**Amenazas informáticas que más impacto tuvieron durante el último trimestre**

Repasamos algunos incidentes de seguridad, así como descubrimientos de vulnerabilidades y campañas maliciosas que más impacto tuvieron durante el trimestre abril-junio de 2019

[**Luis Lubeck**](https://www.welivesecurity.com/la-es/author/luis-lubeck/)**17 Jul 2019 - 12:01PM**

Lo que sucede en el campo de la seguridad de la información no recibe tanta atención de los medios tradicionales, o al menos no en proporción a la cantidad de hallazgos, investigaciones y alertas que día a día surgen en distintas partes del mundo y que afectan a empresas y servicios que tienen un alcance global. Sin embargo, la realidad indica que el [cibercrimen es un problema que crece](https://www.welivesecurity.com/la-es/2019/07/16/cibercrimen-problema-empeora-exige-actuar-cuanto-antes/%22%20%5Ct%20%22_blank). En este sentido, informarse permite a las personas tomar dimensión de los problemas que diariamente forman parte de la seguridad y a partir de conocer diferentes casos y ejemplos, los usuarios puedan incorporar hábitos que les permitan prevenir ser víctimas de ataques similares en el futuro. Es por eso que a continuación, repasamos algunas noticias sobre amenazas informáticas e incidentes de seguridad que más impacto tuvieron durante trimestre abril-junio de 2019.

En sintonía con lo que se predijo para este año en nuestro [informe Tendencias 2019](https://www.welivesecurity.com/la-es/2018/12/18/tendencias-2019-ciberseguridad/), la fuga de información ha sido uno de los incidentes que más impacto tuvieron en la región. Casos como el de [Canva](https://www.welivesecurity.com/la-es/2019/05/27/filtraron-datos-privados-millones-usuarios-canva/%22%20%5Ct%20%22_blank), en el que se filtraron datos privados de más de 100 millones de usuarios luego de que atacantes se aprovecharan de un fallo de seguridad en la popular plataforma, fue de los que más impacto tuvieron; al menos desde el punto de vista cuantitativo.

La invasión a la privacidad de los usuarios tuvo como protagonista durante el último trimestre un caso particular como fue el de La Liga Nacional de Fútbol profesional (LFP) de España y su aplicación oficial. El organismos propietario de los derechos del fútbol de España fue multado tras ser acusado de utilizar la app para [espiar a través del micrófono](https://www.welivesecurity.com/la-es/2019/06/11/multan-laliga-uso-app-espiar-microfono-movil/) de los dispositivos móviles de los usuarios con el objetivo de buscar transmisiones ilegales de los partidos.

En otro escenario que también forma parte de la seguridad, los ataques que buscan infectar a los usuarios con mineros de criptomonedas también estuvo presente en el último trimestre. En este sentido, la investigación de ESET sobre [Loudminer](https://www.welivesecurity.com/la-es/2019/06/24/loudminer-minero-multiplataforma-oculto-programas-vst-crackeados/%22%20%5Ct%20%22_blank) es un ejemplo de cómo han cambiado los tipos de ataque utilizados por los cibercriminales que buscan obtener rédito a través de criptomonedas en reemplazo del ransomware como forma de obtener beneficios económicos; algo que también se mencionó en el informe sobre tendencias en el campo de la seguridad para este 2019. El caso de Loudminer se trata de un **minero de criptomonedas persistente** que afecta a usuarios de macOS y Windows y que es **distribuido a través de copias piratas de programas VST y Estaciones de Audio Digital**, conocidas por sus siglas en inglés como DAW. Estos programas son utilizados para la producción de audio, por lo que se entiende que las computadoras que tengan instaladas estas aplicaciones VST cuentan con un buen poder de procesamiento. Entre los programas pirateados a través de los que se distribuía el minero son: Ableton Live, Sylenth1, Nexus, Reaktor 6 o AutoTune.

