UIDE
Powered by
Arizona State University

eig Business School

Maestría en

CIBERSEGURIDAD

Trabajo de investigación previo a la obtención del título de Magíster en Ciberseguridad

AUTORES: Coello Vargas Jorge Alberto
Holguin Samaniego Helen Patricia
Quinteros Moran Jonathan Elvin
Saca Quizhpe Frank Joel

TUTORES: Alejandro Cortés

Iván Reyes

TEMA:

"Ingeniería Inversa a un Malware."

Abstract

Currently, the most common way that cyber attacker groups use to try to infiltrate the computer system of their potential victims is to send emails that contain malicious files or software known as malware. In the face of these cyberattacks, many Antivirus software development companies have reinforced their security signatures to try to contain these malware type files as much as possible and prevent damage to the operating system of the computer where it has been detected, or even prevent the theft of data from the user who owns or is responsible for the computer equipment. While it is true that antivirus security firms work optimally and assertively, for a cybersecurity specialist this is not enough, and they must try to know how the malicious code was created and propagated. That is why technical document has been developed, which explains the procedure followed by the method known as Reverse Engineering, which allows a thorough examination of malicious software, to understand its operation and design logic. The results obtained by applying this method provide valuable information to the researcher, because it also allows him to detect the possible security breach through which the malware entered his computer system.

Keywords: cybersecurity, malware, reverse engineering, security breach.

Jonathan Quinteros Morán.

Agradezco a mi abuela, pilar fundamental en mi vida, y a mi madre, por su confianza, apoyo incondicional y guía constante. A mis hermanos, por su apoyo y escucha en momentos difíciles, y a mi novia, por su paciencia, comprensión y aliento en cada obstáculo.

Frank Saca Quizphe

Resumen

En la actualidad la forma más común que utilizan los grupos de ciber atacantes para tratar de infiltrarse a los sistemas informáticos de sus posibles víctimas, es el envío de correos electrónicos que contienen archivos maliciosos o conocidos como malware.

Ante estos ciber ataques, muchas empresas desarrolladoras de software de Antivirus han reforzado sus firmas de seguridad para tratar de contener al máximo estos archivos de tipo malware y evitar un daño al sistema operativo del computador donde ha sido detectado, o incluso evitar el robo de datos del usuario propietario o responsable del equipo informático. Si bien es cierto las firmas de seguridad de los antivirus trabajan de manera óptima y asertiva, para un especialista en ciberseguridad esto no es suficiente, y debe de tratar de conocer como fue creado y propagado el código malicioso. Es por esto que se ha desarrollado este documento de carácter técnico, en el cual se explica el procedimiento que sigue el método conocido como Ingeniería Inversa, el cual permite examinar a fondo el software malicioso, para entender su funcionamiento y lógica del diseño. Los resultados que se obtienen al aplicar este método aportan información valiosa al investigador, porque le permite detectar también la posible brecha de seguridad por donde entró el malware su sistema informático.

Palabras Claves: ciberseguridad, malware, ingeniería inversa, brecha de seguridad.