Supply-Chain Security

IS THE SOLARWINDS SUNBURST CAMPAIGN AN INFLECTION POINT OR JUST BUSINESS AS USUAL?

BOB SIPES
WWW.LINKEDIN.COM/IN/BOBSIPES
TWITTER: @BOBSIPES

Agenda

- **Introduction**
- **Ground rules and expectations**
- **Short presentation setting the foundation for discussion**
- **Group discussion**
- **Concluding slides and remarks**

Ground Rules

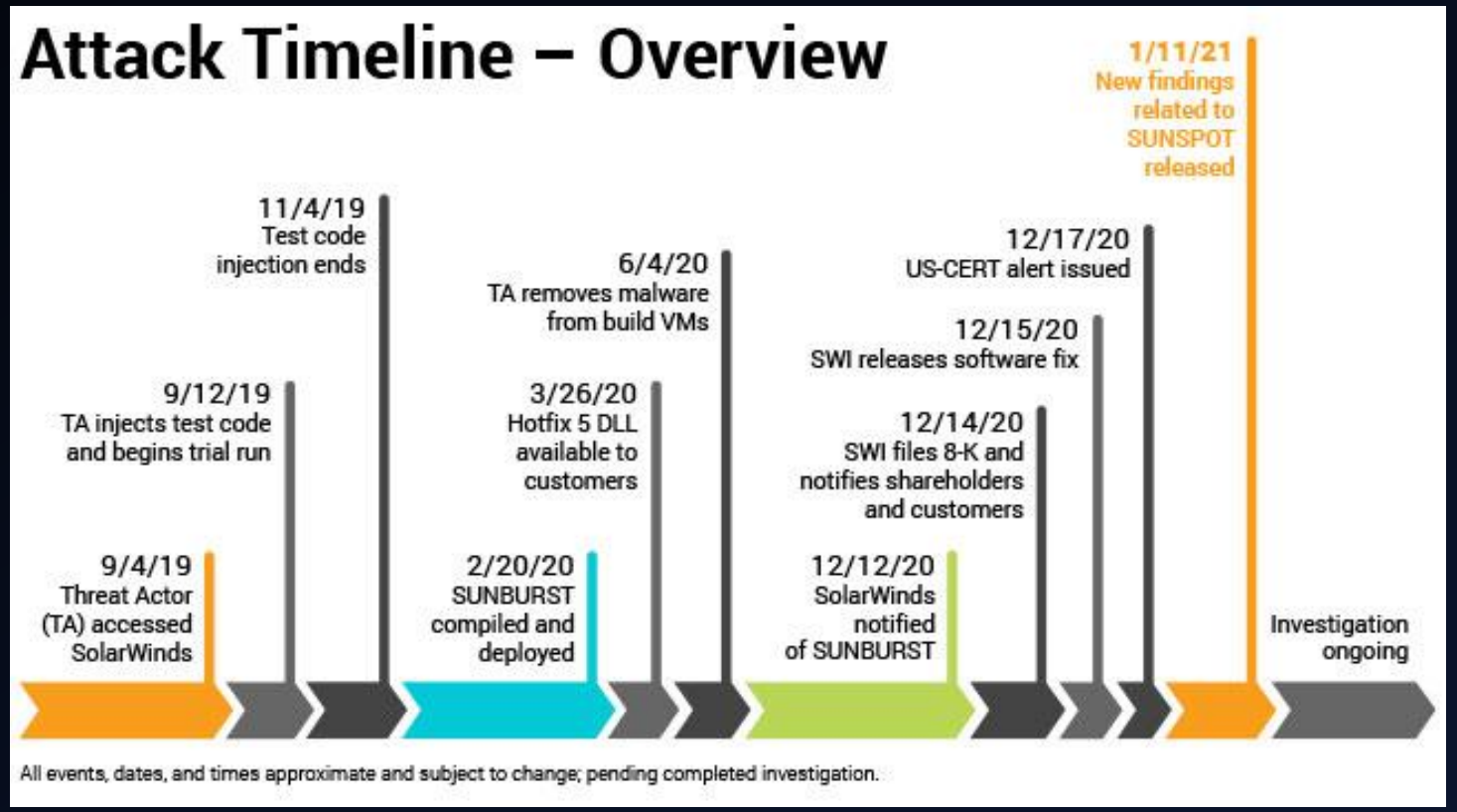
- This presentation and discussion is being recorded.
- Do not provide sensitive information.
- Keep muted unless speaking to reduce background noise

