Ransomware Attacks in the Software Supply Chain: A Review of Attack Vectors, Defenses and Gaps

Corey Brookins
Kennesaw State University

Ava Norouzinia
Kennesaw State University

Asia Shavers
Kennesaw State University

Miranda Dominguez
Kennesaw State University

Marie Nassif
Kennesaw State University

See next page for additional authors

Presenters

Corey Brookins, Ava Norouzinia, Asia Shavers, Miranda Dominguez, Marie Nassif, Kenneth Burke, and Shamar Lake

Abstract for Spring Symposium 2023

Title: Ransomware Attacks in the Software Supply Chain: A Review of Attack Vectors, Defenses and Gaps

FYS Names: Corey Brookins, Ava Norouzinia, Asia Shavers, Miranda Dominguez, Marie Nassif, Kenneth Burke, Shamar Lake

Mentor: Nazmus Sakib, Hossain Shahriar

Corey Brookins[1], Ava Norouzinia[2], Asia Shavers[3], Miranda Dominguez[2], Marie Nassif[4], Kenneth Burke[2], Shamar Lake[4], Nazmus Sakib[5], Hossain Shahriar[5]

[1]Department of Mechanical Engineering, Kennesaw State University, USA
[2]Department of Computer Science, Kennesaw State University, USA
[3]Department of Information Security, Kennesaw State University, USA
[4]Department of Computer Engineering, Kennesaw State University, USA
[5]Department of Information Technology, Kennesaw State University, USA

Abstract

The proliferation of cyberattacks in the software supply chain domain is a pressing concern making them a formidable threat to software security and compromising its integrity and credibility which needs to be critically acknowledged and investigated. The lack of familiarity with the design and pattern of emerging attacks has contributed to the occurrence of several vulnerable software supply chain attacks in the preceding years. This project aims to conduct a comprehensive study of the various tactics and techniques employed by cybercriminals in this domain along with a focus on exploring the influence of software supply chain stakeholders' traits, limitations, and actions on the likelihood of a successful attack. Furthermore, this research also identifies the regulatory tools and protocols administrating software supply chain that assist in reducing an organization's susceptibility to these challenges. Using a rigorous methodology, we investigate the frequency, how and where ransomware attacks occur. We review current defence techniques and gaps. The findings will provide valuable insights concerning the recent trends in disrupting the security and efficiency of software supply chain and offer recommendations to researchers, organizations, and practitioners to remain cautious and proactive in their cybersecurity posture.

Keywords:

Software Supply chain attacks, ransomware attacks, defence techniques, regulatory frameworks