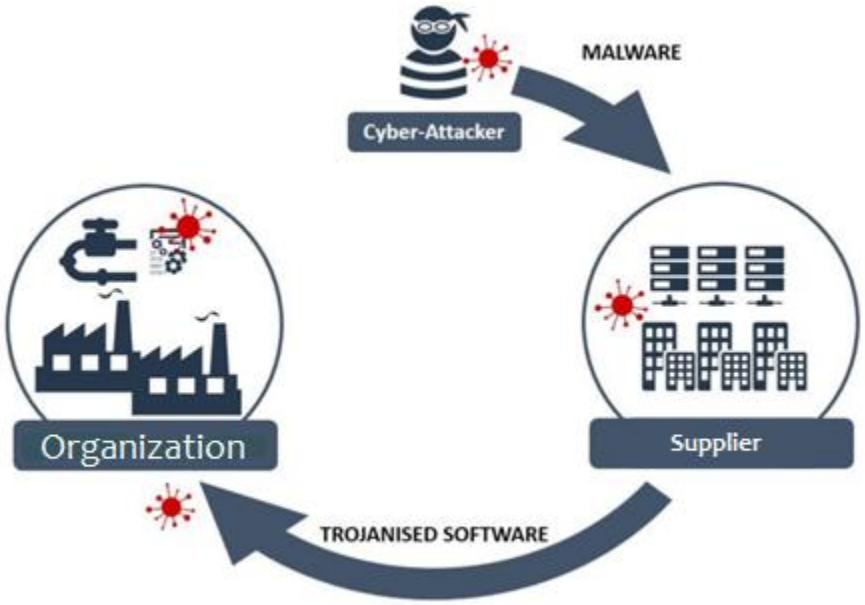


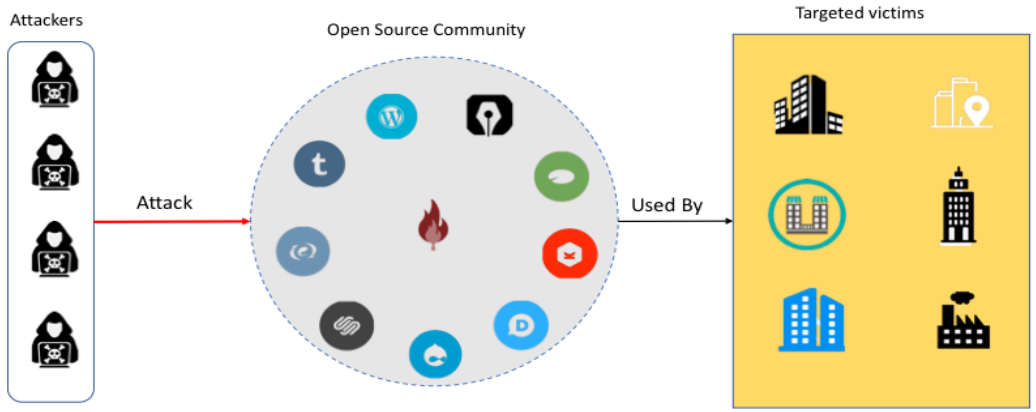
CYBER SUPPLY CHAIN RISK MANAGEMENT

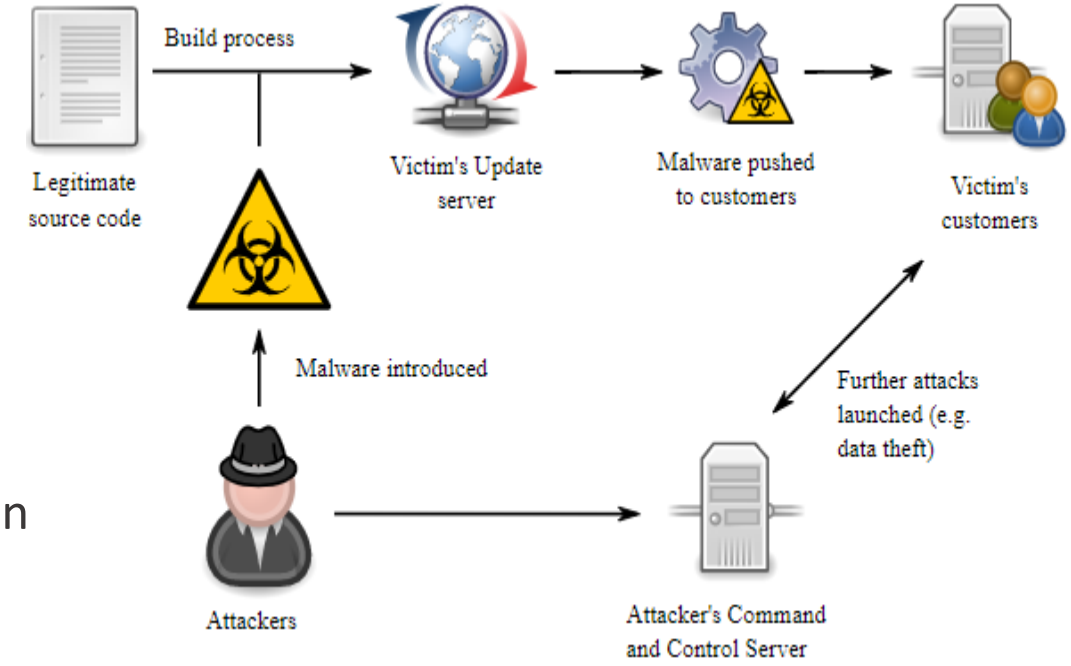
PRESENTED TO RRM TASK FORUM

- Design
- Development and Production
- Distribution
- Acquisition and Deployment
- Maintenance
- Disposal

SUPPLY CHAIN LIFECYCLE

- Supply chain is the network of retailers, distributors, and suppliers that participate in the sale, delivery, and production of hardware, software, and managed services.
- Supply Chain Lifecycle has six phases.
- At each phase of Supply Chain Lifecycle, software is at risk of malicious.