- Please join in the conversation. This is not a panel discussion, but a group discussion.
- Feel free to use the chat to comment or ask questions.
- The questions contained within the presentation are thought and conversation starters.

- Let’s share knowledge and experience, learn from each other and have fun!

SolarWinds Malware Infection Timeline (SolarWinds)

- Test code injected in Oct 2019.
- SUNBURST inserted in releases 20 Feb 2020.
- SUNBURST removed from environment in June 2020.
- Volexity investigates a client incident involving SolarWinds appliances but does not identify SUBURST in July 2020.
- Notified of SUNBURST by FireEye on 12 Dec 2020.



SolarWinds Compromised In 2017?

Intel 471 @Intel471Inc · Dec 16, 2020

Our full statement on our knowledge of SolarWinds and the cybercriminal underground

Most large organizations are going to have multiple security issues that manifest themselves within the underground marketplace in some form or fashion. It's tough to discern whether these are related to a specific incident such as what we're seeing with SolarWinds.

In October 2017, Intel 471 observed the Russian-language actor fxmsp advertise access to SolarWinds on the Exploit cybercrime forum. The actor — a prolific seller of network accesses wanted by the FBI for involvement in several high-profile incidents — allegedly attempted to work his way deeper inside the SolarWinds network and eventually to the source code of its products.

More recently in April 2020, Intel 471 observed a claim by a separate Russian-language actor, Veseliy Arkadiy, alleging to have access to the SolarWind network. The actor also hinted at partnering with the REvil ransomware crew to attack the company. Intel 471 cannot confirm any links between the above events, nor ascertain any direct connections with the supply chain attacks linked to SolarWinds.

Prolific actors are constantly going after high-revenue customers like SolarWinds because they see an increased chance of making larger profits by selling access to ransomware partners and other buyers. Whether it's by exploiting vulnerabilities, launching spam campaigns or leveraging credential abuse, access is typically advertised and auctioned to the highest bidder for a profit. Whether this was the motivation for the current SolarWinds incident remains to be seen.

4 151 384

Vinoth Kumar @vinodsparrow · Dec 14

Was reading about a sophisticated attack on FireEye leveraging Solarwinds. Hmmm how that would happened?🤔. Then realized their password was *****123 🤣 #FireEye #SolarWinds

