UÍDE
Universidad Internacional del Ecuador

MAESTRÍA EN CIBERSEGURIDAD

INFORME DE INVESTIGACIÓN

TÍTULO: “ANÁLISIS Y PERFILAMIENTO BASADO EN EL RIESGO INFORMÁTICO DEL COMPORTAMIENTO DEL USUARIO EN TELETRABAJO”

Alumno: D. Yolanda Ayala Santacruz

Tutor: Profesor D. Sebastián Tamayo

Quito, mayo de 2021

ABSTRACT

Las organizaciones se enfrentan a atacantes silenciosos que – en promedio – se mantienen en la red de datos durante 200 días realizando conexiones sin ser detectados en ésta y así, poder obtener la mayor cantidad de información posible de la víctima; especialmente con teletrabajo. El elevado número de conexiones hace casi imposible un monitoreo de forma manual por parte de los analistas por lo que alternativas como el aprendizaje de máquina facilitarían en gran medida dicho análisis y en la definición de patrones en el tráfico de datos. En este proyecto de investigación se usó el algoritmo *k-medias* para determinar el comportamiento de las conexiones agrupándolas en clústeres de distancias a un centroide similares, en conjunto del algoritmo *z-score* para la determinación de atípicos. Finalmente, en base a reglas del comportamiento habitual de los atacantes se evaluaron los patrones a ser supervisados en el monitoreo.

Companies face to silent attackers which – in mean – are in the data network for 200 days performing connections without option to be detected so they can get more information about the victim, especially with teleworking. Manual supervision by analyst is impossible due to the huge number of data transactions, that is why it is important to apply other alternatives as machine learning to do those analysis and traffic pattern definition easier. K-means algorithm was used to define the pattern behavior of connections grouping by the distances to a centroid into similar clusters and z-score algorithm was applied for outlier detection and removal. Finally, patterns were analyzed in based of behavior rules of attackers.

PALABRAS CLAVE

Aprendizaje de máquina, k-medias, z-score, ciberseguridad

Machine learning, k-means, z-score, cybersecurity