Cyber-Attack Scoring Model Based on the Offensive Cybersecurity Framework

Cameron Noakes

December 2021

1 Sentence Overview

The researchers evaluated advanced persistent threats (APTs) and file-less cyber-attacks that occurred between 2010 and 2020 based on the methodology they developed.

2 Introduction - Notes

Explanations of cyber physical systems (CPS) and self-driving cars was detailed as an introductory paragraph. It also outlined what offensive cyber security entails. The initial introduction paragraph also described an internet of things (IoT) attack for reference to how prevalent offensive security is.

Acknowledgement of there being a lack of research regarding systematic measurement of cyber-attacks.

3 Offensive Security Framework Proposal

The researchers outline a proposal of an offensive cybersecurity framework as a new way to systematically measure a score for cyber attacks in an isolated event, since, according to their research, there has been no score representation for cyber attacks.

File-less cyber attacks uncovered from 2014 to 2018 and APT threats were selected for the proposed solution.

The overall scoring system of the proposed model was decomposed in two steps.
1) Calculate the score for how many Offensive Cybersecurity elements were used in each stage of the Cyber Kill Chain (CKC).
2) Calculate how many cyber-attack techniques were used in 12 ATTCK matrix.

4 Literature Review

The researchers accurately review other literature and research papers to conclude on summaries to aid in their survey paper.

The researchers of this paper incorporated a literature review which is the first i have seen after surveying over 13 of these Mitre papers.

4.1 'Security for CPS' - Lit review by researchers

'Security for CPS' (Cyber Physical Systems) was outlined to focus on areas of address concepts, architecture, and research opportunities of smart cities as well as IoT and automobile attacks, spoken from the researchers conclusions. This paper said to have surveyed over 150 papers related to attacks on autonomous vehicles.

4.2 'Offensive Cyber security' - Lit review by researchers

'Offensive Cyber security' was concluded to describe how the researcher of the mentioned paper analysed the history of three generations of offensive cyber security research from 1993 to 2017.

By doing this allowed the author to investigate offensive attacks on specific vulnerabilities such as buffer overflows outlined by the researchers of this literature review.

Further literature reviews were conducted but the main ones are these first two.

5 Scoring System

The researchers collected roughly 150 reports with analyses of attacks using the links that had already been collected by the APT Group list.

They then calculated the cyber-attack score based on the offensive cybersecurity elements. MITRE ATTCK evaluations showed the scoring result for some APT groups as well.

A mathematical equation involving sigma was used to return the resulting cyber attack complexity where the equation takes into account offensive cyber security modules.

The scoring system is assessed in diagrams from the outputted results of the proposed model in order to detail findings and conclusions to the reader.

6 What problem does this solve?

The proposed solution framework was developed to give a better understanding of file-less and APT threat attacks to conclude on better strategies using the concluding information.

7 How do they solve it?

They conducted research on the complexity of attacks and proposed a model for offensive cybersecurity as well as identified offensive security areas of focus within it. This enabled derived scores for file-less and APT group cyber attacks. They also outlined a proposal of an offensive cybersecurity framework.

8 How do they assess it?

Assessments were made based on the returned scores of APT threats and file-less offensive attacks to conclude various details such as severity, ones that are most common etc.

9 Conclusion - Notes

Explanations were given as to why a proposed solution is detailed and how it can help aid in the defense of APT and file-less attacks using various Mitre Attach techniques.

Acknowledgement was also given to how the cyber security industry is constantly changing and due to this requires newly proposed security models.