Open Github Repo Leaking FTP Credentials of http://downloads.solarwinds.com

Vinoth Kumar
Tue 2019-11-19 14:32
To: psirt@solarwinds.com

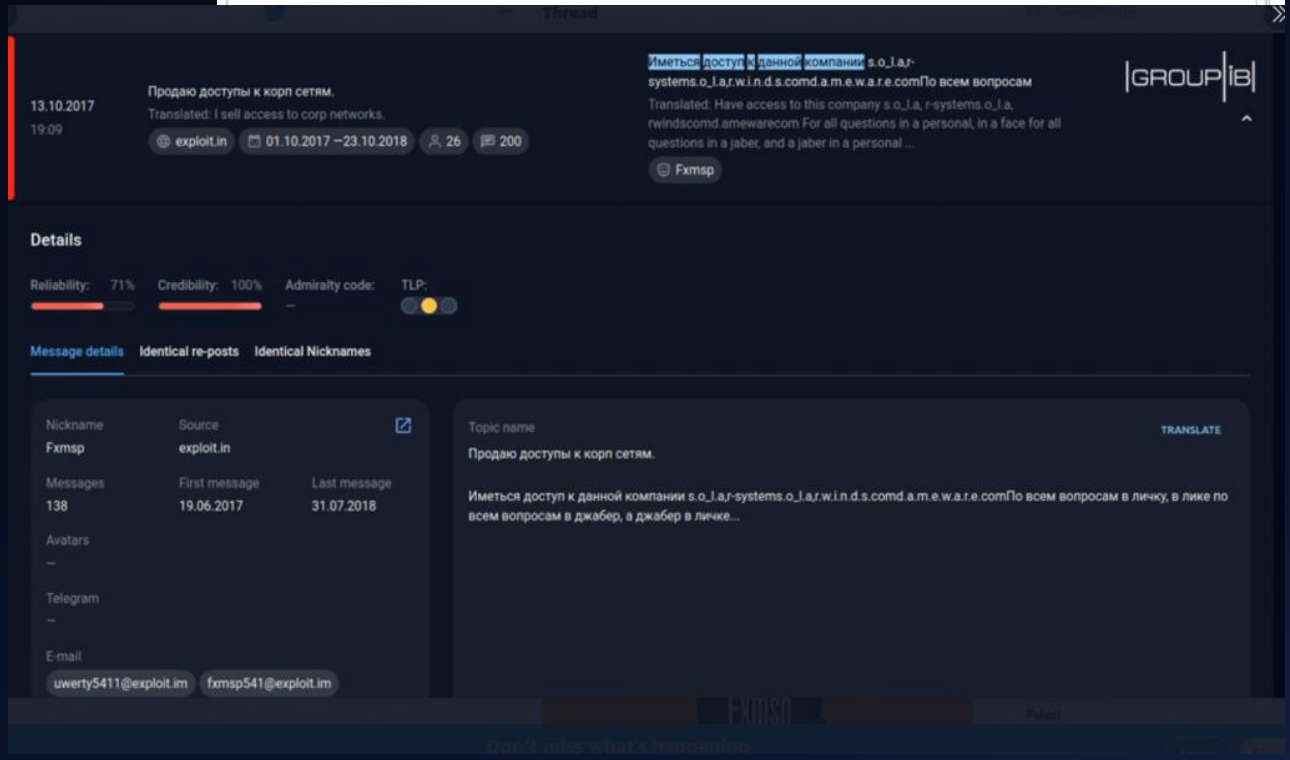
Hi Team,

I have found a public Github repo which is leaking ftp credential belongs to SolarWinds.

