2017

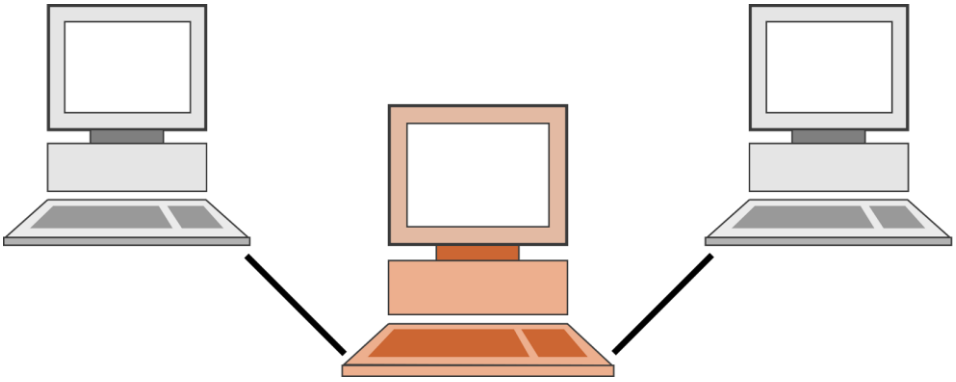
Cómo actúan los piratas informáticos

BELINDA GONZÁLEZ HARO
JAIME FRÍAS FUNES
JOSÉ LUIS LÓPEZ SÁNCHEZ

Cómo se ocultan

Conectarnos a través de un proxy.

En internet tu identidad es tu IP, en el momento que pones un servidor proxy por medio es su IP la que sale al mundo para darte las páginas que solicitas. Aunque el servidor final desconozca tu IP el proxy podría guardar una relación entre tu IP y lo que has visitado. Para resolver este problema existen dos vías.



La primera es utilizar proxies que sean "anónimos". Los más cautelosos incluso utilizan varios **proxies encadenados**, y cuando decimos varios, nos referimos a 10 o 12 y además ubicados en distintos países. Con que solo 1 de la cadena no tenga el log el rastreo será imposible.

La otra vía consiste en acceder al PC de un usuario, ya sea buscando un fallo de seguridad o aplicando técnicas de ingeniería social e instalar un servidor proxy en su ordenador sin que el usuario tenga constancia. De este modo el cracker utilizar a su víctima como servidor proxy y todo lo que haga lo hará desde la IP pública de su víctima.

Conectarnos a través de una VPN

Una conexión VPN es, a grandes rasgos, similar a la de un Proxy, con la diferencia de que **el tráfico entre nosotros y el servidor VPN se cifra**, evitando dejar el más mínimo rastro de él por la red. Existen muchos servidores VPN diferentes, y cada uno se avala por unas leyes, por lo que, si de verdad queremos ocultar nuestra identidad, debemos leer detenidamente los términos del servicio que utilizamos.
A continuación, os dejamos algunos de los servidores recomendados para este 2017.

Reenviar nuestro tráfico a través de la red Tor

Tor es una red que implementa una técnica llamada **Onion Routing**, diseñada con vistas a proteger las comunicaciones en la Marina de los Estados Unidos. La ideas es cambiar el modo de enrutado tradicional de Internet para garantizar el anonimato y privacidad de los datos.

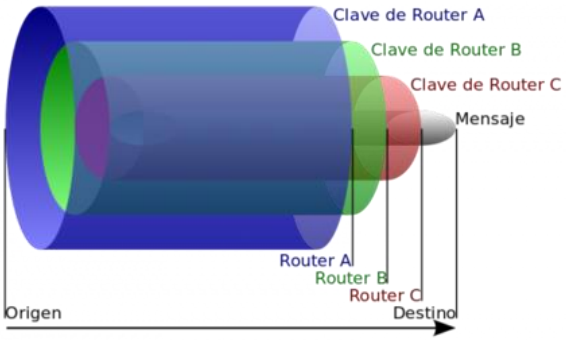
El enrutado tradicional que usamos para conectarnos a servidores en Internet es **directo**. Por ejemplo, si quieres entrar en Google: tu ordenador se conecta de forma directa a los servidores de Google. La ruta es, a grandes rasgos, sencilla: de tu ordenador a tu router, de ahí a los enrutadores de tu ISP (proveedor de Internet) y después directos a los servidores de Google.

