UIDE
Powered by
Arizona State University

Maestría en

CIBERSEGURIDAD

Ejecución y análisis de un ransomware dentro de un ambiente seguro para la creación de un manual de buenas prácticas

Proyecto previo a la obtención del título de Master en Ciberseguridad

AUTORES: Bryan, A. Lopéz
Diana, M. Garcés
Elvis, B. Campaña
Andrés, E. Narváez
Jorge, A. Aguayo
Alex, D. Simbaña
Hernán, J. Nacimba

QUITO – ECUADOR | 2022

RESUMEN

Durante la pandemia del COVID 19 los ciberataques en el Ecuador aumentaron significativamente perjudicando a las empresas y a la población con la encriptación y difusión de datos confidenciales e importantes como son los ataques ocurridos al Banco del Pichincha y CNT en 2021. La investigación se enfoca en el análisis dinámico de un malware tipo ransomware; con este tipo de este análisis se experimenta la conducta del mismo y la interacción del entorno en que se desenvuelve. Se estudia las interrupciones que realiza a la red, las interrupciones de los puertos, datos capturados, archivos cifrados, actividades operativas, entre otras. Se utilizaron herramientas de Sandboxing que facilitan el análisis del código fuente permitiendo conocer más información del malware. Todo este análisis descrito se lo realiza en un ambiente virtualizado para un mejor estudio. Al finalizar el estudio y tras conocer las características y comportamiento que presentó el ransomware se elaboró un manual de buenas prácticas que incremente las seguridades ante este tipo de ataque.

PALABRAS CLAVE: Ransomware, malware, sandboxing, análisis estático

ABSTRACT

During the COVID 19 pandemic, cyber-attacks in Ecuador increased significantly, harming companies and the population with the encryption and dissemination of confidential and important data, such as the attacks that occurred on Banco del Pichincha and CNT in 2021. The research focuses on the dynamic analysis of ransomware-type malware; With this type of analysis, its behavior and the interaction of the environment in which it operates are experienced. The interruptions made to the network, port interruptions, captured data, encrypted files, operational activities, among others, are studied. Sandboxing tools were used that facilitate the analysis of the source code, allowing more information about the malware to be known. All this described analysis is carried out in a virtualized environment for a better study. At the end of the study and after knowing the characteristics and behavior of the ransomware, a manual of good practices was drawn up to increase security against this type of attack.

KEYWORDS: Ransomware, Malware, Sandboxing, Static Analysis