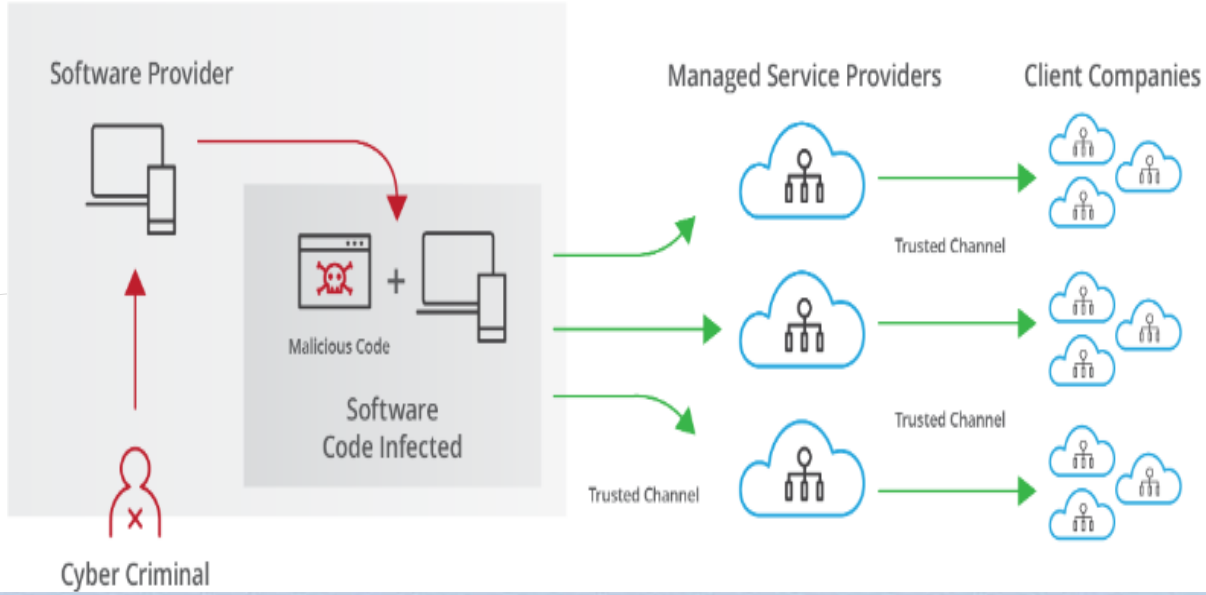




ATTACK VECTORS

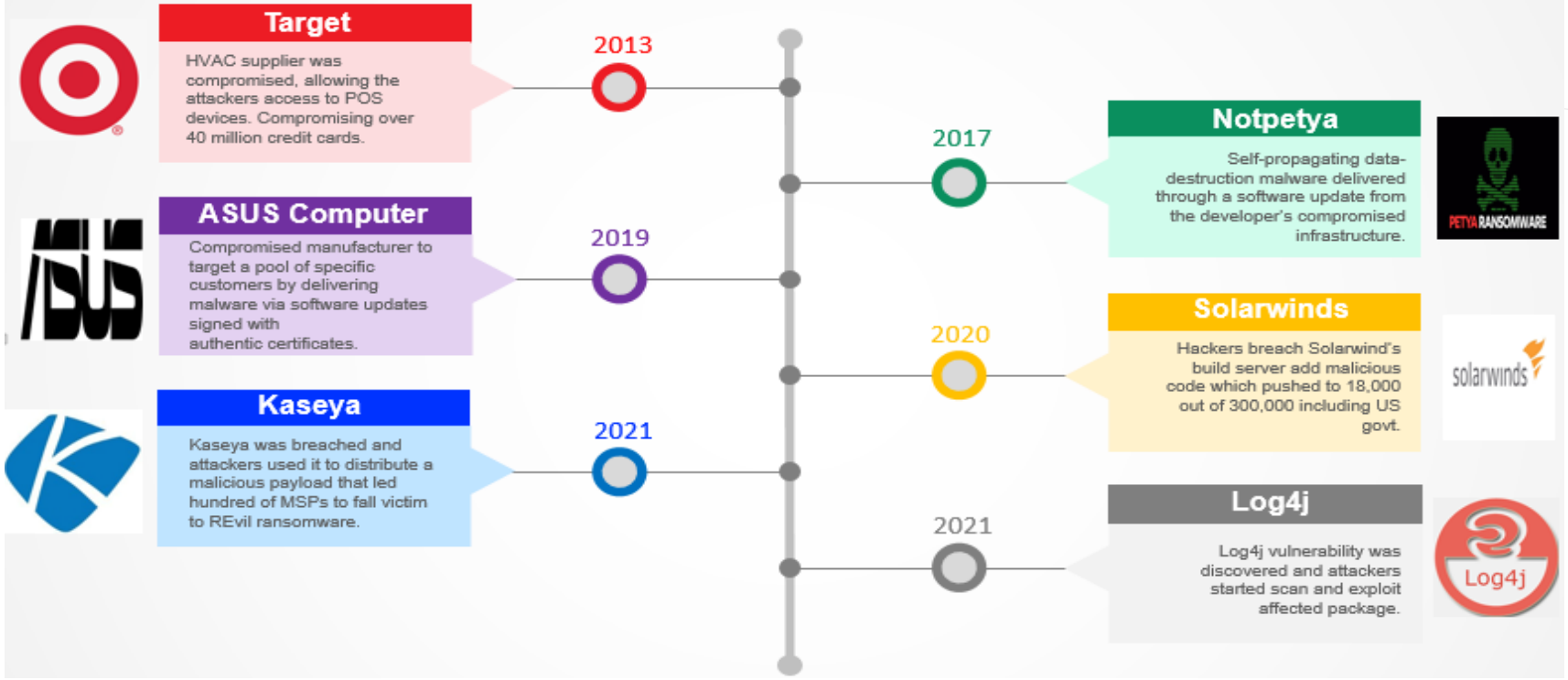
Attack vectors for software supply chains are the various ways in which attacker can compromise software.

