

DATOS DE LA ACTIVIDAD							
No. de Actividad:	1.2	Investigación	Investigación de Noticias de Ataques de Red				
Unidad:	1: Riesgos de seguridad informática en infraestructura de red						
Carrera:	Tgo. en Desarrollo de Software						
Materia	Seguridad en ITI					Clave	MPF3608DSO
Profesor:	Andrés Figueroa Flores						
Alumno:	David Alejandro López Torres					Registro:	17300155
Institución:	Centro de Enseñanza Técnica Industrial plantel Colomos						
Semestre:	8	Grupo:	D1	Período:	Feb-Jun 2021	Fecha:	11/02/2021
Compet. Genéricas		4.1, 4.5, 5.2, 5.5		Compet. Profesional		CP1-1	

## 1. Objetivo(s) de la actividad

- Identificar información relevante en los ataques informáticos

## 2. Instrucciones (Descripción) de la actividad

- 1- Investigar noticias relacionadas con ataques a redes informáticas.
- 2- Identificar en cada noticia, el tipo de ataque, quien realizó el ataque y quien fue atacado.
- 3- Usando el archivo de machote de actividades, para realizar esta actividad.
- 4- Subir el archivo terminado y dar clic para marcar como entregada la actividad.

## 3. Desarrollo de la actividad

### Nota 1:

### Uber ocultó que sufrió un hackeo masivo que afectó a 57 millones de usuarios

*Uber fue víctima de un hackeo masivo y llevaba un año ocultándolo.*

En un comunicado, el consejero delegado de la compañía, Dara Khosrowshahi, quien asumió el cargo en agosto, desveló el incidente y cómo ocurrió, aunque no precisó por qué la firma decidió esconder que había pasado.

Según su relato, dos individuos externos a la compañía accedieron a los datos almacenados por Uber y descargaron información de 57 millones de usuarios, entre ellos, 600.000 conductores en Estados Unidos.

Los hackers obtuvieron los nombres y los números de licencia de los conductores y los nombres, correos y números de celular de las personas que utilizaron el servicio, de todas partes del mundo.

La compañía asegura, no obstante, que sus expertos "no vieron ninguna indicación" de que se descargaran números de tarjeta de crédito, cuentas bancarias, números de la seguridad social, historiales de viajes o fechas de nacimiento.

Uber pagó a los hackers US\$100.000 para que borrasen la información robada, publicó Bloomberg, el primer medio en desvelar lo ocurrido.

Según esta fuente, el anterior consejero delegado Travis Kalanick supo del robo hace alrededor de un año.

En el momento que ocurrió el robo, Uber dio pasos para proteger sus datos y cerrar el acceso a los hackers.

"Identificamos posteriormente a los individuos y obtuvimos garantías de que la información descargada se había eliminado", precisa el comunicado, sin dar más detalles.

Uber ha creado ahora una página para atender a los conductores afectados y asegura que establecerá un sistema de protección de la identidad para sus conductores sin coste alguno. El comunicado no especifica si tomarán medidas similares con los clientes.

"Se preguntarán por qué estamos hablando de esto ahora, un año después. Yo tuve la misma pregunta, así que inmediatamente pedí una profunda investigación de lo que ocurrió y cómo lo gestionamos", afirmó el consejero delegado.

De momento, la empresa ha despedido a dos de las personas -cuyas identidades no especificó- que dirigieron la respuesta al incidente.

"Nada de esto tenía que haber pasado, y no daré excusas. Pese a que no puedo eliminar el pasado, puedo comprometerme en nombre de todos los empleados de Uber de que aprenderemos de nuestros errores", subrayó Dara Khosrowshahi.

La empresa debía haber comunicado el incidente a las autoridades competentes, pero no lo hizo hasta ahora y no es la primera vez que esconde una situación similar.

En enero, fue multada con US\$20.000 por no informar sobre un robo similar -aunque menor- ocurrido en 2014.

El hackeo y sobre todo la ocultación del mismo se suma a otros escándalos que han sacudido a la empresa en tiempos recientes y en cuyo centro se encontraba el anterior consejero delegado, Travis Kalanick, quien dimitió a mediados de este año entre presiones de los inversores.

Las denuncias de acoso sexual realizadas en la empresa realizadas una exempleada en febrero de este año marcó el inicio de la crisis que vive la startup, según señaló el reportero de tecnología de la BBC Dave Lee.

A ello se sumaron posteriormente otras polémicas como un video en el que Kalanick le hablaba de manera despectiva a un conductor.

Pese a su salida como consejero delegado, Kalanick aún mantiene poder de decisión como cofundador de la empresa, pues continúa en la junta directiva.

