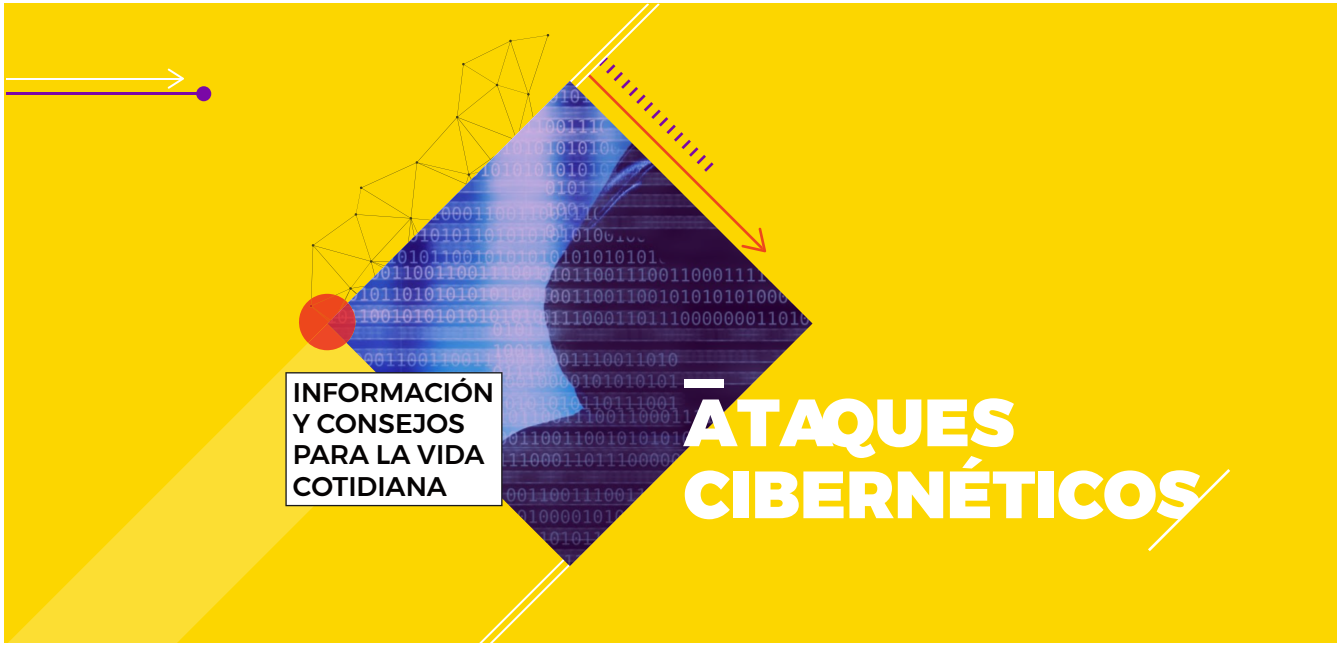
BA CSIRT
Vamos Buenos Aires | Centro de Ciberseguridad
Agencia de Sistemas

www.ba-csirt.gob.ar

BOLETÍN
N°46
FECHA DE PUBLICACIÓN
31 | 10 | 18



CIBERATAQUES:
LAS ESTRATEGIAS DELICTIVAS DEL MUNDO DIGITAL

"Slammer infectó una planta nuclear en Ohio y colapsó la red de cajeros automáticos del Bank of America; Blaster paralizó los trenes en las vías a las afueras de la ciudad de Washington y cerró los sistemas de facturación de Air Canada de los aeropuertos canadienses; Sasser infectó todos los sistemas de varios hospitales en Europa."

-Mikko Hypponen.

En varias oportunidades, dentro de muchos de los materiales que publicamos, hablamos o hacemos referencia al concepto de "ataques informáticos" o "ciberataques" y, si bien ambos nombres resultan bastante intuitivos en su significación, desde **BA-CSIRT** creemos conveniente profundizar en la explicación de los mismos, dado que constituyen uno de los elementos principales que vuelven necesaria la Seguridad Informática.

Entonces, empecemos por la definición: **¿Qué son exactamente los ataques informáticos?**

Son acciones deliberadas, llevadas adelante por ciberdelincuentes organizados o personas que no necesariamente se dedican al cibercrimen pero tienen la intención de provocar daños en sistemas, redes y/o dispositivos informáticos de terceros, con múltiples propósitos.