Fácil y sencillo, salvo por el hecho de que si alguien intercepta los paquetes de datos en un punto intermedio **sabrá perfectamente de dónde vienen y a dónde van**. Incluso aunque se cifren los datos de cada paquete (por ejemplo, visitando una página HTTPS) las cabeceras de este no se cifran, y los campos del remitente y destinatario (entre otros) siguen siendo visibles.

Ahí es donde entra el Onion Routing. Habréis oído que consiste en **enviar el paquete por un camino no directo**, a través de varios nodos, pero en realidad es algo más complejo que eso.

Primero, el ordenador A, que quiere enviar el mensaje a B, calcula una ruta más o menos aleatoria al destino **pasando por varios nodos intermedios**. Después, consigue las claves públicas de todos ellos usando un directorio de nodos.

Usando cifrado asimétrico, el ordenador A **cifra el mensaje como una cebolla: por capas**. Primero cifrará el mensaje con la clave pública del último nodo de la ruta, para que sólo él lo pueda descifrar. Además del mensaje, incluye (también cifradas) instrucciones para llegar al destino, B. Todo este paquete, junto con las instrucciones para llegar al último nodo de la lista, se cifra de nuevo para que sólo lo pueda descifrar el penúltimo nodo de la ruta.



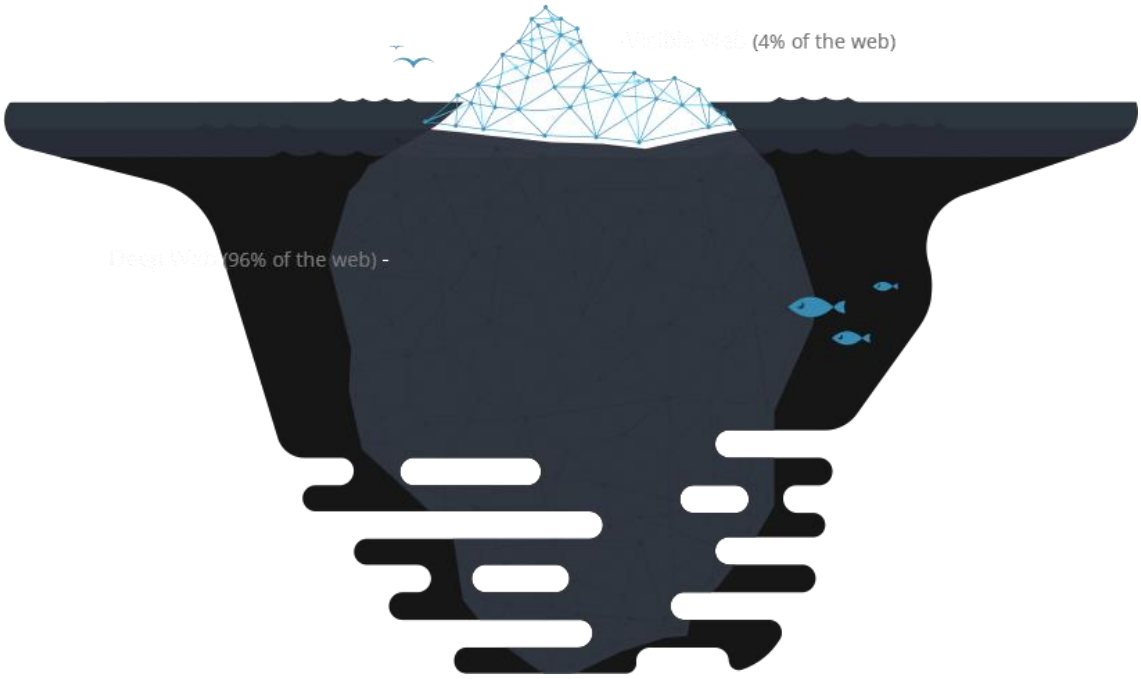
El paquete está en el centro, protegido por varias capas (cifrados) para cada uno de los nodos.

El proceso se repite hasta que acabamos con todos los nodos de la ruta. Con esto ya tenemos el paquete de datos listo, así que **toca enviarlo**. El ordenador A conecta con el primer nodo de la ruta, y le envía el paquete. Este nodo lo descifra, y sigue las instrucciones que ha descifrado para enviar el resto del paquete al nodo siguiente. Éste descifrará de nuevo y volverá a enviar al siguiente, y así sucesivamente. Los datos llegarán finalmente al nodo de salida, que enviará el mensaje a su destino.

