

Kennesaw State University

DigitalCommons@Kennesaw State University

Symposium of Student Scholars

Software Supply Chain Security Attacks and Analysis of Defense

Juanjose Rodriguez-Cardenas
Kennesaw State University

Jobair Hossain Faruk
Kennesaw State University

Masura Tansim
Kennesaw State University

Asia Shavers
Kennesaw State University

Corey Brookins
Kennesaw State University

See next page for additional authors

Follow this and additional works at: <https://digitalcommons.kennesaw.edu/undergradsymposiumksu>



Part of the [Databases and Information Systems Commons](#), [Information Security Commons](#), and the [Software Engineering Commons](#)

Rodriguez-Cardenas, Juanjose; Faruk, Jobair Hossain; Tansim, Masura; Shavers, Asia; Brookins, Corey; Lake, Shamar; Norouzi, Ava; Nassif, Marie; Burke, Kenneth; and Dominguez, Miranda, "Software Supply Chain Security Attacks and Analysis of Defense" (2022). *Symposium of Student Scholars*. 253. <https://digitalcommons.kennesaw.edu/undergradsymposiumksu/Fall2022/presentations/253>

This Poster is brought to you for free and open access by the Office of Undergraduate Research at DigitalCommons@Kennesaw State University. It has been accepted for inclusion in Symposium of Student Scholars by an authorized administrator of DigitalCommons@Kennesaw State University. For more information, please contact digitalcommons@kennesaw.edu.

Presenters

Juanjose Rodriguez-Cardenas, Jobair Hossain Faruk, Masura Tansim, Asia Shavers, Corey Brookins, Shamar Lake, Ava Norouzi, Marie Nassif, Kenneth Burke, and Miranda Dominguez

Abstract Fall Symposium 2022

Title: Software Supply Chain Security Attacks and Analysis of Defense

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

Mentor: Dr. Hossain Shahriar

Keywords: Software Supply Chain Attacks, Cybersecurity, Software Security, Software Reusability

Abstract:

The Software Supply chain or SSC is the backbone of the logistics industry and is crucial to a business's success and operation. The surge of attacks and risks for the SSC has grown in coming years with each attack's impact becoming more significant. These attacks have led to the leaking of both client and company sensitive information, corruption of the data, and having it subject to malware and ransomware installation, despite new practices implemented and investments into SSC security and its branches that have not stopped attackers from developing new vulnerabilities and exploits. In our research, we have investigated Software Supply Chain security tools and their infrastructure along with ways to help mitigate and reduce the risk of an attack. As well as following the route an Attacker takes, and the steps taken to cause such an attack. Ransomware is one of the more popular attacks in recent years in which the attacker gains access to the system and blocks its usage from anyone else until a ransom is paid. This ransom is often delivered in cryptocurrency to ensure anonymity from the attacker. Our goal is to extend the research to where Software Supply Chain attacks can be reduced for companies and develop solutions for vulnerable systems.