Tal como explica Emmanuel Millán, doctor en Ciencias de la Computación y docente de la carrera de Redes y Telecomunicaciones, en una nota realizada por el Instituto Universitario de UNCUYO, "***hay distintos objetivos a la hora de efectuar un ciberataque: puede ser por diversión, para obtener información o para bloquear un servicio***. *Generalmente se trata de ataques momentáneos que pueden durar minutos u horas. Sin embargo, para algunos servicios, como Amazon, una caída de una hora significa pérdidas enormes, ya que son ventas que no se están haciendo*"[1].

Otros ejemplos interesantes, los aporta el investigador finlandés Mikko Hypponen en su artículo Ciberataques, al referirse a casos de infecciones por virus que se dieron durante el año 2003: "*Slammer infectó una*

planta nuclear en Ohio y colapsó la red de cajeros automáticos del Bank of America; Blaster paralizó los trenes en las vías a las afueras de la ciudad de Washington y cerró los sistemas de facturación de Air Canada de los aeropuertos canadienses; Sasser infectó todos los sistemas de varios hospitales en Europa."[2]

Como vemos, las motivaciones de los responsables pueden ser muchas y de mayor o menor magnitud en virtud de sus consecuencias. Sin embargo, **todos los ataques informáticos causan daño y alteran, en uno o más sentidos, el curso normal de las actividades y ocupaciones de los afectados**. En tal sentido, Hypponen afirma: "*Si se quiere seguir el ritmo de los ciberdelincuentes, la clave está en la cooperación.*"[3]

En algunos casos los exploits pueden resultar útiles. Por ejemplo, las pruebas de intrusión autorizadas que se realizan con herramientas como Metasploit pueden incrementar la seguridad de una organización. A esa clase de prácticas se las denomina Hacking Ético.

Es por ello que resulta importante conocer, al menos a grandes rasgos, **cuáles son los tipos de ataques informáticos más comunes y cómo funcionan**. Para analizarlos, los dividiremos en cuatro grandes categorías: Infecciones por malware, Denegaciones de servicio, Ejecución de expolits e Ingeniería social.

Así, cuando hablamos de **Infecciones por malware** nos referimos a lo que comúnmente se conoce como "infecciones por virus". Es decir, sea por hacer clic en algún enlace inseguro o navegar por sitios "peligrosos", descargar adjuntos infectados, conectarse a alguna red WiFi vulnerada, conectar unidades de memoria externa infectadas a los dispositivos o cualquiera otra acción similar, el dispositivo resulta infectado por alguno de las tantas variedades de software maliciosos existentes. Estos varían de acuerdo al daño que generan o su modo de funcionamiento. Los más frecuentes son:

Algunos malware infectan los dispositivos con el objetivo de tomar control de los mismos y hacerlos funcionar en redes "botnets".

- **Virus.** El virus permanece inactivo hasta que un usuario lo ejecuta; cuando ello sucede, comienza a infectar los archivos extendiéndose por todo el equipo.
- **Worms (gusanos).** El objetivo de los gusanos informáticos es infectar los archivos del equipo para propagarse. Tienen la capacidad de extenderse a otros equipos sin necesidad de que un usuario los ejecute.
- **Troyanos.** Los troyanos muestran la apariencia de un programa fiable, pero esconden otro tipo de malware que es instalado automáticamente cuando el programa "confiable" se ejecuta, con el objetivo de tomar el control del equipo.
- **Keyloggers.** Son capaces de registrar todas las pulsaciones del teclado. Esta información es utilizada para conseguir contraseñas y datos de la víctima.
- **Spyware.** El objetivo principal de este malware es el robo de información.
- **Adware.** El adware se encarga de mostrar publicidad al usuario a través de banners, pop-ups, nuevas ventanas en el explorador... En muchos casos, el objetivo secundario también

Es importante tomar precauciones con la privacidad de nuestras cuentas y el uso que hacemos de ellas ya que a pesar de que no tengamos nada que ocultar, todos nuestros datos son nuestros. Nadie tiene el derecho de acceder a ellos sin nuestro consentimiento.

es obtener información sobre la actividad del usuario en la red.

- **Ransomware.** Es el tipo de ataque más común en la actualidad. Se basa en el cifrado de los datos, restringiendo el acceso a los archivos del equipo para pedir un pago por el rescate de los mismos. Es decir, se trata de un secuestro de información. En la mayoría de los casos, el pago se solicita en bitcoins.[4]

En lo que respecta a los ataques de **Denegación de Servicio (DDoS)**, consisten en generar una enorme cantidad de tráfico desde numerosos dispositivos a un sitio web determinado. Como consecuencia del gran aumento de tráfico, el rendimiento de la red disminuye hasta el punto en que se satura y, de ese modo, se interrumpe su funcionamiento normal.

