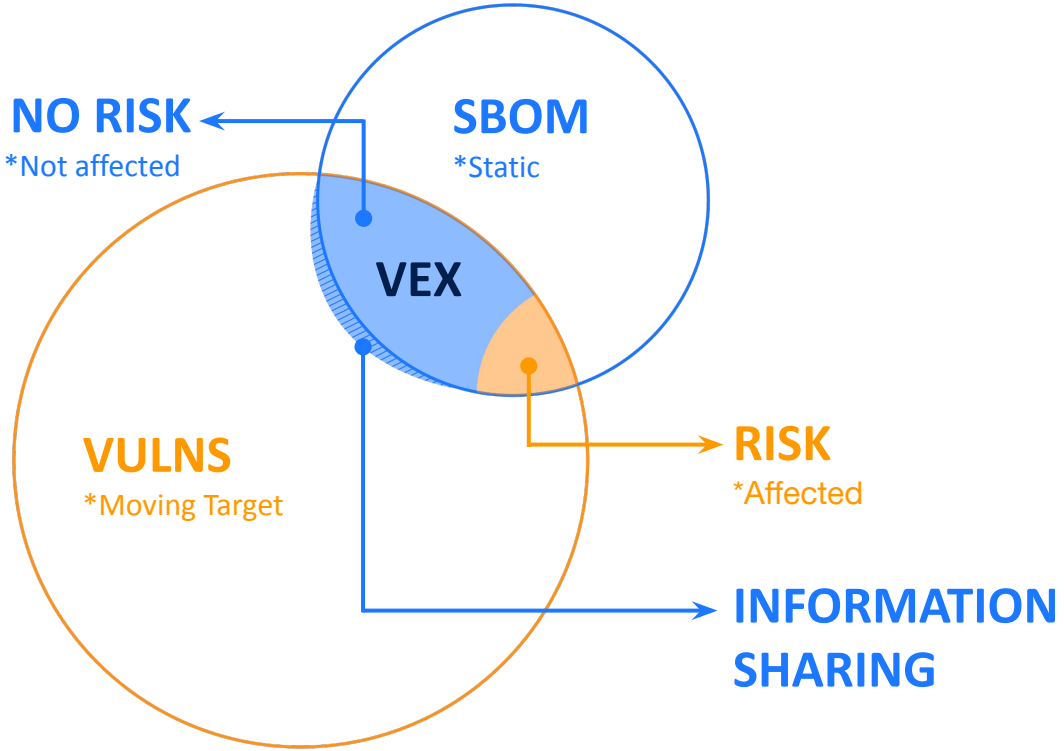
Deployed SBOM

Provides an inventory of software that is present on a system

Runtime SBOM

Captures only components present in the running system, external call-outs and dynamically loaded components

How SBOM ties to VEX



We have LOG4J

- Exploitable
- Not exploitable

We don't have LOG4J

Vulnerability disposition

Security Advisory