ZDMP Blog

Secured Installation

Securely Installing Third-party Apps for Industry 4.0

By Leticia Montalvillo. IKERLAN Research Center

Some questions for you

- Do you need to install, use, or deploy applications developed by third party developers or companies?
- Do these third-party applications need to access any type of proprietary, sensitive or process data in any way?
- Are you aware or concerned if these third-party applications implement latest security patterns?
- Are you aware or concerned if these third-party applications can introduce security holes in your enterprise?

Motivation

Cyberattacks are on the rise and specially manufacturing businesses are the favourite targets for cybercriminals. To combat the threat of a cyberattack, companies are investing huge capital in securing their own on-premises infrastructure and data. However, there are other ways in which a company can be attacked. One of which is by taking advantage of the security vulnerabilities and holes that installing third-party applications can create.

Indeed, third-party apps can bring better functionality for organizations and allow them to monetize the business and generate more revenues. However, these apps can also present significant security risks and privacy threats to the sensitive data. Third party apps are usually made available in third party marketplaces, which have their own security vetting and approvals processes; some of which may not be up to standard. Therefore, the apps coming from third party app stores may carry certain risks. Hence, as a business, it is important to control where app downloads are coming from and controlling what is exactly being installed, and how. These apps are usually insecure for different reasons:

- Usually are not developed with reference enterprise security standards. According to Veracode research [1] 90% of third-party code does not comply with enterprise security standards such as the OWASP Top 10 [2]
- Commonly leave large vulnerabilities that can be exploited by cybercriminals [3]. These vulnerabilities lie hidden within the code and it is a race between the criminals and the cybersecurity researchers to see who can find them first. The US government sponsors the Common Vulnerability Enumeration (CVE) list [4] and the National Vulnerability Database [5], which in 2019 more than 8,000 new vulnerabilities were added
- Can be malicious by nature (malware), developed to harm companies in any form, and make profit out of it (encrypt the data, steal credentials, etc)

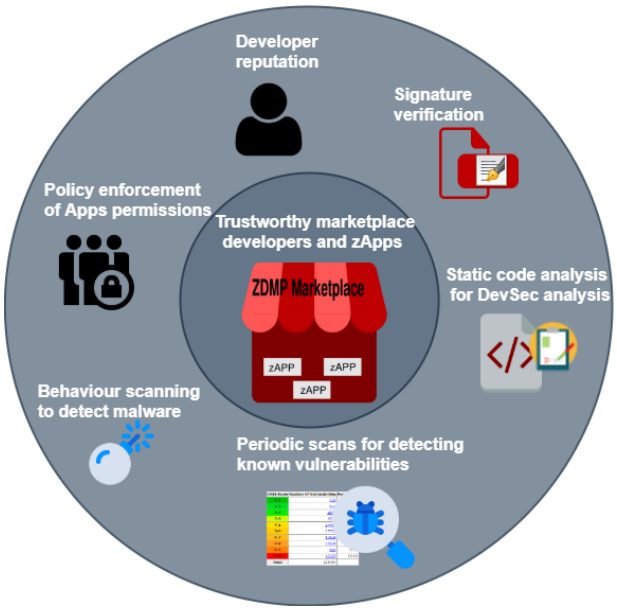
A process for securely installing apps in enterprises need to address these issues.

Measures for secure installation of third-party Apps

It is critical to assess the risks a third-party apps might cause if installing them into your business infrastructure. Otherwise, the installation of unsecure or malware applications can lead to creating backdoors which cybercriminals can use and have access to your business, clients, and financial data. The question is: How can you make sure an app is secure and does not bring any security risks when running it into your business? Before even buying or downloading any App, pay attention to the site you are downloading the applications from. Is this a secure site? Is it trustworthy, or known to have poor security standards for uploading apps? Commonly, trustworthy marketplaces have strong security guidelines for app developers (e.g. Atlassian guidelines [6]). Hence, make sure the marketplace complies with the highest security standards. However, in some marketplaces these standards are just recommend guidelines and best

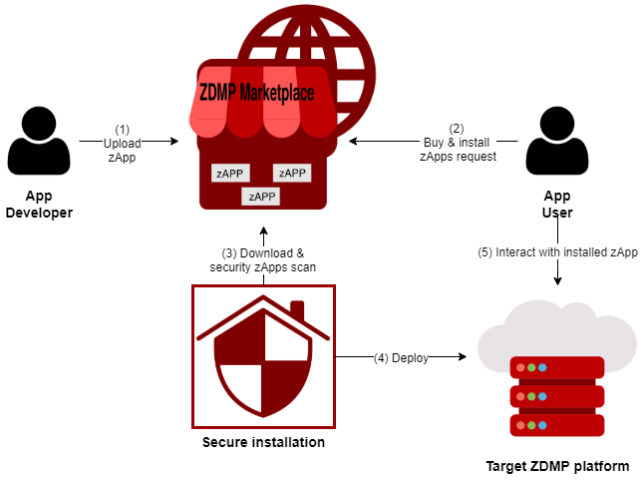
practices, and hence, these are not always enforced. So, how can it be ensured that they have no vulnerabilities? How can it be known if this application would interact with sensitive data and disclose it? A secure installation process is needed to download an app hosted in a Marketplace and deploy it into the target infrastructure, while ensuring the security of the business data and services. The installation process should entail:

- Signature verification of the application to verify its integrity and the absence of any kind of tampering
- Static code analysis that checks the security level of the app, ensuring they are secure against known vulnerabilities and follow secure code development standards (such as OWASP Top 10 [2])
- Behaviour checking when the application is running. By running the application in a secure sandbox, its behaviour can be monitored to detected zero days malware, and identifying unwanted behaviours, eg accesses to resources not allowed
- Configure and enforce app security policies for the application. This deals with granting only the access to needed data and services, by enforcing the principle of least privileged (PoIP)



What will ZDMP achieve

The ZDMP secure installation service, as one of the component services for the ZDMP platform, can help on installing applications on Industry 4.0 platform. This service acts on behalf on when they request an installation of a a zero-defect manufacturing App) the ZDMP Marketplace (the trustworthy Marketplace developed for hosting allows automatic inspections to disclose risks, as well as it configures security enforcements following the PoIP



provided available securely the user zApp (ie through zApps). It security policy principle.

ZDMP Links

• Architecture Component(s)	Secure Installation
• Work Package	WP6 – ZDMP Core Services and Middleware
• Tasks	T5.2 – Robust Industrial Network Support

References

[1] https://info.veracode.com/state-of-software-security-report-volume5.html
[2] OWASP TOP 10 https://owasp.org/www-project-top-ten/
[3] https://www.veracode.com/security/web-application-vulnerabilities
[4] CVE Mitre. https://cve.mitre.org/
[5] NIST. https://nvd.nist.gov/
[6] https://developer.atlassian.com/platform/marketplace/app-security-guidelines/

[7] https://www.csoonline.com/article/3488804/2019-in-review-data-breaches-gdprs-teeth-malicious-apps-malvertising-and-more.html