Plotting OSS-based Supply Chain attack strategies and the defense failure

Arpita Dinesh Sarang[1][0000−0003−4461−711X], Sang-Hoon Choi[2][0000−0002−9549−0887], and Ki-Woong Park[3][0000−0002−3377−223X] ⋆

[1] SysCore Lab, Department of Information Security, and Convergence Engineering for Intelligent Drone, Sejong University, Seoul 05006, South Korea
arpita.sarang@sju.ac.kr
[2] SysCore Lab, Sejong University, Seoul 05006, South Korea
csh0052@gmail.com
[3] Department of Information Security, and Convergence Engineering for Intelligent Drone, Sejong University, Seoul 05006, South Korea
woongbak@sejong.ac.kr

Abstract. The supply chain attack, which targets open-source software, is currently the most discussed cyberattack. This is due to the recent open-source XZ utils and PyPI projects based attacks where the attackers employed similar strategies. A backdoor was injected in the libraries developed by these projects for future exploitation when software users installed them on systems. These attacks were executed by the trusted developers of these projects and influenced by unknown promoters. Therefore, there is a need to scrutinize Open Source Software(OSS) Security to protect the legacy of Open Software development for the future. This paper provides an overview of these two attack strategies through their case studies, which aid in the creation of a generic attack framework for supply chain attacks on OSS. We present the existing detection methods for OSS security in this work and their lacunas taking into account at various stages of a supply chain attack. This makes it necessary to build platforms that allow the current OSS security detection modules to be utilized in sequence. Therefore, we introduce an OSS security Detection platform that does not completely address the limitations of the detection technique, but when combined, they can maximize the effectiveness of an OSS security quality check.

Keywords: Supply Chain Attack · Linux distribution · Cyber Security · Supply Chain Attack as a Service(SCAaaS) · Open Source Software(OSS) Security · Software Bill of Materials(SBOM)

1 Introduction

A software-based supply chain attack is a cyber-attack that distributes software or its library with a backdoor that can exploit the critical data on systems they

⋆ Corresponding author.