
Tales from the Supply Chain Security Sausage Factory
RSA Conference: Birds of a Feather Session (SBX4-XBF7) – 2021.05.20
AMPERE

INTRODUCTION

- CEO, Ampere Industrial Security
- Centro de Ciberseguridad Industrial (CCI) US Coordinator
- EnergySec Founder, Director and President Emeritus
- Former Principal Investigator US DOE National Electric Sector Cybersecurity Organization
- Former utility staff (telecommunications, water & electric)
- Drafter of NERC CIP standards and formal interpretations
- First NERC CIP auditor in the US
- NERC CIP Supply Chain Working Group contributor
- Cybersecurity Advisory Team for State Solar, NARUC/NASEO
- Advisor to multiple industrial security product vendors
- GCIP, CISA, CRISC, CISSP-ISSAP, SSCP, NSA-IAM, CVI, TCP, SCP

SUPPLY CHAIN SECURITY HISTORY

- Market history has driven us to a global supplier construct
- Nationalism, Balkanization, politics, and fence posts happen
- Hardware and software are getting much more complex
  - Increased potential attack surface
  - Increased availability/opportunity
- What if bad things are embedded in critical systems?
  - Infrastructure is a high-value/impact target
- Goal is often theft, control, sabotage or destruction
- Potential concerns beyond security
  - Quality
  - Safety
  - Economics

WHO IS USING SUPPLY CHAIN ATTACKS?

- Nation States
- Non-Governmental Organizations (NGOs)
- Organized crime
- Competitors

- Someone who probably has more people, money, and time than you do - it takes significant resources

- If it were easy or cheap, everyone would do it all the time

WHY USE A SUPPLY CHAIN ATTACK?

- Difficult to execute well
- High error potential
- High level of effort to create
- Why not use something easier like…
  - Bad passwords
  - Unpatched systems
  - Malware/ransomware
  - Phishing
  - Social engineering
  - 0-days
  - Etc…

BECAUSE IT WORKS

- If it wasn't effective, it wouldn't be a viable option
- Can be surgically targeted or widely catastrophic
- Often very difficult to detect
- Often overlooked or deemed unlikely
- Extensive attack surface to protect
- Difficult to get 100% coverage
- Can be more challenging to get attribution

WHAT CAN YOU DO ABOUT IT?

- Focus on buying only “trusted” products and services, right?
  - From whom?
  - From where?
- But what does this really mean?
  - How do you get trust?
  - Is trust transitive?
- How long does trust last?
- How much assurance is enough?

SOME POSSIBLE SOLUTIONS

- Make it yourself, but from what? From where?
- Software Bill of Materials (SBOM)
- Independent certification body
- Transparency centers
- Self-vetting
- “Herd immunity” or public, crowdsourced, or external vetting
- Development standards
- Regulation, Executive Orders, and “sabre rattling”
- Cyber Insurance

HOW DEEP DO YOU GO?

- Country of origin
  - Will your allies still be allies over the life span of the product?
- Hardware components and subcomponents
- Software components and subcomponents
- Firmware and BIOS
- Compilers, libraries, drivers, microcode
- Developers
- Technicians
- Couriers

BUYER IMPACTS

- Procurement and purchasing
  - May only be able to purchase from specific vendors or countries of origin
- Security team(s)
  - Review and assessment of vendor security practices
  - Incident response
- Project management
  - Extended project duration and cost
- Installation and maintenance
  - Specific installation, service and maintenance practices such as vetted personnel, source validation, etc
- Regulatory overhead (audit and compliance)
- Risk and insurance
- Higher costs for full life cycle of product or service

VENDOR PRODUCT IMPACTS

- Competing international standards
- Unique customer assessment requests
  - Frequency and granularity matters
- Specific contract language (T&Cs) for everyone
- Specific production locations
- Specific production components
- Specific production staff (vetted, monitored)
- Market-constrained sources for everything
- Audit and compliance, but to everything
- Higher cost to make = higher cost to buy

VENDOR SERVICE IMPACTS

- Personnel vetting
- Personnel training and certification
- Retention
- Access management
- Audit and compliance
- Higher cost to make = higher cost to buy

AT THE END OF THE DAY

Costs increase for everyone

- *This makes everyone behave accordingly*

STORIES FROM THE FIELD

- Internal relationships are strained
- Buyer-vendor relationships are strained
- Governmental and political relationships are strained
- Teflon, finger-pointing and selective memory
- Supply chain stigma (predictive purchase policing)
  - Undeserving losers and carpetbaggers happen
- Security professionals are mixed on the value
- How far down the rabbit hole are you willing to go?
  - You may be required to justify why you stopped where you did…

WHAT REALLY WORKS?

- You must do something – for many reasons
- You still need to do the basics – all of them
- Don't eat the elephant – start small and continuously improve
- You can't transfer all the risk to a vendor (it's too expensive)
- Expect to do much of the heavy lifting yourself (it's cheaper)
- Treat it like anything else in your security program
  - Don't create dependencies you can't do manually
  - Validate the sources as best you can
  - Monitor internally and externally for issues
  - Practice incident response like its game day
- Lather, rinse, repeat

SUPPLY CHAIN SECURITY FRAMEWORKS

- DNI NCSC SCRM
- NIST CSF; SP800-161; CREATe
- IEC-62443
- BSI: BS ISO 28000:2007
- WCO SAFE
- SANS
- *So many more…*

CONTACT ME


@PATRICKCMILLER


LINKEDIN.COM/IN/MILLERPATRICKC


PMILLER@AMPERESEC.COM


WWW.AMPERESEC.COM


+15032721414