UIDE
Powered by
Arizona State University

Maestría en

CIBERSEGURIDAD

Estudio de ataques RAT en dispositivos móviles Android a funcionarios de instituciones públicas que manejan información sensible.

Proyecto previo a la obtención del título de Master en Ciberseguridad

AUTOR: Asqui Yánez Gustavo Misael
Cadena Salgado Christian Germán
Piedra Ramírez Paulina Gabriela
Rentería Balseca Andrea Gabriela
Riera Sayay Danny Mauricio
Téllez Gómez Wernher Braun
TUTOR: Msc. Alejandro Cortés López

QUITO – ECUADOR | 2022

RESUMEN

El teléfono móvil es el articulo más utilizado para comunicarnos y entretenernos, con una variedad de aplicaciones que se puede instalar en el teléfono inteligente, por otra parte, es el dispositivo que los ciberdelincuentes utilizan para el robo de información, utilizando técnicas como el phishing para engañar a los usuarios, también el atacante cibernético crea malware con el objetivo de introducirse al teléfono móvil sin autorización del propietario, con la finalidad de obtener de forma fraudulenta información de las víctimas o de entidades públicas o privadas donde laboran, con el propósito de realizar divulgación no autorizada de información, el cual representa un peligro grave para la integridad de la persona o de la institución, por lo tanto, nuestro estudio es conocer el software malicioso Remote Administration Tool (RAT) que el atacante utiliza para vulnerar los teléfonos móviles con sistema Android, el cual puede acceder de forma remota al teléfono móvil, donde puede tener control y obtener los datos que almacena el teléfono, para nuestra práctica utilizamos un caso de una institución pública donde el personal manipula información sensible y clasificada que representa un peligro grave para la seguridad general del país; el propósito de la investigación es dar a conocer el ataque informático con malware de tipo RAT y mitigar el robo de información, con esto aportar a una cultura de ciberseguridad.

PALABRAS CLAVES: Malwares, Smartphone, Android, Remote Administration Tool, vulnerabilidad, ciberdelincuentes

ABSTRACT

The cell phone is the most used item to communicate and entertain nowadays, since it has a variety of applications that can be installed on the smartphone with facility. On the other hand, it is the main device that cybercriminals use to steal information by using techniques such as phishing to deceive users. Cyber attackers also create malware with the aim of entering the mobile phone without the owner's authorization in order to fraudulently obtain information from the victims or from public or private entities where they work, with the purpose of carrying out unauthorized disclosure of information which represents a serious danger to the integrity of the person or the institution. Therefore, our study is to know the Remote Administration Tool malicious software that the attacker uses to violate cell phones with Android system, which can remotely access the phones where you can have control and obtain the data stored by the phone. For our practice we use a case of a public institution where the staff manipulates sensitive and classified information that represents a serious danger to the general security of the country. The purpose of the research is to publicize the computer attack with RAT-type malware and mitigate information theft, thereby contributing to a culture of cybersecurity.

KEY WORDS: Malwares, Smartphone, Android, Remote Administration Tool, vulnerability, cybercriminals