Deep web

Características

- Posee entre **400 y 500 veces más información** que la Web normal
- Entorno al 95% de la web profunda es de **información accesible al público**, es decir, no hay que pagar nada por ella.
- Hay más de **200 mil millones de sitios web** asociados a la Deep Web
- La relación **contenido-calidad es de alrededor de un 1000%** respectod de la web superficial.
- Las páginas funcionan bajo **software que protege su identidad**, como puede ser TOR



Lo que hay:

- **Páginas de descargas pirata**, como los torrents y de descarga masiva
- **Foros Onion Chan**, portales de pornografía infantil, venta de objetos robados, tráfico de armas…
- **Sitios de extremistas**, grupos ilegales, etc.
- **Redes gubernamentales**, sitios web de acceso restringido, programas de espionaje…

Asegurar la privacidad

Aunque los 3 métodos anteriores funcionan, en realidad la seguridad no es del 100%. Por ello, si de verdad queremos evitar que nos identifiquen a través de la red, debemos poner en práctica una serie de configuraciones como, por ejemplo, conectarnos a través de una red Wi-Fi pública (un bar, una biblioteca, etc), utilizar un sistema operativo Live-USB, como, por ejemplo, Tails, del que hablará mi compañero a continuación, y utilizar herramientas para cambiar la MAC de nuestra tarjeta de red de manera que la MAC original quede suplantada y no se pueda identificar con ninguna conexión anterior.

TIPOS DE ATAQUES INFORMÁTICOS

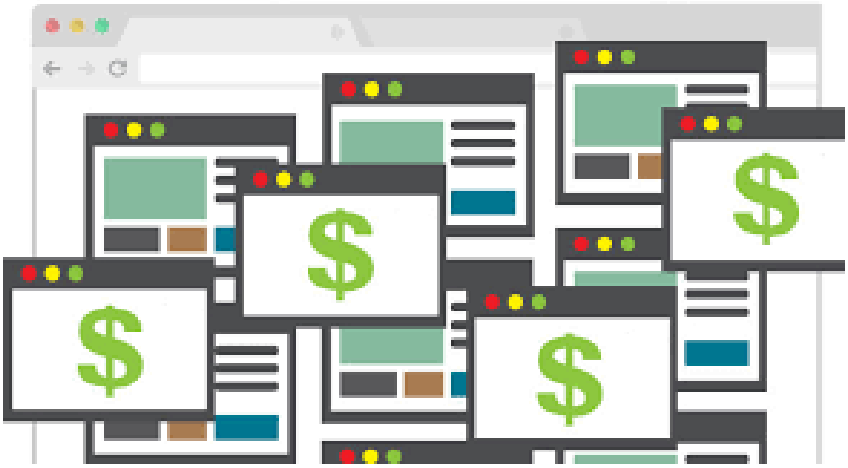
Algunos de los tipos de malware son:

Virus

Esta es la forma más conocida del malware, se diferencia de otros tipos de malware en que **su función comúnmente es únicamente causar daños en el Sistema Operativo**, deshabilitando funciones, ralentizándolo o, los más peligrosos, eliminando carpetas esenciales para el funcionamiento del Sistema Operativo, obligando a reinstalar el Sistema.
No se reproduce a sí mismo, por lo que **su forma de reproducirse es infectando archivos con su código**, por lo que conectar una USB o CD en un equipo infectado y reproducirlo en otro no infectado, provocará que el virus se propague hacia el equipo no infectado.

Adware

Es una forma de malware que se dedica a **mostrar publicidad intrusiva al usuario**, al no causar daño directamente al equipo, y al ser instalado “voluntariamente” (mediante engaños) por el usuario, no siempre es considerado malware.
Es bastante común encontrar Adware en los computadores, incluso más que los virus, ya que se propaga mediante instaladores de programas gratuitos que muestran “*programas recomendados*” o publicidad durante su instalación. Si el usuario acepta descargar uno de esos programas, voluntariamente estará infectando su equipo.
Otra razón por la que es común encontrarlo es porque no daña directamente al Sistema Operativo (por lo que no muchos usuarios no se esfuerzan en eliminarlo), pero puede ralentizarlo.



