EasyChair Preprint

№ 10844

# Professional Ecosystem to Support the Malware Life Cycle

Irvin Sáenz



September 6, 2023

# Ecosistema profesional para el soporte del ciclo de vida del Malware

Ing. Irvin Sáenz Córdoba, Máster

*Especialidad Ciberseguridad*
*Ministerio de Educación Pública*
San José, Costa Rica
irvin.saenz.cordoba@mep.go.cr

**Resumen-** En la actualidad uno de los ataques más sofisticados que tienen los Ciberdelincuentes tanto a nivel de empresas como en casos a nivel personal son los virus denominados Malware; que entre otras cosas permite el robo de la información personal, social, financiera o corporativa de las organizaciones e individuos. Ante esta situación se deben de aplicar mecanismos que les permitan en ambos escenarios aplacar este tipo de ataques tomando como referencia la guía de ciberseguridad CyBOK.

La Guia es una referencia oficial que les permite a los profesionales en informática y ciberseguridad implementar medidas que les permitan crear un ecosistema óptimo para la puesta en marcha y soporte del ciclo de vida del Malware y sus derivaciones. El ataque contra el este tipo de amenazas en las empresas supone un reto para prevenir, detectar y eliminar este tipo de ataques los cuales deben de administrarse con prioridad y cautela por parte de los involucrados quienes deben buscar la forma de mitigar este tipo de amenazas de manera estratégica. Hoy por hoy una de las principales motivaciones que tienen los atacantes es el dinero por lo que el malware se convierte una manera relativamente "sencilla" para perpetrar el secuestro de información y obtener grandes ganacias económicas por estos hechos.

***Abstract*—** Currently, one of the most sophisticated attacks that Cybercriminals have both at the company level and in personal cases are the viruses called Malware; which among other things allows the theft of personal, social, financial or corporate information of organizations and individuals. Faced with this situation, mechanisms must be applied that allow them to appease this type of attack in both scenarios, taking the CyBOK cybersecurity guide as a reference.

The Guide is an official reference that allows IT and cybersecurity professionals to implement measures that allow them to create an optimal ecosystem for the implementation and support of the life cycle of Malware and its derivations. The attack against this type of threat in companies is a challenge to prevent, detect and eliminate this type of attack, which must be managed with priority and caution by those involved who must find ways to mitigate this type of threat. strategic way. Today, one of the main motivations of attackers is money, so malware becomes a relatively "simple" way to perpetrate information hijacking and obtain large financial gains for these events.

***Palabras claves*—**Malware, Ransomware, subasta de datos, suplantación de identidad, secuestro, estrategia anti-malware.

## I. INTRODUCCIÓN

El proceso de segmentación en TI se ha convertido en un reto para las organizaciones que aún no cuentan con personal en riesgos y ciberseguridad, ya que la experiencia en el campo de la seguridad informática no solamente involucra a programadores, analista de sistemas, administradores de base de datos, telemáticos y soportistas técnicos por mencionar las principales figuras tradicionalmente en el área sino también engloba a nuevos puestos en el área como desarrolladores de malware y antivirus, cazadores de ciberamenazas e investigadores que deben desarrollar nuevos paradigmas para afrontar las estrategias más sofisticadas que desencadenan este tipo de ataques.

El estado de vulnerabilidad de las empresas y personas es latente y son cada vez más los tipos de ataques de esta dimensión, es por ello que los departamentos de TIC, deberán crear los mecanismos necesarios basados en la guía CyBOK para llevar de la manera adecuada la detección, administración, seguimiento y control de los incidentes de esta dimensión

## II. TIPOS

Los malware por su naturaleza son virus que irrumpen, dañan y alteran los sistemas informáticos de tal manera que lo vuelven inutilizable es por ello que se consideran o clasifican en distintos tipos:

**Un virus:** Este tipo de malware que se puede copiar a sí mismo y distribuirse a otros archivos, por lo general este tipo de programa afecta a otros programas y se propaga replicándose en la computadora, su fuente se puede dar de dispositivos de medios extraíbles, descargas de internet o bien desde una fuente de correo electrónico que es uno de los casos más típicos.