Un buen ejemplo de un ataque de DDoS, fue el que se llevó adelante el 21 de octubre de 2016 contra la empresa Dyn DNS. Dicho ataque generó la caída, durante varias horas, de servicios internacionalmente conocidos como: Airbnb, Amazon Web Services, Boston.com, Box, FreshBooks, GitHub, GoodData, Heroku, Netflix, The New York Times, PayPal, Reddit, Shopify, Spotify, Twitter, Vox y Zendesk.

Lo más curioso del caso fue que, contrario a lo que podríamos pensar, el dispositivo o aparato que disparó el ataque no fue la súper computadora de un genio de la informática; en absoluto. En esa oportunidad, se utilizaron miles de dispositivos que fueron previamente infectados con un malware del tipo "gusano", específicamente diseñado para hacer que estos funcionen como zombies. Ello significa que los dispositivos infectados pasaron a funcionar como robots (denominados 'bots' en el ambiente informático) que actuaban bajo las órdenes de los cibercriminales responsables del ataque. Y lo más increíble es que todo ocurrió sin que los dueños de tales equipos tuvieran conocimiento alguno de lo que estaba sucediendo y de los fines con los que sus dispositivos estaban siendo utilizados.

Por otra parte, la **Ejecución de exploits** no es ni más ni menos que el aprovechamiento de vulnerabilidades de programación para dañar sistemas y/o archivos o acceder a ellos. Tal como explica Hypponen, "*de acuerdo con los efectos que tengan en los sistemas objeto de ataque, los tipos de vulnerabilidad pueden dividirse en denegación de servicio, elevación de privilegios o ejecución de código. La denegación de servicio permite al agresor ralentizar o cerrar el sistema. La elevación de privilegios puede utilizarse para obtener permisos adicionales en un sistema. La ejecución de código permite la ejecución de comandos. Las vulnerabilidades más graves son las de ejecución de código remoto. Y son estas las que necesitan los agresores.*"[5]

No obstante lo que acabamos de decir, es importante aclarar que "*en algunos casos los exploits pueden resultar útiles. Por ejemplo, las pruebas de intrusión autorizadas que se realizan con herramientas como Metasploit pueden incrementar la seguridad de una organización.*"[6] A esa clase de prácticas se las denomina **Hacking Ético**.

Un estudio de McKinsey revela que más del 80% de los breaches [filtraciones de datos] son por contraseñas débiles o robadas y que casi el 90% de los manager senior admiten compartir datos por error.

Uno de los ransomware más famosos, que afectó a más de 100 países durante el 2017 fue el WannaCry.

Finalmente, la **Ingeniería Social** es un conjunto de técnicas que se basan en el aprovechamiento de los errores y/o faltas de atención y precaución de los usuarios para acceder a información confidencial, privada de los mismos y luego, poder utilizarla a conveniencia. El caso más típico que se enmarca en esta categoría es el phishimg, que se realiza por correo electrónico.

Hasta aquí, todas las definiciones. Ahora bien, **¿qué dicen los expertos en relación a este tema?** Sebastián Stranieri, CEO de la firma VU Security, explica:

"Según el Reporte Regional de Amenazas Avanzadas en América Latina realizado en base al primer semestre de 2017, los ciberataques más comunes son el malware y el phishing, que busca engañar al usuario haciéndose pasar por una entidad confiable y conocida para robar datos los números de tarjetas de crédito o contraseñas.

El estudio, llevado a cabo en 14 países latinoamericanos, revela que **al menos un 20% del total de ciberataques son tipo malware**. Los más afectados por este tipo de ataque son Panamá (50,3%), Colombia (46,7%), Venezuela (46,1%), Ecuador (45,6%), México y República Dominicana (ambos con 45,3%), seguidos por Honduras (43%), Paraguay (42,9%), Costa Rica (42,4%) y Perú (39,9%). **La Argentina, con 31,2% se encuentra entre los tres menos afectados, junto a Chile y Uruguay**.

Por otro lado, el phishing sólo alcanza un máximo de 20% del total de ciberataques, en Ecuador (20,9%), para luego descender a 16,6% en Perú. Le siguen México (16,1%), **Argentina (15,9%)**, Costa Rica (15,1%), Uruguay (14,8%), Chile (14,6%), Paraguay (14,3%) y Guatemala (13,9%). Los menos afectados son Colombia, República Dominicana (ambos 12,6%), Venezuela (12,2%) y Honduras (6,5%).

