

SIMULACION DE ATAQUE RANSOMWARE

2023



1.0 Introducción/Propósito

Ciber-ejercicio con el objetivo de obtener una visión general sobre el comportamiento y la efectividad de la solución CHECKPOINT ante un ataque de RANSOMWARE.

2.0 Alcance

Equipos de laboratorio de entorno controlado.

3.0 Detalles

Fecha de Realización de Simulación: 01/02/2023

3.1 Esquema de Fases

El ejercicio para evaluar el sistema de protección ante ataques de RANSOMWARE se plantea acorde a las siguientes fases:



3.2 Preparación del Entorno

Se disponen de dos equipos en un ambiente controlado para dicho ciber-ejercicio, relacionado al ataque de RANSOMWARE.

EQUIPO A: Atacante

EQUIPO B: Víctima

- El EQUIPO A posee datos del sistema y de los usuarios del EQUIPO B.

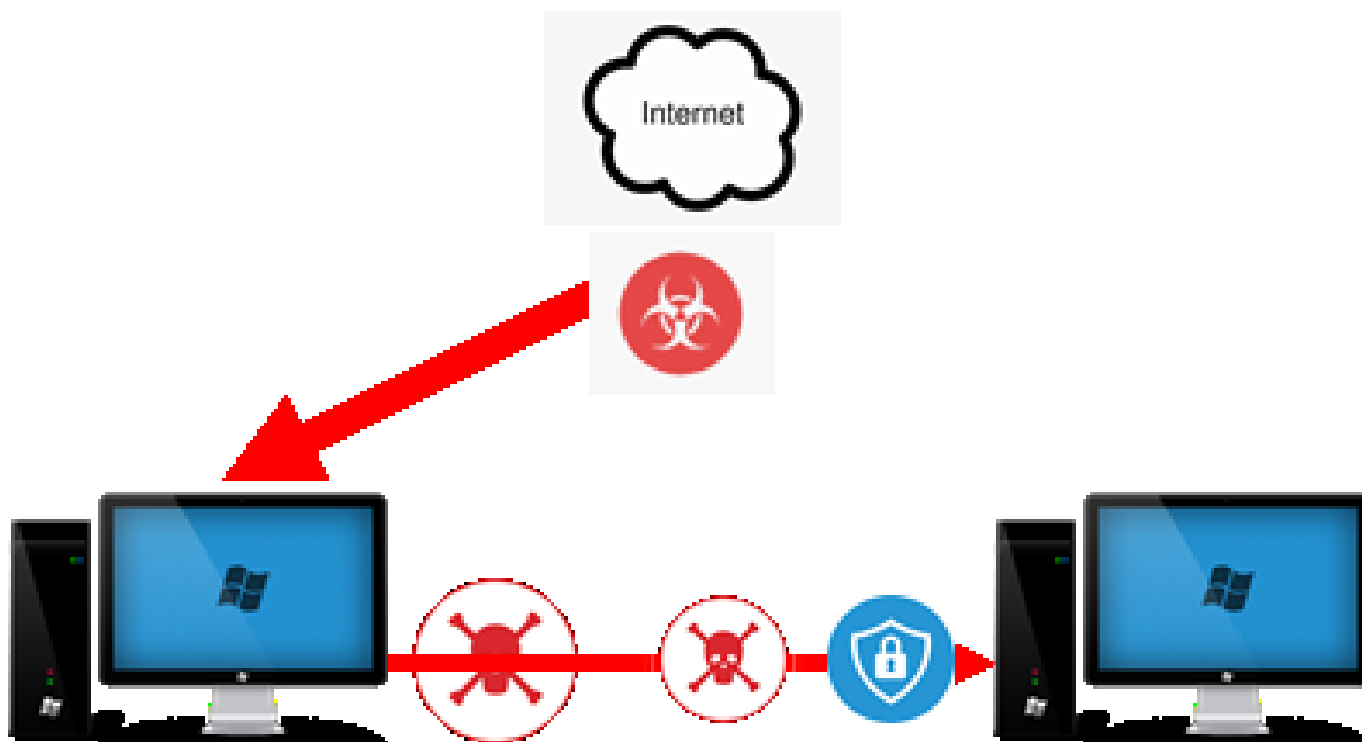
EQUIPO A inyecta en los procesos la ejecución en programa JAVA con RANSOMWARE infectado.

3.3 Participantes/Integrantes

Participantes	Nro. de Legajo	Firma
Antonio Ramón Galeano	1754	
Reinaldo Daniel Gunther Gamarra	3228	

3.4 Diseño de Muestra


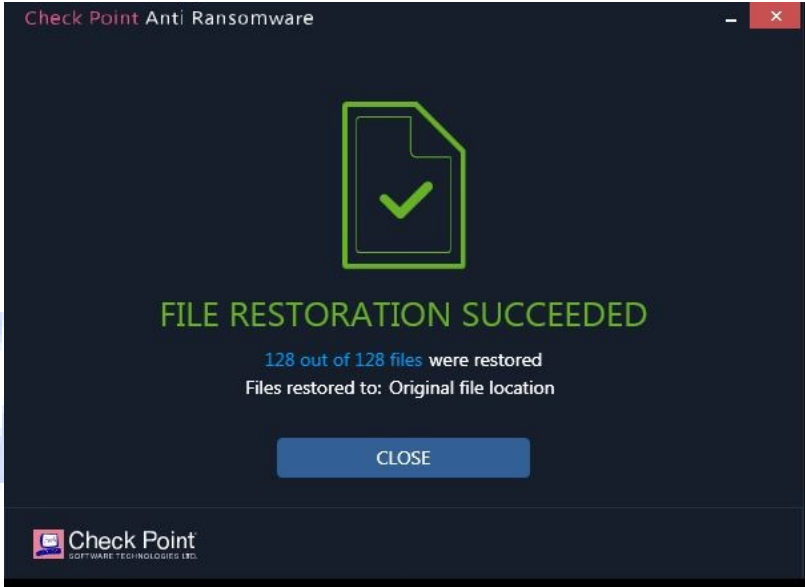
Se ejecutan los archivos de encriptación; dichas muestras permiten analizar las características y el nivel de defensa, ofrecido por la plataforma REMO.





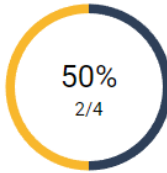








3.5 Ejecución de Muestras

Con el objetivo de identificar las vulnerabilidades y/o limitaciones de los dispositivos de protección, se hace la ejecución de la siguiente secuencia:

Equipo	Acción	Imagen
A	Inyecta ataque en procesos	

B	Detección del ataque del ERD	
B	Detiene y restaura archivos encriptados	

Resultado	
Mínimo impacto en el negocio	<div>  BUSINESS IMPACT : What was the potential damage done? </div> <div>  134 Data Loss  147 Data Ransom </div> <div>  REMIEDIATION : Were all incident created elements removed? </div> <div>  50% 2/4  terminated processes  100% 144/144  restored files </div>
Resumen forense	<div>  BUSINESS IMPACT (2 categories, 281 events) : INFO001: 5180b7e3-3df7-4914-b23c-87f30853357b </div> <p>These are potentially important events that have business impact.</p> <ul style="list-style-type: none">  Data Loss (134 events)  Data Ransom (147 files, 144 recovered, 3 unrecovered)

Aprobación

Elaborado por:작성자	Supervisado por:작성자	Aprobado por:승인	Aprobado por:승인 Gerente General LUIS BOLAÑOS ZARZA
-------------------	---------------------	-----------------	--