**Worms o gusanos**: Basado en "el gusano de la manzana de la princesa" este se replica sin intervención humana, similar al anterior a diferencia que es más automatizable.

**Troyanos**: Dado su nombre a la guerra de la mitología griega en que uno de sus principales personajes Odiseo (protagonista de la novela la Odisea) construye un caballo gigante de madera para infiltrarse en la ciudad de Troya y con ello atacar a los troyanos para vengar el secuestro de Helena de Esparta (reina griega), bajo este contexto histórico se le da vida al malware que se hace pasar por un programa legítimo que en el fondo es un malware que se manifiesta de manera ilegitima en la computadora provocando un daño irreversible que en efecto engaña al usuario que lo ejecuta.

**Ransomware**: Unión de las palabras rescate y mercancía es considerado un tipo de malware que encripta la información y que solicita una retribución económica al o a los usuarios para desencriptar la información, actualmente es una de las

amenazas a las que se está más expuestos, enfocándose principalmente en los sistemas operativos de escritorio Windows, Android y MacOS.

**Spyware:** El spyware o software espía actúa como un programa que recopila información personal como usuarios claves, tarjetas de crédito y en el peor de los casos logra activar el hardware del equipo como es el caso del micrófono y cámara del usuario sin previo consentimiento.

**Botnets:** El botnet por su parte congrega a una red de dispositivos infectados con malware que se pueden controlar de forma remota por un atacante o en su defecto por Inteligencia Artificial, uno de los ataques más típicos es la denegación de servicios (DoS) y la denegación de servicios distribuida (DDoS).

**Otras amenazas:** Existen otras amenazas como las bombas lógicas, keyloggers, criptominería, rootkits, adwares que similares a los anteriores pueden provocar daños en la infraestructura crítica de la empresa, es importante mencionar que estos son solo algunas del sin número de amenazas que existen y que para efectos de esta investigación se mencionan las más conocidas en el ámbito.

TABLE I. TIPOS DE MALWARE

| Tipo Malware | Efecto |
|---|---|
| Ransomware | Secuestro y chantaje |
| Spyware | Espionaje e robo de datos |
| Adware | Publicidad extrema |
| Worms | Propaga y llenan memoria |
| Troyanos | Malware enmascarado |
| Bots | Convierte PC en zombie |

## III. TÉCNICAS PARA PROPAGAR MALWARE

### *A. Ingenieria Social:*

C Lopéz y R. Salvador lo definen como "*La aplicación de técnicas, que los hackers utilizan para engañar a un usuario autorizado de sistemas informáticos de una compañía para que revele información sensitiva*" en resumen es el "arte de hackear humanos" utilizando la susceptibilidad psicológica y engaño para lograr su cometido haciendo suplantación de identidad.

### *B. Pishing:*

Los atacantes suelen enviar correos electrónicos, mensajes de texto o mensajes a sistemas de mensajería instantánea y redes sociales con enlaces falsos que parecen ser de fuentes legítimas cuando en realidad son fraudulentos y dañinos, en algunos casos también lo hacen por medio de llamadas locales e internacionales.

### *C. Ataque de Quid Pro Quo:*

Esta técnica está basada en el método que el atacante promete algún beneficio económico o social a la víctima a cambio de información de la organización, este se hace pasar por compañeros de la misma empresa o colaboradores de una entidad suplantando a estos para engañar al usuario final, dentro de los casos comunes se hacen pasar por colaboradores del área de TI o de funcionarios de entidades financieras indicando alguna situación especial con las cuentas bancarias de sus víctimas.

### *D. Baiting:*

Este ataque consiste en dejar a vista y paciencia de las personas que engañaran una USB o Disco con software malicioso para que dicha victima tenga la tentación de ejecutar lo que se encuentra en el dispositivo y con ello infectar los equipos de la red de la empresa, tal fue el caso del Stuxnet en fabricas en Asia, Europa y los EEUU por allá del año 2010, lamentablemente es una técnica muy utilizada por las agrupaciones para dañar empresas.

