

Código malicioso en las redes sociales

En cuanto a seguridad en *smartphones*, a finales de mayo se descubrieron 26 aplicaciones con malware en el mercado oficial de Android. Dichas aplicaciones contenían una versión infectada de DroidDream, también conocido como “Droid Dream Light”.

Se estima que entre 30 y 120 mil usuarios fueron víctimas de la distribución de esta aplicación maliciosa. Dicho malware se encargaba de informar del IMEI, IMSI, modelo y versión SDK del móvil infectado, así como de todas las aplicaciones instaladas. Presumiblemente también era capaz de descargarse e iniciar la instalación de nuevas aplicaciones, aunque a diferencia de sus predecesores, necesitaba la intervención del usuario para completar el proceso.

En cuanto a Redes Sociales se refiere, **Facebook** fue en mayo uno de los principales objetivos de los ciberatacantes. El engaño del falso botón “No me gusta” de Facebook tenía como objetivo suscribir a los usuarios a un servicio Premium de SMS. En primer lugar, el usuario recibía un mensaje de un contacto invitándolo a descargar el supuesto nuevo botón.

Al acceder al enlace, se daba inicio al proceso de instalación, que en uno de sus pasos solicitaba la inclusión de un código, en JavaScript, que permitía que el mensaje continuara su propagación hacia los contactos de la víctima. Una vez concluido el procedimiento, se redirigía a la víctima a una página de suscripción de SMS, servicio del que luego era muy difícil solicitar la baja.

Más adelante, concretamente el 18 de mayo, se hizo público que Facebook había estado mostrando, accidentalmente, tokens de acceso a terceras partes, principalmente a anunciantes.

Este incidente ocurría a través de sus aplicaciones Web integradas en la plataforma Facebook.

Afortunadamente estas terceras partes desconocían que tenían acceso a dicha información. Estos *tokens* de acceso hubieran permitido acceder a perfiles, fotografías, chats y también ofrecían la posibilidad de escribir mensajes en muros públicos y modificar información personal.

Este hecho se descubrió a través de iframes que contenían *tokens* de acceso, y mediante los cuales las aplicaciones de acceso compartían datos con terceras partes, como anunciantes y plataformas de análisis de datos.

Por otra parte, un nuevo gusano se replicó por esta red social a través de un mensaje que instaba a la visualización de un vídeo sobre la ejecución de Osama Bin Laden. El código JavaScript del gusano está disponible en Pastebin. Finalmente, como nota positiva, el 12 de mayo Facebook anunciaba nuevas mejoras de seguridad en su plataforma para evitar sucesos de este tipo en un futuro.

En cuanto a intrusiones en grandes compañías, Sony sigue a la cabeza. En el proceso de resetear todas las contraseñas de los millones de cuentas comprometidas, se encontraron con nuevos problemas.

Hacktivismo

El término hacktivismo es el acrónimo resultante de las palabras “hacker” y “activismo”.

Debido a la situación social del pasado mes, se incluye esta sección en el informe para dar cobertura a las acciones de protesta online que se han desarrollado paralelamente. Aunque originariamente la definición de hacktivismo hace referencia a acciones “*ilegales o legalmente ambiguas*”, actualmente su ejecución se debe a grupos dispersos, difícilmente identificables, los cuales dentro de su activismo político desarrollan una mezcla de actividades, la mayoría de las veces legítimas y, puntualmente ilegales.





25. Observers note that Anonymous is becoming more and more sophisticated and could potentially hack into sensitive government, military, and corporate files. According to reports in February 2011, Anonymous demonstrated its ability to do just that. After WikiLeaks announced its plan of releasing information about a major bank, the US Chamber of Commerce and Bank of America reportedly hired the data intelligence company HBGary Federal to protect their servers and attack any adversaries of these institutions. In response, Anonymous hacked servers of HBGary Federal's sister company and hijacked the CEO's Twitter account. Today, the ad hoc international group of hackers and activists is said to have thousands of operatives and has no set rules or membership.[36] It remains to be seen how much time Anonymous has for pursuing such paths. The longer these attacks persist the more likely countermeasures will be developed, implemented, the groups will be infiltrated and perpetrators persecuted.[37]

De hecho, técnicamente hablando, muchos usuarios incurren en delitos al ayudar a difundir los numerosos *leaks* corporativos y gubernamentales que en estos últimos meses han sido tan frecuentes. Evidentemente en este apartado el conocido grupo **Anonymous**, del que se habló en el informe de Inteligencia de abril, brilla con luz propia.

Su amplia participación en el movimiento de protesta no se limitó a ayudar a difundir y coordinar las acciones desde el ciberespacio, sino que también pudo verse a numerosos miembros de Anonymous, además de a referencias a su iconografía, en las manifestaciones a pie de calle.

Así, el ya conocido tag “#spanishrevolution” que posteriormente fue complementado por “#europeanrevolution” y “#worldrevolution” debió su veloz difusión a la imagen que apareció en la Puerta del Sol de Madrid, la cual rápidamente se convirtió en portada de numerosos medios digitales.

Asimismo, la manifestación frente a la embajada española en Londres, que posteriormente fue seguida en otras capitales europeas, fue convocada a través de los perfiles de Twitter de este movimiento, el cual se encuentra en un momento álgido.

De ser un grupo disperso, pero limitado, está pasando a tener una gran cantidad de simpatizantes esporádicos, que ayudan a difundir sus mensajes.

De hecho en los perfiles de Facebook de personas afines a las protestas es cada vez más común encontrar iconografía de Anonymous.

No puede concluirse este apartado sin hacer referencia al informe publicado por la **OTAN** a finales de mes sobre el hacktivismo. Dicho documento constituye una auténtica declaración de intenciones acerca de esta actividad, y en varias ocasiones señala la necesidad de vigilar a Anonymous, aduciendo el riesgo de difusión de información clasificada. ●