

Kennesaw State University

DigitalCommons@Kennesaw State University

---

Symposium of Student Scholars

---

## 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*

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



Part of the [Other Engineering Commons](#)

---

Brookins, Corey; Norouzinia, Ava; Shavers, Asia; Dominguez, Miranda; Nassif, Marie; Burke, Kenneth; and Lake, Shamar, "Ransomware Attacks in the Software Supply Chain: A Review of Attack Vectors, Defenses and Gaps" (2023). *Symposium of Student Scholars*. 151.

<https://digitalcommons.kennesaw.edu/undergradsymposiumksu/spring2023/presentations/151>

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](mailto:digitalcommons@kennesaw.edu).

---

## 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<sup>1</sup>, Ava Norouzinia<sup>2</sup>, Asia Shavers<sup>3</sup>, Miranda Dominguez<sup>2</sup>, Marie Nassif<sup>4</sup>, Kenneth Burke<sup>2</sup>, Shamar Lake<sup>4</sup>, Nazmus Sakib<sup>5</sup>, Hossain Shahriar<sup>5</sup>

<sup>1</sup>Department of Mechanical Engineering, Kennesaw State University, USA

<sup>2</sup>Department of Computer Science, Kennesaw State University, USA

<sup>3</sup>Department of Information Security, Kennesaw State University, USA

<sup>4</sup>Department of Computer Engineering, Kennesaw State University, USA

<sup>5</sup>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