### *E. Pretexto:*

Esta técnica tiene guiones muy elaborados donde los atacantes de basan en un discurso generando miedo en los usuarios de manera que se ganan su confianza y se valen de su susceptibilidad psicológica para "enredar" a la víctima y con ello lograr su cometido, es similar QPQ sin embargo este tiene una suspicacia psicológica mas elaborada dado el seguimiento que realizan los ciberdelincuentes con sus victimas

### *F. Otras técnicas:*

Existen otras técnicas similares a las anteriores como el caso del whaling, farming, pharming que de igual manera combinan los casos de engaño a través de la confianza por medio de enlaces maliciosos para que la víctima los ejecute.

## IV. SUGERENCIAS CYBOK

Por sus siglas en inglés el Cybersecurity Body of Knowledge" (El Cuerpo de Conocimiento de Ciberseguridad). Brinda una serie de recomendaciones basadas en este cuerpo de conocimiento, dentro de las recomendaciones que podrían ser aplicadas en las organizaciones para enfrentar este tipo de situaciones, destacan las siguiente:

### *A. Implementación del Cyber Kill Chain*

La guía CyBOK sugiere como una actividad clave para identificar, detener y recuperarse ante un ciberataque implementando la estrategia para identificación de operaciones de ciberseguridad básica denominada**: Cyber Kill Chain**, la cual consiste en una serie de siete etapas basadas en el ámbito militar que les permiten a los administradores de incidentes de ciberseguridad administrar y tomar medidas frente a un incidente y como responder de manera adecuada ante un ciberataque, estas etapas según esta guía de conocimiento se detalla a continuación:

1. Reconocimiento (Recopilación del objetivo)
2. Preparación (Preparación ataque)
3. Distribución (Transmisión del ataque)
4. Explotación (Detonación del ataque)
5. Instalación (Instalación malware)
6. Comando y control (Secuestro y control)
7. Acciones sobre los objetivos (Expansión)

Según la mayoría de la literatura relacionada a este modelo se basa en las técnicas de ataque militar a medida que permite a los equipos de informática y ciberseguridad

comprender, detectar y prevenir las ciberamenazas persistentes y de alta complejidad como es el caso de este tipo de software malicioso.


*Ilustración 1: Cyber Security Kill Chain, Fuente: Lockheed-Martin*

### *B. Análisis de Malware*

Dentro de las principales recomendaciones para verificar el código del malware existen dos recomendaciones importantes las cuales son dinámica y estáticamente siempre y cuando se realice en un entorno de zona desmilitarizada (DMZ) en la cual se examina el código en entornos aislados ya que es importante determinar las dimensiones y capacidades destructivas y de daño que tiene el malware que se ha descubierto ante esta situación, parte de las recomendaciones que brida el cuerpo de conocimiento en ciberseguridad están:

- Análisis estático: En algunos casos es necesario verificar el código fuente de manera superficial para ver la dimensión de daño a provocar, es por ello que se recomienda utilizar un entorno aislado sin que vaya a provocar daños a otros equipos en la red de la organización.
- Análisis dinámico: Se recomienda un ambiente sandbox el cual es un entorno aislado donde se puede ejecutar un código o software sin afectar al sistema operativo y archivos de la organización, actualmente se encuentran en entornos de máquinas virtuales, contenedores y en algunos entornos con algunos lenguajes de programación muy populares como Python y Java.
- Aleatorización y fuzzing es aquel método en el que se "testea" el software para identificar comportamientos anómalos y erróneos para predecir el rumbo que toma el programa al garantizar que el software sea seguro y confiable y no sea susceptible a ataques y vulnerabilidades de malware.
- Compartir los hallazgos supracitados con otros analistas de ciberseguridad de la empresa o foros para obtener una retroalimentación del virus para conocer el comportamiento del malware y poder predecir las causas y efectos que podría provocar.
- Otros como la ejecución simbólica y concólica que serían otras técnicas basadas en pruebas del sistema en un contexto mucho más detallado que permiten posibles fallas en los sistemas.
- Otros casos más sofisticados y que con lleva a un mayor análisis e investigación es el del malware polimórfico que por su naturaleza cambia su apariencia y estructura cada vez que se propaga o infecta un sistema dada su amplia estructura incluso son capaces de generar nuevas versiones de sí mismas en tiempo real lo cual complica la labor de los analistas de ciberseguridad en la reducción del daño y evolución.