## **Nota 2:**

### **'Immense' network assault takes down Yahoo**

*February 8, 2000*

*Web posted at: 4:35 p.m. EST (2135 GMT)*

*by Martyn Williams*

(IDG) -- In what company officials are describing as a "fast" and "intense" assault on its network, U.S.-based Web sites of Yahoo Inc. and some of its companion sites were unreachable for about three hours Monday.

"At 10:30 a.m. (Pacific Standard Time), it appears a Yahoo router experienced a distributed denial-of-service attack," a Yahoo spokesperson said on condition of anonymity. "We believe it was coordinated, coming from multiple points on the Internet."

It hit not only the main U.S. Yahoo site but also some companion sites, such as Yahoo Mail and the Yahoo-owned GeoCities Web site.

A denial-of-service attack doesn't involve breaking into the target Web site but simply overloading it -- or in this case the router connecting it to the rest of the Internet -- with so much fake traffic that it becomes unable to cope. Once this is achieved and the site is overloaded, genuine users find themselves unable to get connections. The distributed denial-of-service attack generates traffic from multiple points on the Internet.

The amount of data hitting the router took engineers at Yahoo by surprise.

"This was so fast and so intense that we couldn't even redirect our traffic," the spokesperson said. It was not until three hours later, at 1:30 p.m. PST, that the company began restoring access to most of its sites through the use of filters that removed most of the hostile traffic before it had a chance to hit the router.

"From what I gather from the engineers, this was immense," said Secret Fenton, a spokeswoman for Global Center Inc., the company that hosts Yahoo's Web sites. "Nobody has ever seen one like this before. It was truly huge."

The outage, coming as it did in the middle of the U.S. business day, is likely to have affected millions of users. Together, Yahoo's family of Web sites attracted 42.4 million unique visitors in December 1999, according to Web audience measurement firm Media Metrix Inc. This made it the second most popular Web family on the Internet after those of America Online Inc.

The Yahoo spokesperson was keen to emphasize that no user data was compromised during the attack and that its Web sites and systems were at no time hacked.

Engineers at both Yahoo and Global Center are investigating the incident, and Fenton added that the companies aren't fully certain it was an attack, although at this stage in their investigation, all evidence points toward a distributed denial-of-service attack.

A denial-of-service attack took down the Web site of the FBI last May in one of last year's best-known Internet attacks.

*(Al indagar sobre los eventos redactados en la nota se encontraron diferentes artículos que describen con mayor profundidad los detalles del ataque y del responsable de este. Entre estos artículos se tomó el publicado por Juan Manuel Harán en el portal de “We live security” de ESET).*

Nombre de la noticia	Periódico que la emitió	Tipo de Ataque	Quién realizó el ataque	Quién fue atacado
“Uber ocultó que sufrió un hackeo masivo que afectó a 57 millones de usuarios”	BBC News	Spyware, ya que se filtró información de 57 millones de usuarios de Uber sin el consentimiento del administrador de la base de datos	Dos personas externas a la empresa que fueron posteriormente identificadas por Uber	La empresa de Uber al pagar \$100,000 USD a los hackers y a la privacidad de 57 millones de usuarios
“ 'Immense' network assault takes down Yahoo”	CNN News	DoS (Denegación de Servicios), ya que una sobrecarga de solicitudes dejó sin servicio a Yahoo! por más de 3 horas.	Michael Calce, conocido como “MafiaBoy” a sus 15 años	Yahoo!, Fifa.com, Amazon.com, Dell, Inc., E*TRADE, eBay, y CNN

#### 4. Reflexión:

A pesar de los agigantados pasos que da la tecnología en nuestros tiempos, es claro que la vulnerabilidad de la información y del software se vuelve cada vez más presente. La diversidad de ataques históricos que se han efectuado nos revela la importancia de la seguridad en las redes de grandes empresas. Resultante impactante notar la “simpleza” con la que algunos de estos ataques se han llevado a cabo, como es el caso del ataque de MafiaBoy que a su corta edad fue capaz de poner en la cuerda floja a empresas de calibre mundial.

## 5. Referencias:

Mundo, BBC (2017, noviembre 21). Uber ocultó que sufrió un hackeo masivo que afectó a 57 millones de usuarios. BBC News. Recuperado desde:

<https://www.bbc.com/mundo/noticias-42075627>

Williams, M (2000, February 8). 'Immense' network assault takes down Yahoo. CNN News. Retrieved from:

<https://edition.cnn.com/2000/TECH/computing/02/08/yahoo.assault.idg/index.html>

Harán, J. M. (2020, febrero 10). MafiaBoy: 20 años de uno de los primeros ataques documentados del tipo DoS. We Live Security by ESET. Recuperado desde:

<https://www.welivesecurity.com/la-es/2020/02/10/mafia-boy-20-anos-primeros-ataques-denegacion-servicio/>