WannaCry, ¿se podría haber evitado?

Instituto IMDEA Software
14 de mayo de 2017

- Las vulnerabilidades que explotan los cibercriminales son problemas de software.
- La mejor manera de evitar ataques es investigar para eliminar errores en el software.
- El Instituto IMDEA Software de la Comunidad de Madrid es referencia internacional en software y ciberseguridad.

El Viernes 12 de Mayo de 2017 será recordado en España como el día en el que Telefónica les pidió a los trabajadores de su central que apagaran sus ordenadores y se fueran a casa. La razón fue controlar la propagación del ransom-gusano WannaCry, el cual según diversas informaciones había cifrado los datos de centenares de ordenadores internos, dejándolos fuera de uso. Lo cierto es que WannaCry no afectó sólo a Telefónica sino que fue un ataque global que afectó a empresas y organizaciones de todo el mundo. Igualmente, la imagen de la gente saliendo antes de tiempo del Distrito C de Telefónica porque no podían trabajar sin sus ordenadores quedará para el recuerdo.

Ahora que el ataque empieza a ser controlado es importante pensar en qué se puede hacer para prevenir que se repita tanto a corto plazo como a largo plazo. A corto plazo porque es muy posible que en los próximos días veamos nuevos ataques que utilicen capacidades gusano para propagarse utilizando la misma vulnerabilidad, aunque es de esperar que su impacto sea mucho más limitado puesto que durante este fin de semana muchas organizaciones habrán aplicado los parches que arreglan la vulnerabilidad en Windows que WannaCry usaba para propagarse. A largo plazo porque la existencia de vulnerabilidades en programas informáticos, las cuales pueden permitir a un atacante hacerse con el control de un ordenador los datos que almacena, no son problemas que vayan a desaparecer de hoy a mañana.

Entonces, ¿se podría haber evitado?

Esto nos lleva a la primera parte de la solución, que es la que ha aparecido hasta ahora en los medios de comunicación: mantener el software actualizado, aplicando parches tan pronto estén disponibles. WannaCry utiliza una vulnerabilidad en el servicio SMB de Windows para distribuirse automáticamente dentro de una red privada. La primera infección en una red puede ser a través de un correo eléctrónico con un fichero adjunto malicioso. Una vez dentro, WannaCry utiliza la vulnerabilidad de Windows SMB para extenderse rápidamente. Los parches que arreglan esa vulnerabilidad se encuentran disponibles desde Marzo. En muchos programas, incluyendo Windows, los parches se aplican automáticamente y por eso el número de ordenadores afectados por WannaCry no ha sido tan grande entre usuarios individuales. Sin embargo, muchas organizaciones desactivan la aplicación automática de los parches en cuanto están disponibles y sólo los aplican después asegurarse que sus actividades de negocio no se ven afectadas por el parche. Aunque existen situaciones en las cuales puede ser necesario retrasar la aplicación de un parche, este ataque ha demostrado que organizaciones como Telefónica tienden a seguir esta política incluso en ordenadores que no están directamente relacionados con servicios en producción y

que deberían ser parcheados automáticamente. Otra razón por la que algunas organizaciones se han visto afectadas por WannaCry es que todavía utilizaban sistemas operativos de Microsoft obsoletos como Windows XP para los cuales Microsoft no distribuye parches de forma gratuita. Aunque es posible pagar a Microsoft para seguir recibiendo parches para Windows XP (y Vista), este soporte es caro, como demuestra que el sistema de salud de Reino Unido cancelara su contrato de soporte para Windows XP en 2015, lo cual ha significado parar muchas actividades críticas y desviar pacientes en por lo menos 16 de sus hospitales afectados por WannaCry.