Gusanos

Son una clase de malware caracterizada por tener la capacidad de **replicarse a sí mismos**. Es decir, que si tu PC queda infectada con uno de estos, el malware se copiará a sí mismo y se enviará a otros equipos, en busca de más víctimas. Consecuencias de la presencia de gusanos en tu equipo son: consumo excesivo de banda ancha (por las veces en que el gusano se envía a otros equipos), aumento considerable de recursos como CPU o RAM (consumo causado por la necesidad del gusano de replicarse miles de veces).

Uno de los ejemplos más sonados en el 2000 fue “I love you”

I LOVE YOU

Este virus fue la primera infección masiva a nivel mundial que afectó a más de 50 millones de ordenadores conectados a Internet de al menos 20 países y las pérdidas superaron los 5000 millones de dólares. Instituciones como el Pentágono, la CIA o el Parlamento Británico padecieron las consecuencias. En España, el 80% de las empresas sufrieron los ataques de este virus.

En el años 2000, un estudiante de Filipinas, Onel de Guzmán fue el creador de este virus preparando una propuesta de tesis que desagradó profundamente a sus profesores.

“Esto es ilegal. No producimos ladrones.”

Se trataba de un virus de tipo gusano y escrito en VBScript. Se extendió rápidamente a través del correo electrónico enviándose como un archivo adjunto nombrado como "LOVE-LETTER-FOR-YOU.TXT.vbs". El fichero empleó una **doble extensión .TXT.vbs**, de forma que en los sistemas operativos que tenían activada la opción de "*Ocultar las extensiones de archivo para tipos de archivo conocidos*" apareciera como un simple fichero de texto.

El mecanismo que empleaba ILoveYou para infectar el equipo y propagarse era el siguiente:

1. Cuando un usuario abría el archivo del gusano, el código malicioso **accedía a la libreta de direcciones** y enviaba una copia de sí mismo.
2. Luego, el virus se copiaba en distintos tipos de archivos, eliminando su contenido anterior. Por ejemplo, reemplazaba todos los archivos *.jpg, *.JPEG, *.VBS, *.VBE, *.JS, *.JSE, *.CSS, *.WSH, *.SCT, *.HTA con copias de los mismos en las que escribía su código y a las que añadía la extensión .VBS. Lo mismo hacía con ficheros *.MP3 y *.MP2. Además, **robaba información de la víctima** que enviaba a varias direcciones de correo electrónico. También infectaba archivos en unidades de red mapeadas y era capaz de enviarse a los usuarios que se unían a una sala de chat en las que había un miembro infectado.
3. Por último, el virus intentaba comunicarse con alguno de los cuatro sitios Web en Filipinas que tenían preparado para su descarga el archivo llamado WIN-BUGSFIX.exe. Estos sitios **dejaron de estar *online*** al día siguiente de la infección masiva.

Ransomware

Es un tipo de malware que “secuestra” tu computadora, ya que **cifra tu disco duro**, encargándose que no puedas acceder a tus datos. Mientras tanto lo único que podrás ver será una pantalla mostrando un aviso falso de la policía, la NSA, CIA o cualquier otra institución gubernamental, donde se te solicitará un pago para liberar tu equipo.

WannaCry

¿Cómo funciona el ransomware WannaCry?

Este ransomware encripta ordenadores, apropiándose de sus archivos y datos, y posteriormente solicita al usuario del ordenador infectado un rescate a pagar en bitcoins para recuperar los archivos. Si bien programas de este tipo se han convertido en una amenaza bastante común, WannaCry se está distinguiendo por una capacidad de propagación inédita.

No se puede ver los archivos infectados porque se quedan encriptados y se bloquea el acceso a los mismos. Para poder tener la información de vuelta, tal y como estaba anteriormente, el virus solicita el ingreso de un número de bitcoins (moneda de Internet) a cambio. Por ejemplo, a los equipos infectados de la compañía española Telefónica les pedían 300 bitcoins para poder recuperar los archivos atacados, que poseían información de carácter confidencial.

Ha afectado ya a 74 países, en España el más sonado ha sido recientemente el de Telefónica, empresa que ha reconocido ser afectada por él.

Otros casos han sido: al servicio de hospitales británicos, a la multinacional francesa Renault, el sistema bancario ruso y al grupo de mensajería estadounidense FedEx, así como al servicio de ferrocarriles alemán y a universidades en Grecia e Italia.

