**Jared Tjiong**

**11/21/21**

**Week 11: Related Research Write-up – Related Work - (2/3 of a column) 11/21**

**Paragraph Description of the Problem Domain**

The problem domain for my final paper is the prevention of supply-chain attacks on cyber supply-chain (CSC) networks that occur when hackers exploit security weaknesses in a vendor to gain access to multiple clients that utilize the vendor’s product. The most recent example of this attack occurred at SolarWinds Inc. SolarWinds is an American company that provides third-party software and information technology services to businesses and government agencies.  The company’s Orion IT performance monitoring platform was specifically targeted by foreign entities using ransomware attacks disguised as software updates.  The malware allowed the attackers to gain remote access to the affected systems which led to files being stolen or modified from multiple clients. This creates a problem of confidentiality and integrity.

**Hypothesis**

Predicting when a supply-chain attack is about to occur or has occurred is a major problem when safeguarding cyber supply-chain (CSC) networks. Using the SolarWinds hack for my analysis, I hypothesize that incorporating multiple security mechanisms into a cyber threat intelligence (CTI) life cycle process will enable the identification of the most effective methods to prevent or mitigate future supply-chain attacks.

For my analysis, I will analyze the vulnerabilities of the Orion IT performance monitoring platform and damage suffered by SolarWinds from the supply-chain attack.  The solution I provide is different from current solutions as a result of my incorporating multiple security mechanisms into a CTI life cycle process to determine the most effective method to prevent or mitigate future threats.  A CTI lifecycle process contains the following phases - direction, identification, process, analysis, report, disseminate, and review.  In addition, the attack lifecycle contains two phases - the direct phase and the identification phase. The direct phase seeks to identify tactics, techniques, procedures (TTPs), attack patterns, and threat indicators.  The identification phase will determine the weaknesses, level of risk, and the method of attacks that could damage key assets within the CSC network. [2]

**Related Research**

* Goal – compare your results to prior results
* At least 3 academic (peer reviewed) references – Paragraph for each, 3 sentences each
  + Not reports, conference/journal proceedings
* How does your method different from each?
  + You may be building on what they have done
  + You may bring their solution to a new domain (i.e. db to web)
  + There may be a use case they cannot handle
* Sentence 1 - [Last Name 1 and Last Name 2 or Last Name 1 et. al.] do X.
* Sentence 2 - Explain why this does not work (or work well) for your problem
* Sentence 3 - Explain what you do differently

1. **Complex strategy against supply chain attacks**

Coufalíková, Klaban, and Šlajs wrote a research paper that “defines the most discussed supply chain attacks, briefly summarizes significant events of successful supply chain attacks and outlines complex strategy leading to the prevention of such attacks;” (Coufalíková, Klaban, and Šlajs, 2021).  This academic reference works well with my problem because it provides background information required when discussing previous supply chain attacks.  It also gives explanations for current security mechanisms used to mitigate these threats.  My research paper will be different from this academic reference as I will be analyzing the SolarWinds hack - the most recent example of a successful supply chain attack.  I will also input security mechanisms listed in this academic reference into a CTI lifecycle process as well as the threats mentioned in the attack lifecycle.

1. **Cyber Threat Intelligence for Improving Cyber Supply Chain Security**

Yeboah-Ofori, Islam, and Yeboah-Boateng’s research “…paper contributes to improving the cybersecurity of CSC by using the CTI approach to understand the attack trends to determine the appropriate controls.  They also use a smart grid case study in the CSC context to demonstrate their approach.  The result of this study demonstrates how the CTI approach is applied to assist in the prevention of cyberattacks and how it disseminates threat information sharing.” (Yeboah-Ofori, Islam and Yeboah-Boateng, 2021).  This academic reference works well with my problem domain as I will be incorporating multiple security mechanisms into a CTI life cycle process that will identify the most effective methods to prevent or mitigate future supply-chain attacks.  My research paper will be different from this academic reference as I will be discussing the SolarWinds hack in place of the smart grid case study that the authors used to demonstrate their approach.

1. **Cyberattack Ontology: A Knowledge Representation for Cyber Supply Chain Security**

Yeboah-Ofori, Ismail, Swidurski, and Opoku-Boateng explore “...cyberattack ontology learning to describe security concepts, properties and the relationships required to model security goals. Cyberattack ontology provides a semantic mapping between different organizational and vendor security goals that has been inherently challenging. They also discuss concepts for threat intelligence and knowledge reuse.” (Yeboah-Ofori, Ismail, Swidurski and Opoku-Boateng, 2021). This academic reference works well with my problem domain because the modeling of CSC cyberattack ontology security goals through semantic mapping organizes security goals, threats, threat actors, vulnerabilities, and TTP present CSC attacks. These cyberattack ontology concepts will aid in my CTI gathering process and strengthen my analysis. My research paper will be different from this academic reference as I will not be modeling a cyberattack ontology for semantic mapping and knowledge representation. However, I will apply this information to the SolarWinds hack when implementing the CTI lifecycle process.

**Academic References and Other Sources**

<https://ieeexplore-ieee-org.proxy.library.nyu.edu/document/9502768>

[1] A. Coufalíková, I. Klaban and T. Šlajs, "Complex strategy against supply chain attacks," *2021 International Conference on Military Technologies (ICMT)*, 2021, pp. 1-5, doi: 10.1109/ICMT52455.2021.9502768.

<https://ieeexplore-ieee-org.proxy.library.nyu.edu/document/9058357>

[2] A. Yeboah-Ofori, S. Islam and E. Yeboah-Boateng, "Cyber Threat Intelligence for Improving Cyber Supply Chain Security," *2019 International Conference on Cyber Security and Internet of Things (ICSIoT)*, 2019, pp. 28-33, doi: 10.1109/ICSIoT47925.2019.00012.

<https://ieeexplore-ieee-org.proxy.library.nyu.edu/document/9565164>

[3] A. Yeboah-Ofori, U. M. Ismail, T. Swidurski and F. Opoku-Boateng, "Cyberattack Ontology: A Knowledge Representation for Cyber Supply Chain Security," *2021 International Conference on Computing, Computational Modelling and Applications (ICCMA)*, 2021, pp. 65-70, doi: 10.1109/ICCMA53594.2021.00019.

[4] Graves, R., 2015. Honeypots and Honey Tokens for Webmail ID/IR. [ebook] Available at: <<https://sansorg.egnyte.com/dl/9GSb3GAawz>> [Accessed 4 November 2021].

[5] Okta 2021. The State of Zero Trust Security 2021 Identity and Access Management Maturity in Global Organizations. [ebook] San Francisco. Available at: <<https://www.okta.com/sites/default/files/2021-07/WPR-2021-ZeroTrust-070821.pdf>> [Accessed 4 November 2021].

<https://www.upguard.com/blog/prevent-supply-chain-attacks-with-honeytokens>

<https://ieeexplore-ieee-org.proxy.library.nyu.edu/document/9448097>