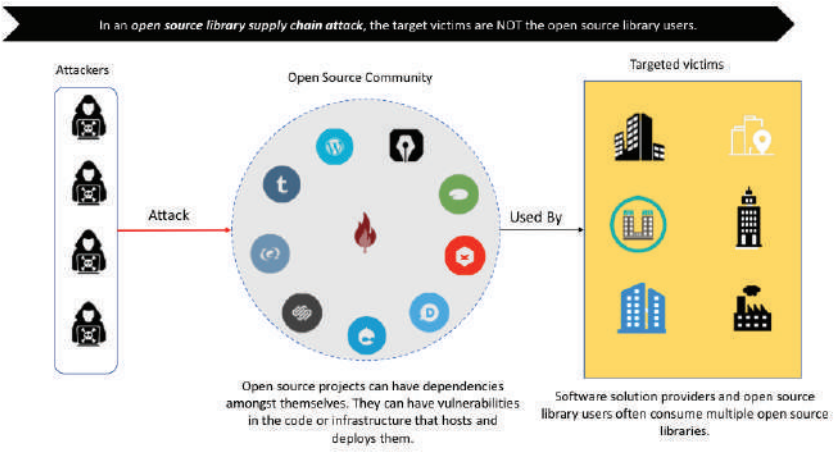
Open-Source Software Library
Trusted Supply Chain Attack...



Open Source Software Libraries (OSSLs) are widely used by organizations and developers nowadays. According to a recent study, on average, modern software is made up to 79% of reusable libraries from open source projects. This code is then deployed into live production environments where it is consumed by the organization's customers.

Account to a 2018 OSSRA report, 96% of closed environment applications scanned contained open source components, with many containing more open source than proprietary code. In fact, most of today's software systems and products are built on software that is supplied by various third-party open source providers.

Unfortunately, OSSLs most often run with the same privileges granted to an organization's custom code, without any constraints or extra checks. Organizations and developers are used to trusting them implicitly, with most developers assuming that the legitimacy of OSSLs from established sources are beyond suspicion. As such, they overlook the need to implement appropriate and preemptive security controls and mechanisms.

The problem with OSSL is that it is created all over the world, mostly authored by both known entities and anonymous individuals. There is no single owner, no proper identification or trust verification, instead the responsibility is shared within the community for ensuring the quality of the code. This community is more focused on the performance of the code, not if that code has been manipulated or not.

Think about it, if an attacker is able to modify the code stored in an open source library, they can inject malicious code within it. This code is then used by the trusting OSSL community, who use this code in production.

How to prevent OSSL Trust Attacks?

Unfortunately, this new attack pattern is too new to have a large-scale solution. And with the vast variety of software in the open source environment, a defense solution that addresses a specific language, framework and technology is not readily available. Therefore, it is imperative to test software and code before deploying it in production and after installing any and all major updates.

- **Source: Venafi, NCSC UK and Cybereason**

BEETLES
THE HACKER'S APPROACH
+8802-9513744
query@beetles.io
www.beetles.io
Aziz Bhaban
93 Motijheel C/A (3rd Fl.)
Dhaka-1000, Bangladesh