**0.UNIVERSIDAD REY JUAN CARLOS**

MÁSTER EN CIBERSEGURIDAD Y PRIVACIDAD



**Análisis e Ingeniería Inversa de Olympic Destroyer**

**Autor:** Julio Alberto Ceballos Camarena

**Director:** Gerardo Fernández Navarrete

**Guadalajara, Junio de 2019**

**Resumen y Palabras clave**

**Abstract**

**1. INTRODUCCIÓN**

1.1 Objeto y objetivos del estudio

1.2 Metodología

1.3 Herramientas utilizadas

**2. ANÁLISIS ESTÁTICO**

**3. ANÁLISIS DINÁMICO**

**4. CONCLUSIONES**

**5. BIBLIOGRAFÍA Y REFERENCIAS**

**6. ANEXOS**

**Resumen**

Los Juegos Olímpicos de Invierno de Pyeongchang (Corea del Sur) de 2018 sufrieron un ciberataque durante su ceremonia de apertura, unos hackers desconocidos atacaron los servidores justo antes de la misma, y como consecuencia, muchos espectadores se quedaron sin asistir a la ceremonia por no poder imprimir sus entradas. Como resultado del ataque, el malware, apodado Olympic Destroyer, inutilizó el sitio oficial de los Juegos y el wifi del estadio; afectando también a la retransmisión del evento.

En lo que respecta al mecanismo de propagación, Olympic Destroyer es un gusano de red. Las plataformas que se infectaron de inicio y se usaron para propagar el gusano, fueron: [pyeongchang2018.com](http://pyeongchang2018.com/), servidores de red de estaciones de esquí y los servidores de Atos, el proveedor de servicios informáticos.

Desde estas plataformas, el gusano se propagó de forma automática por la red a través de los archivos compartidos en la red de Windows. Por el camino, robó contraseñas guardadas en ordenadores infectados, las almacenó y las usó para su posterior propagación. El objetivo final de Olympic Destroyer era eliminar archivos de unidades de red que el gusano pudiera alcanzar y bloquear los sistemas que infectaba.

En el presente trabajo se aborda el estudio, desde una perspectiva estática y dinámica, del malware Olympic Destroyer, con el fin de diseccionar su funcionalidad, origen e impacto potencial para comprender cómo se comporta.

**Palabras Clave**

- Ingeniería Inversa

- Análisis Malware

- Olympic Destroyer

- Ciberataques

- Juegos Olímpicos

**Abstract**

The 2018 Olympic Winter Games in Pyeongchang (South Korea) suffered a cyberattack during their opening ceremony. Unknown hackers attacked the servers just before the event, and as a consequence, many spectators were unable to attend the ceremony because they could not print their tickets. As a result of the attack, the malware, nicknamed Olympic Destroyer, made unavailable the official website of the Olympic Games and the WiFi of the facilities, therefore affecting the broadcasting of the event.

As far as the propagation mechanism is concerned, Olympic Destroyer is a network worm. The platforms that were infected at the beginning and were used to propagate the worm were pyeongchang2018.com, network servers of ski resorts and the servers of Atos, the provider of computer services.

From these platforms, the Worm spread automatically via shared files in the Windows network. Along the way, it stole the passwords stored on the computers it infected, stocked them and used them for further propagation.

The ultimate goal of Olympic Destroyer was to remove files from network drives that it could reach and block the systems it infected.

This master thesis focuses on the study, from a static and dynamic perspective, of the Olympic Destroyer malware, in order to dissect its functionality, origin and potential impact so that its behaviour can be understood.

**Keywords**

- Reverse engineering

- Malware Analysis

- Olympic Destroyer

- Cyberattack

- Olympic Games

**1. Introducción**

**1.1 Objeto y objetivos del estudio**

En el presente trabajo se aborda el estudio, desde una perspectiva estática y dinámica, del malware Olympic Destroyer, con el fin de diseccionar su funcionalidad, origen e impacto potencial para comprender cómo se comporta.

Para ello, partimos de siete muestras que se van a analizar una por una con diferentes herramientas de análisis que nos permitan ver cómo actúan tanto en estático como de forma dinámica en un entorno o laboratorio de máquina virtual Windows 7.

Objeto general:

Identificar el tipo de amenaza para la aplicación de técnicas de análisis de malware a las muestras, estudiar posibles archivos infectados y determinar patrones de comportamiento que faciliten crear medidas de contención, mitigación y remediación de los daños y/o prevención del mismo.

Objetivos específicos:

Utilización de distintas herramientas de análisis de malware para intentar obtener la mayor cantidad de información posible sobre el mismo.

Recomendar herramientas para el análisis facilitando evidenciar las infecciones de este malware y observar sus comportamientos.

Aplicar las muestras experimentales sobre un entorno controlado para evidenciar su funcionamiento y propagación.

Realizar el análisis de las muestras concluyendo con los hallazgos significativos para cada caso.