### *C. Entornos recomendados*

Los entornos que sugiere el CyBOK basado en comparación de entornos de análisis de malware son sugerentes ya que distintas investigaciones arrojan que los ambientes virtualizados son más seguros en comparación a ambientes bare metal que son más propensos a fallas. El análisis de malware en entornos virtuales es seguro ya que no puede dañar el sistema operativo o los archivos de los usuarios, por otra parte el entorno precisamente es usado a menudo para fines de investigación y desarrollo según la recomendación de esta literatura.

## V. POLITICAS A IMPLEMENTARSE

A partir de la lectura se desprende la importancia que tiene la implementación de políticas basadas en el cuerpo de conocimiento en ciberseguridad del CyBOK en la que se podrían poner en práctica las siguientes actividades en aras de minimizar el impacto de los virus:

### *A. Mejorar la cooperación entre los actores del ecosistema:*

Los diferentes actores del ecosistema profesional para el soporte del ciclo de vida del malware deben mejorar su cooperación. Entre ellos se involucran a los altos directivos, colaboradores de rango intermedio, personal técnico, personal TI y demás actores en un sentido que todos tengan acceso a la misma información y que estén trabajando juntos para desarrollar las mejores defensas contra el malware, ya sea con capacitación continua, investigación y desarrollo así como análisis continuo de las principales amenazas que se dan cotidianamente esto con el objeto para desarrollar nuevas técnicas para detectar y responder al malware y convertir a la empresa en una organización más resiliente a este tipo de ataques

### *B. Educar a los usuarios finales:*

Los usuarios finales de la organización deben estar educados sobre las amenazas de malware y sobre cómo protegerse, no solamente es capacitación continua, sino también demostraciones, análisis de casos, seguimiento de incidentes a nivel mundial, con esta serie de elementos se ayudaría a mitigar un poco estas falencias.

### *C. Implementar políticas y procedimientos de seguridad:*

Las organizaciones deben implementar políticas y procedimientos de seguridad para proteger sus sistemas contra el malware. Estas políticas y procedimientos deben ser diseñados para abordar las amenazas específicas que enfrenta la organización que deben ser puestas en práctica.

### *D. Realizar simulacros de ataques de malware:*

Las organizaciones deben realizar simulacros de ataques de malware para evaluar su preparación para un ataque real. Estos simulacros ayudarán a identificar áreas donde la organización puede mejorar su defensa contra el malware, importante considerar a todos los colaboradores de la empresas para estos ensayos.

## VI. CONCLUSIONES

De esta forma se da una pincelada de las principales recomendaciones abordadas en la investigación esperando sean un insumo suficiente el cual pueda servir de soporte para el manejo de este tipo de amenazas y como departamento aplicar las mejores estrategias de resiliencia.

## REFERENCIAS

Para la elaboración de esta guía se toman como referencia las siguientes investigaciones y proyectos relacionados con la ciberseguridad.

Para artículos publicados en revistas de traducción, proporcione primero la cita en inglés, seguida de la cita original en el idioma extranjero.


[1] Crego Sánchez, C. A. (2021). Guía de prevención y respuesta frente a ataques de ransomware.

[2] Kohnke, A., Tenbergen, B., & Mead, N. (2022). Using Cybersecurity Body of Knowledge (CyBOK) Case Studies to Enhance Student Learning, Cap 6.

[3] López Grande, C. E. (2015). Ingeniería social: el ataque silencioso. Revista Tecnológica: no. 8.

[4] Moreno, J., Rodriguez, C., & Leguias, I. (2020). Revisión sobre propagación de ransomware en sistemas operativos Windows. I+ D Tecnológico, 16(1), 39

[5] Orueta, G. D. (2016). ¿ Qué es el malware?.

[6] Ruiz de Elvira, Antonio (1982). Mitología clásica. Madrid: Gredos. ISBN 84-249-0204-1.

[7] Ruiz de Elvira, Antonio (1982). Mitología clásica. Madrid: Gredos. ISBN 84-249-0204-1.

[8] Saenz, Irvin (2023). Elaboración Propia (sf).