UIDE
Powered by
Arizona State University

Maestría en

CIBERSEGURIDAD

Tesis previa a la obtención del título de Magíster en Ciberseguridad

AUTOR: Ing. Marco Victor Caicedo López
Ing. Cristian Wladimir Chamba Montesdeoca
Ing. Esteban Alejandro Naranjo Andrade
Ing. Juan Andrés Tello Guerra

DIRECTOR DE TESIS: Ing. Alejandro Cortés López

Análisis forense en incidentes de phishing en la empresa A&K Ecuador

QUITO – ECUADOR | 2023

Resumen

El phishing es una técnica de ciberataque que consiste en enviar correos electrónicos fraudulentos que simulan ser de entidades legítimas con el fin de engañar a los usuarios para que revelen información personal o financiera, o para que ejecuten archivos maliciosos. Este trabajo presenta un estudio de caso de un incidente de phishing ocurrido en la empresa A&K Ecuador, una compañía dedicada a la venta de servicios turísticos. El objetivo es identificar la metodología para realizar el análisis forense, analizar la trazabilidad y toda la ruta del ataque, identificar apropiadamente las evidencias y realizar el análisis de estas, adicionalmente encontrar los indicadores de compromiso y los resultados, impacto y consecuencias del ataque y por último la ejecución de prevención y mitigación mediante concientización hacia los usuarios. Para ello, se utilizan herramientas y técnicas de análisis forense digital, como el examen del sistema de archivos, el registro, los correos electrónicos y los archivos adjuntos; donde se logrará determinar el origen, el vector, el alcance y el daño del ataque, así como las medidas correctivas y preventivas para evitar que se repita.

Palabras clave

Análisis forense, phishing, ciberseguridad, evidencias digitales, ataque cibernético, indicadores de compromiso, prevención, mitigación, concientización, usuarios, seguridad informática, amenazas cibernéticas, investigación de incidentes, recopilación de pruebas, análisis de malware, riesgo cibernético, cadena de ataque, respuesta a incidentes, informática forense, análisis de amenazas, seguridad de la información, análisis de impacto, evaluación de consecuencias, seguridad empresarial, ciberdelincuencia, protección de datos, políticas de seguridad.

Abstract

Phishing is a cyberattack technique that involves sending fraudulent emails that pretend to be from legitimate entities in order to trick users into revealing personal or financial information, or into executing malicious files. This paper presents a case study of a phishing incident that occurred in the company A&K Ecuador, a company dedicated to the sale of tourism services. The objective is to identify the methodology to perform the forensic analysis, analyze the traceability and the entire route of the attack, properly identify the evidence and perform the analysis of these, additionally find the indicators of compromise and the results, impact and consequences of the attack and finally the execution of prevention and mitigation through awareness among users. This is done by using digital forensics tools and techniques, such as file system examination, logging, emails, and attachments; where it will be possible to determine the origin, vector, scope and damage of the attack, as well as the corrective and preventive measures to prevent its recurrence.

Key words

Forensic Analysis, Phishing, Cybersecurity, Digital Evidence, Cyberattack, Indicators of Compromise, Prevention, Mitigation, Awareness, Users, Computer Security, Cyber Threats, Incident Investigation, Evidence Collection, Malware Analysis, Cyber Risk, Attack Chain, Incident Response, Computer Forensics, Threat Analysis, Information Security, Impact Analysis, Consequence Assessment, Business Security, cybercrime, data protection, security policies.