**1.1 Metodología**

Los métodos por los que se realiza el análisis de malware son de dos tipos:

Análisis estático: El análisis estático o de código se realiza diseccionando los diferentes recursos de las muestras sin ejecutarlas y estudiando cada componente. De esta manera, podemos realizar la “autopsia” para conocer qué es lo que hace o cuáles son las consecuencias que generará si llegase a infectar un sistema. Este primer acercamiento nos permite conocer si el malware está empaquetado, en qué lenguaje de alto nivel fue desarrollado, ver qué librerías importa, las funciones que va a utilizar, el tamaño de sus secciones y otros datos de color.

Las muestras también serán desensambladas, haciendo ingeniería inversa con un desensamblador. De esta forma, podremos entender todas las acciones que realiza la amenaza y cómo es que logra infectar un sistema para robar información, realizar ataques a otros sistemas o propagarse por la red.

Análisis dinámico: El análisis dinámico o de comportamiento se realiza observando el comportamiento del malware mientras se está ejecutando en un sistema “host”. Así, podemos conocer de una manera rápida y efectiva qué acciones realiza esta amenaza en el sistema, obteniendo información acerca de los archivos creados, conexiones de red, modificaciones en el registro, etc. Este análisis se ha llevado a cabo utilizando una máquina virtual con un sistema Windows 7 para evitar que el malware infecte realmente ningún sistema. El malware también va a ser depurado mientras se ejecuta para observar el comportamiento y los efectos en el sistema host del malware paso a paso mientras se procesan sus instrucciones.

**1.3 Herramientas utilizadas**

Las herramientas que se usan en este estudio son las siguientes:

- **Detect It Easy**: es un programa multiplataforma gratuito para analizar los archivos que se cargan en la aplicación. Detecta, entre otras cosas, el compilador, revela las firmas de los archivos y cómo se empaquetan.

- **GMER**: es una aplicación que detecta y elimina rootkits.

- **Pestudio**: es una herramienta desarrollada para poder analizar fácilmente todo tipo de archivos ejecutables (de los cuales no podemos ver el código fuente), identifica la información relevante sobre el funcionamiento de los mismos y nos la muestra en una ventana pudiendo saber qué módulos de los ejecutables pueden ser peligrosos.

- **PortexAnalyzer**: es una biblioteca de Java para el análisis de malware estático de archivos ejecutables portátiles. Se centra en la robustez de las malformaciones de PE y en la detección de anomalías.

- **Process Explorer**: es una herramienta para sistemas Windows que muestra información sobre los procesos activos en el sistema pudiendo ver las DLL que se han creado o los “handles” de dichos procesos.

- **Process Monitor**: es un programa que monitoriza cualquier tipo de actividad en el sistema, como la creación de ficheros temporales, operaciones de lectura o escritura en disco, operaciones en el registro, recepción o transmisión TCP/UDP, creación de hilos, procesos… etc.

- **Cerbero** **Profiler Advanced**: es una herramienta para el análisis forense y de malware que admite una gran cantidad de formatos de archivo en los que realiza análisis permitiendo inspeccionar su diseño interno.

- **Protection ID**: aplicación de empaquetado UPX.

- **ApateDNS**: es una herramienta que permite redirigir todas las consultas DNS a través del puertoUDP 53 hacia dónde especifiquemos y de esta manera identificar los sitios a los cuáles se intenta conectar el código malicioso bajo análisis.

- **MagicISO Maker**: es una utilidad de imagen de CD/DVD que puede extraer, editar, crear y grabar archivos ISO.

**2. Análisis estático**

**Muestra 1**

**Muestra 2**

**3. Análisis dinámico**

**Muestra 1**

**Muestra 2**

**4. Conclusiones**

**5. Bibliografía y referencias**

- <https://www.kaspersky.es/blog/olympic-destroyer/15492/>

- <https://es.wikipedia.org/wiki/An%C3%A1lisis_de_malware>

- Informes:

Code Similarities with Cyber Attacks in Pyeongchang – Intezer

Dissecting Olympic Destroyer – a walk-through – cyber.wtf

Gold Dragon Widens Olympics Malware Attacks, Gains Permanent Presence on Victims' Systems

JoeSandBox report

Malicious Document Targets Pyeongchang Olympics

Malware and Winter Olympics

Olympic Destroyer Returns to Target Biochemical Labs

Olympic Destroyer Takes Aim At Winter Olympics

Olympic Destroyer's 'False Flag' Changes the Game

OlympicDestroyer is here to trick the industry – Securelist

Who Wasn’t Responsible for Olympic Destroyer

- <https://www.welivesecurity.com/la-es/2014/01/14/bases-analisis-estatico-malware-bases-desensamblado/>

- <https://www.welivesecurity.com/la-es/2011/12/22/herramientas-analisis-dinamico-malware/>

**6. Anexos**