Repo URL: https://github.com/ .config

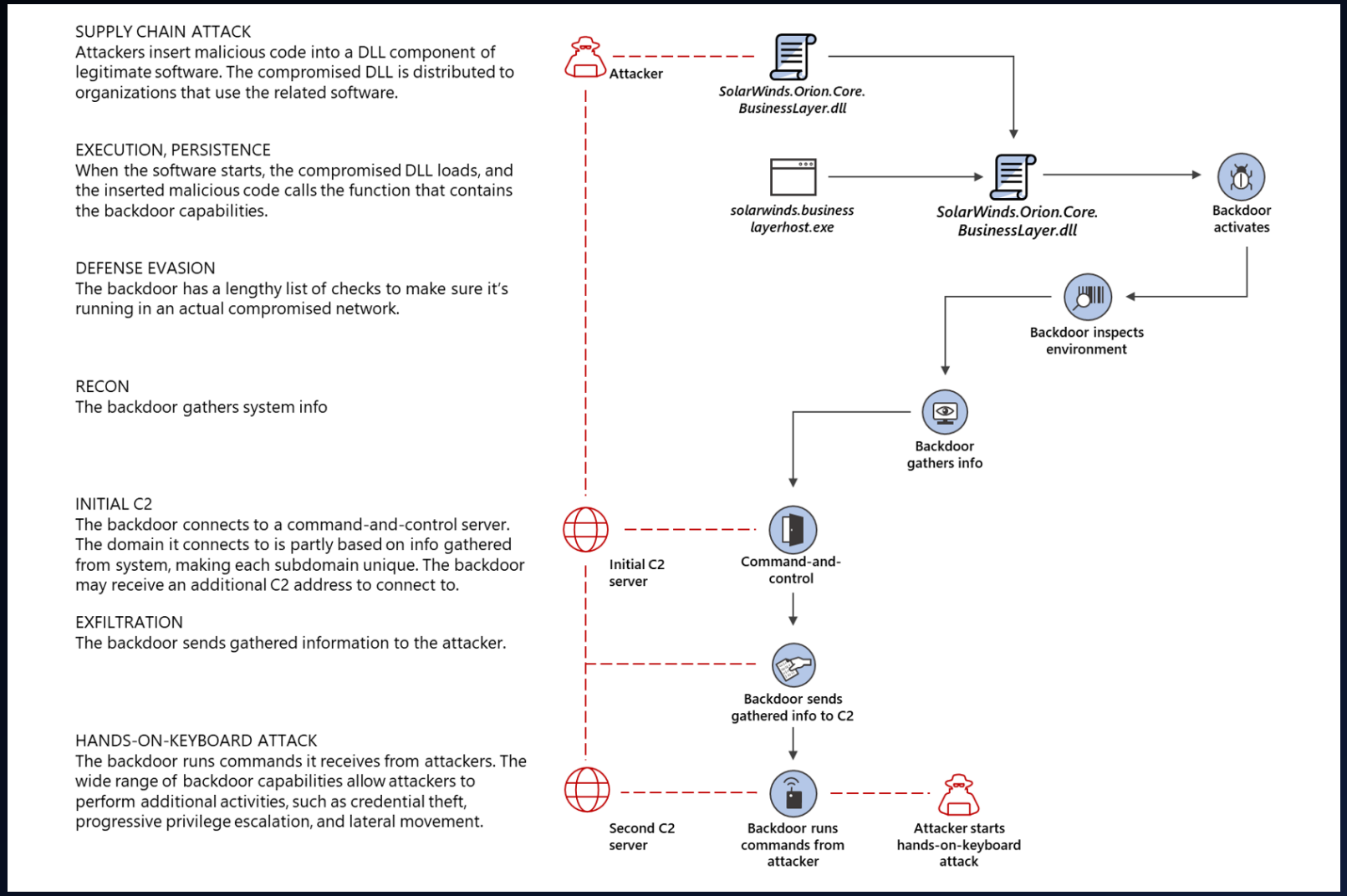
Downloads Url: http://downloads.solarwinds.com
FTP Url: ftp://solarwinds.upload.akamai.com
Username:
Password:
POC: http://downloads.solarwinds.com/test.txt

I was able to upload a test POC.
Via this any hacker could upload malicious exe and update it with release SolarWinds product.



SolarWinds Malware Infection Chain (Microsoft)

- Highly sophisticated code insertion process
  - Mutexes for single instance and managed process termination.
  - Encrypted logs
  - Debugging privileges
  - Clean code swap and removal of malicious source.
  - Removed compile warnings for malicious code segments
- Stealthy behavior once installed on client device
  - Delay 2 weeks
  - Random C2 URLs
  - Mimic Orion Improvement Program communications



Other Supply Chain Attacks (HW, SW, Services, Human Element)