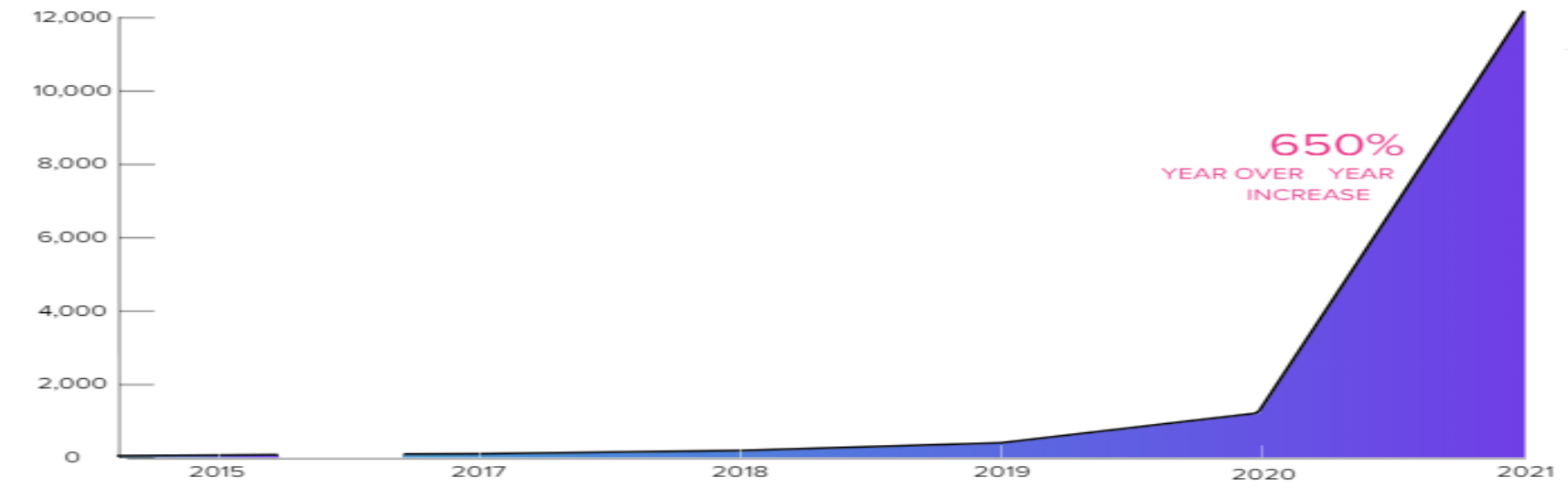
- Open source software package
  Source: Venafi (Machine Identity Management)
- Target organization build servers.
  Source: ZeroFox Solution
- MSPs or cloud services
  Source: Pratum (InfoSec Services firm)



PAST SUPPLY CHAIN ATTACK & TREND

- Here's a quick breakdown of the most impactful supply chain attacks over the last decade or so.
- Supply chain attacks are on the rise. Research shows that 2021 saw a 650% increase according to Sonatype and most organizations had experienced a breach caused by one of their vendors.





CDC PRACTICES

- **SECURITY OPERATION CENTER (SOC)**


PAM


EDR


VA

SIEM

- **THREAT MODELING**
  - Functional Security
  - Geopolitical Risk Assessment

- **PEN TESTING OF SYSTEMS AND APPLICATIONS**

- **DYNAMIC APPLICATION SECURITY TESTING**
  - Vulnerabilities discovery
  - Software Composition Analysis
- **AGREEMENT / NDA**
  - Secure Engineering Principle (Authentication, Authorization and Session Handling)
  - Formal Certification Such as ISO, SOC Type 2 etc.

THANK YOU

info@cdcpak.com

https://www.cdcpakistan.com/