Otro hito importante del trimestre que acaba de pasar fue sin dudas el hallazgo de [BlueKeep](https://www.welivesecurity.com/la-es/2019/05/17/vulnerabilidad-critica-windows-podria-tener-consecuencias-similares-wannacry/%22%20%5Ct%20%22_blank), la vulnerabilidad que Microsoft reportó a mediados de mayo y que afecta a varios sistemas operativos de Windows anteriores a Windows 10. La particularidad de esta vulnerabilidad es que, según afirma la propia compañía, podría tener consecuencias similares a WannaCry debido a que las características del fallo permitirían a un malware propagarse hacia otros sistemas vulnerables. La preocupación llevó a la Microsoft a lanzar el 30 de mayo un segundo comunicado alertando a la comunidad de usuarios acerca de la importancia de actualizar sus sistemas operativos lo antes posible –se estima que existen casi un millón de equipos vulnerables a BlueKeep. Además, ya existen pruebas de concepto públicas en GitHub que demuestran que es posible explotar el fallo.

En lo que a explotación de vulnerabilidades se refiere, durante el último trimestre se conocieron reportes sobre el hallazgo de algunos fallos de seguridad explotables a nivel de hardware, tal como fue el caso de [ZombieLoad](https://www.welivesecurity.com/la-es/2019/05/16/zombieload-exploit-hace-vulnerables-ataque-procesadores-intel/%22%20%5Ct%20%22_blank) (vulnerabilidad descubierta en chips de Intel que permite extraer información sensible desde el procesador) o el hallazgo de una [vulnerabilidad en cámaras D-Link que permite espiar](https://www.welivesecurity.com/la-es/2019/05/02/vulnerabilidad-camaras-d-link-permite-atacante-espiar-transmisiones/) transmisiones. En cuanto a la explotación de vulnerabilidades a nivel de aplicaciones, los casos qué más visibilidad tuvieron fueron el de [WhatsApp](https://www.welivesecurity.com/la-es/2019/05/14/vulnerabilidad-whatsapp-permite-instalar-spyware-pegasus/) y la posibilidad de instalar el spyware Pegasus en dispositivos Android e iOS, y el de la vulnerabilidad crítica en [Firefox](https://www.welivesecurity.com/la-es/2019/06/19/vulnerabilidad-zero-day-critica-firefox/) que se descubrió estuvo siendo explotada en ataques dirigidos hacia propietarios de criptomonedas.

Los ataques que hacen uso de la ingeniería social siguen sumamente activos, principalmente aquellos que eligen plataformas como WhatsApp para distribuirse. En este período de tiempo reportamos distintas campañas de phishing que prometían, por ejemplo, [accesos a Spotify premium de forma gratuita](https://www.welivesecurity.com/la-es/2019/04/17/engano-promete-spotify-premium-gratis-whatsapp/), así como engaños más elaborados y que también hacían uso de la ingeniería social, pero que iban dirigidos a usuarios que habían sido [víctimas del robo de un iPhone](https://www.welivesecurity.com/la-es/2019/04/12/iphone-ha-sido-localizado-trampa-despues-robo/).

Por último, otro hallazgo relevante que salió a la luz durante el último trimestre fue el [descubrimiento de una serie de vulnerabilidades en el nuevo protocolo WPA3](https://www.welivesecurity.com/la-es/2019/04/12/fallo-protocolo-wpa3-permite-robar-contrasenas-redes-wi-fi/), que, en caso de ser explotadas, permitirían a un atacante obtener la contraseña de una red Wi-Fi e ingresar a la red. Si bien este descubrimiento parece alarmista, es importante tener presente que el hallazgo se dio en una etapa temprana de la implementación del nuevo protocolo WPA3.

Como para no dejar todo en alertas únicamente, ofrecemos algunas recomendaciones indispensables para evitar ser víctima de algunos de los ataques o vulnerabilidades que presentamos en este resumen:

* Mantener siempre actualizadas las versiones de las aplicaciones.
* Realizar las descargas desde los repositorios oficiales (AppStore o Google Play) o en su defecto de la página oficial y verificada de la empresa.
* Contar con soluciones robustas de seguridad para mantener monitoreada la actividad de los dispositivos en todas sus capas.
* Contar con soluciones de seguridad también en los dispositivos móviles.
* Verificar siempre dónde se ingresa la información de tipo personal o privada.
* Evitar acceder a enlaces que llegan a través de servicios de mensajería con ofertas o mensajes de dudosa procedencia.

La seguridad tiene un gran componente de soluciones tecnológicas, pero un factor fundamental es la constante capacitación por parte de los usuarios.