- **Target (Nov – Dec 2013)**
  - Compromised HVAC services provider Fazio Mechanical Services and used their credentials to penetrate Target's network.
  - https://arxiv.org/pdf/1701.04940.pdf
- **Cloud Hopper (2010? – 2017)**
  - Chinese actors penetrated major technology service providers and subsequently compromised targeted clients.
  - Fujitsu, Tata Consultancy Services, NTT Data, Dimension Data, HPE, CSC, and DXC
  - https://www.reuters.com/investigates/special-report/china-cyber-cloudhopper/
- **NotPetya (June 2017)**
  - Compromised the update process of Ukrainian MeDoc software to insert destructive malware.
  - Leveraged NSA exploits EternalBlue and EternalRomance from the ShadowBrokers dump, then laterally moved throughout networks
  - https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world
  - This is a must-read article for corporate executives describing the impact and actions taken by Maersk who suffered a $300M impact.
- **CCleaner (Sep 2017, Sep 2019)**
  - https://blog.avast.com/progress-on-ccleaner-investigation
  - CCleaner, a PC health tool by Avast, was compromised and used as the first stage in an attack chain targeting very select tech and telecom companies. Similar to SolarWinds, not all (few) compromised systems were exploited to the second stage.
- **Tesla (Aug 2020)**
  - https://arstechnica.com/information-technology/2020/08/russian-tourist-offered-employee-1-million-to-cripple-tesla-with-malware/
  - What if this had been an attempt to insert malware into the source code for controlling an automobile?

Discussion

- How did your organization respond?
- How has your risk profile changed? What actions are being taken in response to the increased risk?
- What long-term changes are you considering for improving the integrity of your supply chain?
- How does this affect your companies risk management of suppliers, service providers, vendors, partners, etc.?
- Does your threat intel include your supply chain? Will it in the future?
- What actions are you considering to protect/detect/react against a similar attack (assume you're similarly compromised through your supply chain)?
- How to protect against / detect a malicious code injection into your software development pipeline?
- What are your supply chain security best practices?

Thoughts For Reducing Supply Chain Risks

- Software Development
  - Code scans pre-compile to identify unexpected functionality (use of crypto, inter-process monitoring, disabling compile warnings, etc.)
  - Reverse engineering functionality analysis to determine unexpected functions, indications of tampering, etc.
  - Implement Code Provenance strategy to ensure attestation of the origin of all source code (reference Uber, Google)
  - Maintain a Software Bill of Materials (SBoM) for tracking all components (Consortium for Information & Software Quality)
  - Implement Secure Software Design Lifecycle processes (Security-by-Design)
- Basics
  - Supplier, service provider, vendor, partner inventory
  - Supplier, service provider, vendor, partner risk rating based on many factors including criticality to your operations, position in network, level of access and integration, etc.
  - Collaborate with and subscribe to suppliers, etc.; include, as appropriate, in tabletop exercises
- Include supply chain in threat intel scope
  - Raise the operational awareness for suppliers who have heightened risk indicators (i.e., public compromise, creds for sale on internet, ...)
    - Communicate the indicators to your supplier(s) – If you identified the indicators through internal or other engaged parties, do not assume your supplier is aware!
    - Increase monitoring, vendor specific use cases (rules), …
  - Consider restrictions for suppliers with heightened risk indicators (block updates or patches, ask for supplier internal security assessments, pen tests, …)
- Enterprise
  - Implement zero-trust with any supplier connectivity or integration
  - Supplier risk assessments, 3rd party audits, self-assessments, pen tests, …
  - Obtain 3rd party risk assessments via BitSight, Security Scorecard, RiskRecon, UpGuard, etc. - Not conclusive, but indicative of behavior and posture
  - Implement Supply Chain Risk Management program focused on all aspects of the supply chain (HW, SW, Services, Human Element)