Este ha afectado a todo tipo de sistemas operativos tales como Linux, Windows... Pero los casos más sonados han sido debido por fallos del sistema Microsoft Windows, que en su versiones recientes, desde XP en adelante (todas las que se lanzaron de 2009 en adelante: Windows Vista, Windows 10, etc.) ha permitido a WannaCry entrar en los sistemas informáticos si las versiones no estaban convenientemente actualizadas. Muchísimos equipos del mundo trabajan con estos sistemas, de ahí que la invasión del virus haya sido de tal calado y se ha haya extendido tan rápidamente.

Otro de los problemas adicionales que plantea este ransomware en concreto es que no solo afecta a los datos locales, **sino que además se propaga por la red**, cifrando los formatos de fichero más populares para acabar "destruyendo" el acceso a datos compartidos en una intranet sin que los usuarios puedan hacer mucho por evitarlo.

Rogueware

Intenta pasar por software auténtico, utilizando nombres genéricos como “Antivirus 2014 Pro” o similares para llamar la atención de los usuarios con pocos conocimientos. Es muy frecuente ver ejemplos de rogueware en publicidad de sitios de descargas, en otras ocasiones, pueden aparecer como *pop-ups* que simulan ser un aviso del Sistema Operativo advirtiendo que se han encontrado amenazas dentro de tu equipo, y que con ese software falso podrías eliminarlo.
Una vez instalado el rogueware, **se dedica a distribuir malware** por todo el equipo.

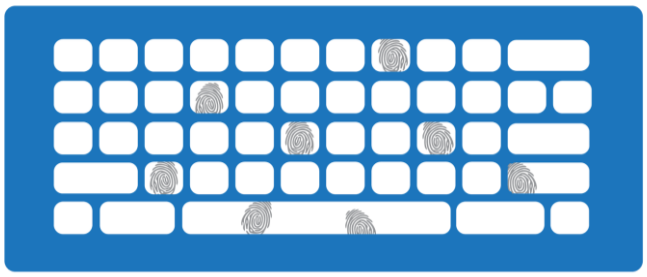
Spyware

Es el malware dedicado a recopilar información del usuario a sus espaldas, enviándola a destinos desconocidos, comúnmente agencias de publicidad.

Actualmente es común encontrarlo dentro de otro tipo de malware, normalmente Adware, que mediante los buscadores y programas falsos instalados puede recopilar información del usuario. Un tipo de spyware muy utilizado son los keyloggers, que se dedican a registrar cada pulsación ocurrida en el teclado. También existen variables capaces de grabar vídeo y tomar fotos por la webcam, o capaces de registrar el historial del navegador.

KEYLOGGER

- Herramienta para registrar las pulsaciones del teclado en un equipo.
- Roban gran volumen de información sin que la víctima se percate de ello.
- Los keylogger con software suelen formar parte de malware mayores.
- Los keylogger con hardware, por el contrario, necesitan que el atacante acceda físicamente al ordenador (más difíciles de detectar).



¿Cómo defenderse?

- Son difíciles de detectar.
  - No son como otros programas maliciosos.
  - No buscan información de valor.
  - No destruyen información.
- Permanecen ocultos y pasan desapercibidos.
- Se pueden evitar arrancando el sistema desde un CD o USB o usando un teclado virtual, que evite que el malware reciba las pulsaciones del teclado.

Cross-Site Scripting (XSS)

A menudo mal entendido, y aún más a menudo subestimada, XSS es un estilo de ataque en el que la parte delantera de la página web actúa como un punto de lanzamiento para ataques a otros usuarios que visitan el sitio web. Esto sucede cuando los desarrolladores no prueban correctamente su código para posibilidad de permitir scripts de ser inyectados. Los scripts pueden ser ejecutados sin funcionalidad original del sitio de la intención que sean.

Si una vulnerabilidad XSS está presente en un sitio web, entonces un atacante puede crear código que se ejecuta cuando otros usuarios abren el mismo sitio web. Esto hace que los nuevos usuarios interactúen con la entidad fondo malicioso creado por el atacante. Una vez que una conexión se ha iniciado, por lo general a través de tácticas de ingeniería social para convencer a un usuario a hacer algo que no debe, el atacante es capaz de infiltrarse en las computadoras de sus visitantes del sitio web.