UIDE
Powered by
Arizona State University

Maestría en

CIBERSEGURIDAD

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

AUTOR: Ing. Xavier Noboa López

Ing. Fernando Villacres

Ing. Yadira Patricia Avila

Ing. Nicolas Inchiglema

TUTOR: Msc. Ing. Alejandro Cortés López

Realizar una infección de Wannacry a una estación de trabajo a través del uso de Flipper Zero y realizar la ingeniería inversa del malware distribuido.

RESUMEN.

El uso de dispositivos usb indetectables se ha vuelto común en estos últimos años con el lanzamiento de Flipper Zero, Rubber Ducky, Bash Bunny, etc; los cuales permiten a los atacantes ejecutar scripts de manera automatizada, vulnerando la seguridad de los dispositivos permitiendo tomar el control total de los mismos. La mayoría de las personas usan sus estaciones de trabajo sin percatarse de que se encuentra conectado a un dispositivo adicional o innecesario, esto da cabida a que los atacantes se aprovechen de puertos o periféricos para inyectar códigos maliciosos de manera imperceptible. Actualmente los ataques de ransomware tienen una media aproximada de ocurrencia cada 14 segundos, sumado a que en las organizaciones no mantienen actualizados sus sistemas, esta es una gran brecha de seguridad informática que se ha visto sobre todo en sistemas operativos Windows 7 que cuentan con muchas vulnerabilidades explotables como la de EternalBlue (MS17-010) y la cual puede afectar directamente a la organización y al negocio, ya que la información es el activo más importante de las organizaciones, por otro lado para entender cómo el atacante puede tomar el control sobre los dispositivos, es importante realizar ingeniería inversa tanto estática como dinámica, en donde se encuentra las porciones de código que ejecuta y cómo afecta a los dispositivos, para luego de ello proceder con una respuesta al incidente y mantener la disponibilidad del negocio apoyándose en DRP o en un manejo seguro de respaldos.

Palabras claves: Ciberseguridad, Ransomware, EternalBlue, Flipper Zero.

ABSTRACT

The use of stealthy usb devices has become common in recent years with the release of Flipper Zero, Rubber Ducky, Bash Bunny, etc; which allow attackers to execute scripts in an automated way, violating the security of the devices allowing them to take full control of them. Most people use their workstations without realizing that they are connected to an additional or unnecessary device, allowing attackers to exploit ports or peripherals to inject malicious code imperceptibly. Ransomware attacks currently have an approximate average occurrence of every 14 seconds, added to the fact that organizations do not keep their systems up to date, this is a major information security breach that has been seen especially in Windows 7 operating systems that have many exploitable vulnerabilities such as EternalBlue (MS17-010) and which can directly affect the organization and the business, since information is the most important asset of organizations, on the other hand to understand how the attacker can take control over devices, it is important to perform both static and dynamic reverse engineering, where the portions of code that it executes are located and how it affects the devices, to then proceed with an incident response and maintain business availability by relying on DRP or in safe management of backups.

Keywords: Cybersecurity, Ransomware, EternalBlue, Flipper Zero.