Deliver Uncompromised: A Strategy for Supply Chain Security…

- **Supply Chain: This strategy document is focused on the DoD supply chain; however, the principles provided can easily be applied to any supply chain.**
  - https://www.mitre.org/publications/technical-papers/deliver-uncompromised-a-strategy-for-supply-chain-security
  - https://www.mitre.org/sites/default/files/publications/pr-18-2417-deliver-uncompromised-MITRE-study-26AUG2019.pdf
  - Few if any holistically consider the entire blended operations space from a counter-intelligence perspective and act on it. Risk quantification and mitigation, as a mission, receive insufficient resources and prioritization. Too little attention is directed toward protection of operational security or software assurance.
  - “We must have confidence that industry is delivering capabilities, technologies and weapon systems that are uncompromised by our adversaries, secure from cradle to grave.” - Kari Bingen, DoD Deputy Undersecretary for Intelligence
  - Adversaries have shifted their strategy to asymmetric attacks facilitated through blended attacks.
    - The four primary attack vectors in an asymmetric blended operation are supply chain (software, hardware, services), cyber-physical (cyber systems with real-time operating deadlines including weapons systems and industrial control systems), cyber-IT (informational technology), and human domain (witting or unwitting; foreign intelligence service or insider). Most operations use more than one of these vectors to realize an operational effect, moving between them as a function of time as access and opportunity allow. Viewing only cyber-IT as the primary vector affords the adversary a great degree of obfuscation and opportunity in the other three.

Deliver Uncompromised: A Strategy for Supply Chain Security (cont'd)

- Courses of Action:

1. Elevate Security as a Primary Metric in DoD Acquisition and Sustainment
2. Form a Whole-of-Government National Supply Chain Intelligence Center (NSIC)
3. Execute a Campaign for Education, Awareness, & Ownership of Risk
4. Identify and Empower a Chain of Command for Supply Chain with Accountability for Security and Integrity to DEPSECDEF
5. Centralize SCRM-TAC with the Industrial Security/CI mission owner under DSS and Extend DSS Authority
6. Increase DoD Leadership Recognition and Awareness of Asymmetric Warfare via Blended Operations
7. Establish Independently Implemented Automated Assessment and Continuous Monitoring of DIB Software
8. Advocate for Litigation Reform and Liability Protection
9. Ensure Supplier Security and Use Contract Terms
10.Extend the 2015 National Defense Authorization Act (NDAA) Section 841 Authorities for "Never Contract with the Enemy"
11.Institute Innovative Protection of DoD System Design and Operational Information
12.Institute Industry-Standard Information Technology (IT) Practices in all Software Developments
13.Require Vulnerability Monitoring, Coordinating, and Sharing across the Supply Chain of Command
14.Advocate for Tax Incentives and Private Insurance Initiatives
15.For Resilience, Employ Failsafe Mechanisms to Backstop Mission Assurance

References: SolarWinds/Sunburst

- https://www.fireeye.com/blog/threat-research/2020/12/unauthorized-access-of-fireeye-red-team-tools.html
- https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html
- https://github.com/fireeye/red_team_tool_countermeasures
- https://www.solarwinds.com/securityadvisory
- https://www.cisa.gov/supply-chain-compromise
- https://www.microsoft.com/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/
- https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/
- https://krebsonsecurity.com/2020/12/solarwinds-hack-could-affect-18k-customers/
- https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/
- https://orangematter.solarwinds.com/2021/01/11/new-findings-from-our-investigation-of-sunburst/
- https://unit42.paloaltonetworks.com/solarstorm-supply-chain-attack-timeline/
- http://solarleaks.net/
- https://securelist.com/sunburst-backdoor-kazuar/99981/
- https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html?smid=li-share

References: Supply Chain Security

- https://www.mitre.org/publications/technical-papers/deliver-uncompromised-a-strategy-for-supply-chain-security
- https://www.mitre.org/sites/default/files/publications/pr-18-2417-deliver-uncompromised-MITRE-study-26AUG2019.pdf
- https://csrc.nist.gov/projects/cyber-supply-chain-risk-management
- https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf
- https://medium.com/uber-security-privacy/code-provenance-application-security-77ebfa4b6bc5
- https://www.youtube.com/watch?v=vb08Jkp1f-M&list=PLFTyE08qmQMUOJju0ebY3ep__XT9U3R0G&index=6&t=0s
- https://cloud.google.com/security/binary-authorization-for-borg
- https://www.it-cisq.org/software-bill-of-materials/