El ransomware, un programa que "toma de rehén" información hasta recibir el pago del rescate, **afectó más de 500 millones de dispositivos móviles en el continente, mientras más de 50 millones de usuarios en Latinoamérica han sufrido robos de datos que forman parte de su identidad digital**.

Un estudio de McKinsey afirma, no sin razón, que las amenazas cibernéticas son un riesgo material para los negocios, dado el gran impacto de estos ataques: se estima que el costo promedio por cada data breach [violación de datos] es de 4 millones de dólares. El informe también revela que más del 80% de los breaches [filtraciones de datos] **son por contraseñas débiles o robadas** y que casi el 90% de los manager senior admiten compartir datos por error.

Además, **cada día se crean y distribuyen más de 300 mil nuevos malware**, por lo que el alcance es cada vez mayor, especialmente si se tiene en cuenta que, en los últimos años, hay cada vez más aparatos

Los keyloggers son un tipo particular de malware que registra las pulsaciones del teclado y, de ese modo, permite robar credenciales de acceso y diferentes datos sensibles.

conectados a Internet. Y no sólo tablets o celulares, sino también dispositivos como marcapasos y equipos de seguridad, como cámaras de vigilancia para bebés. En estos casos, los riesgos tienen que ver con la vulnerabilidad del software y la inseguridad de los modelos de conexión remota.

Cómo prevenir los ciberataques:

Para hacerle frente a estos ataques, es necesario considerar que, por un lado, son un negocio; lo que significa que detrás de ellos existe una organización que busca financiarse y, por otro lado, siguen sucediendo porque las compañías y los ciudadanos no actualizan sus dispositivos a la última versión del sistema operativo.

Sin embargo, esto a veces puede no ser suficiente. Las amenazas pueden ser filtradas a través de accesos VPN o redes privadas virtuales. Se pueden agregar sistemas de segundo factor de autenticación como tokens móviles o reconocimiento de rostro y/o voz que ayudan a robustecer los accesos y prevenir los fraudes, junto con software de análisis de comportamiento para alertar y prevenir posibles ataques antes de que sucedan.

Desde VU anticipamos que en los próximos años crecerá la suplantación de identidad, los ataques a sitios web y el fraude contra billeteras de criptomonedas. Estos son algunos consejos para evitar, como usuario, ser víctima de ciberataques:

- Navegar desde una red segura a la hora de introducir datos de pago, preferentemente redes cerradas y evitando redes de WiFi públicas como las de bares, plazas o medios de transporte.
- Evitar hace clic en links que lleguen por email, SMS o redes sociales, ya que pueden conducir a sitios fraudulentos.
- Dudar de las promociones con precios demasiado bajos y comprobar la posibilidad de devolución, ya que la existencia de esta política es una señal de confianza. También, investigar la reputación del vendedor y sus ventas anteriores.
- A la hora de realizar un pago, chequear que la dirección web en el navegador comience con “https://” o bien, que la barra esté marcada con verde, ya que indica que está en una conexión privada y segura.
- Chequear los resúmenes del banco para llevar un registro de los gastos y comparar con las compras realizadas durante el mes.
- De ser posible, realizar compras a través de dispositivos móviles como celulares o tablets, dado que sus sistemas más cerrados permiten mayor nivel de seguridad.

En un mundo cada vez más hiperconectado, es muy importante tener presente que la seguridad digital es un asunto de todos por igual y empieza por cada uno de nosotros.” ▪

[1] http://www.unidiversidad.com.ar/ataques-informaticos-que-son-y-como-evitarlos
[2] https://www.bbvaopenmind.com/wp-content/uploads/2014/01/BBVA-OpenMind-libro-Cambio-19-ensayos-fundamentales-sobre-c%C3%B3mo-internet-est%C3%A1-cambiando-nuestras-vidas-Tecnolog%C3%ADa-Interent-Innovaci%C3%B3n.pdf (p. 110).
[3] Ib (p. 109).
[4] https://sicrom.com/blog/tipos-ataques-informaticos/
[5] https://www.bbvaopenmind.com/wp-content/uploads/2014/01/BBVA-OpenMind-libro-Cambio-19-ensayos-fundamentales-sobre-c%C3%B3mo-internet-est%C3%A1-cambiando-nuestras-vidas-Tecnolog%C3%ADa-Interent-Innovaci%C3%B3n.pdf (p. 116).
[6] Ib. (pp. 118-119).