La otra parte de la solución radica en que las agencias de inteligencia revelen las vulnerabilidades tan pronto sean encontradas, en vez de mantenerlas en secreto para explotarlas en su beneficio. Esto evitaría que cuando estas se filtren o sean robadas, los cibercriminales y otros atacantes las utilicen para sus objetivos. Para el que no haya seguido este ataque en detalle, la existencia de la vulnerabilidad que utiliza WannaCry y la forma en la cual puede explotarse se dió a conocer como parte de una filtración de datos por parte del grupo Shadow Brokers en Abril. Todo indica que los datos filtrados por Shadow Brokers provenían de la NSA, la agencia gubernamental de EE.UU. a cargo de la seguridad (y monitorización) de las comunicaciones. Incluida en esa filtración había varias herramientas que explotaban vulnerabilidades en Windows y que la NSA utilizaría supuestamente para hacerse con el control de los ordenadores de sus objetivos. Algunas de esas vulnerabilidades ya habían sido arregladas (lo que indica que los datos filtrados probablemente eran antiguos) pero otras acababan de ser arregladas por Microsoft en Marzo. El hecho que Microsoft parcheara esas vulnerabilidades justo antes de la filtración hace pensar que bien la NSA o Shadow Brokers avisaron a Microsoft que la filtración iba a producirse y contenía esas vulnerabilidades. Este caso es un buen ejemplo de los riesgos de que los gobiernos almacenen vulnerabilidades sin reportarlas a los desarrolladores de los programas afectados para poder usarlas cuando les sea necesario. A veces esas vulnerabilidades se hacen públicas y acaban siendo usadas en contra de uno mismo. Pero esta es una discusión para otro día.

Más allá de los parches: ciencia y tecnología para mejorar el software

El caso es que las dos soluciones mencionadas hasta ahora no son técnicas sino que requieren de decisiones políticas, bien a nivel de una organización en el primer caso y a nivel de Estado en el segundo.

Pero la misma existencia de estos "parches" de seguridad apunta al verdadero problema de fondo: ¿qué es una vulnerabilidad? ¿por qué existen estas vías de ataque en los programas? Una vulnerabilidad es, simple y llanamente, un error en un programa, un defecto, del que un atacante se aprovecha para penetrar en el sistema. La verdadera solución del problema de las vulnerabilidades es evitar que los programas contengan estos errores. Es vital desarrollar soluciones técnicas que permitan a medio o largo plazo eliminar estos errores, en especial los que conducen a las vulnerabilidades.

Una vulnerabilidad es, simple y llanamente, un error en un programa, un defecto, del que el atacante se aprovecha.

Este es uno de los principales objetivos de la investigación que desarrolla el Instituto IMDEA Software, promovido por la Comunidad de Madrid. La investigación que se lleva a cabo en nuestro Instituto se centra en desarrollar técnicas novedosas que permitan el desarrollo de software de manera efectiva, barata, y, sobre todo, segura. Si nos centramos en el ataque WannaCry existen 3 áreas de investigación de nuestro Instituto que aplican a la protección contra vulnerabilidades

y malware:

- Primero, el **desarrollo de lenguajes de programación seguros** que no permiten siquiera la existencia de ciertas vulnerabilidades. Por ejemplo la vulnerabilidad que usa WannaCry se basa en un desbordamiento de búfer que no es posible con lenguajes de programación de última generación.

- Segundo, el desarrollo de **técnicas automáticas de detección y verificación de la ausencia de de vulnerabilidades en el software**. El Instituto IMDEA Software desarrolla técnicas que garantizan que un programa esté libre de fallos cuando se distribuye, es decir que esté diseñado para ser seguro y proporcione unas garantías de esa seguridad. Estas últimas técnicas son necesarias porque existen muchos programas que están escritos en lenguajes de programación más antiguos, como por ejemplo Windows que tiene una amplia base de C++. En estos programas las vulnerabilidades no pueden prevenirse completamente y dada su complejidad (Windows 10 se estima que tenga unas 65 millones de líneas de código) no pueden ser verificados completamente en la actualidad (ver ejemplo en el cuadro adjunto al final).

- Por último, nuestro Instituto también desarrolla **técnicas de detección y análisis de malware**. El tipo de técnicas que desarrollamos permiten analizar de forma automática el malware para identificar defensas como la que ha permitido controlar la propagación de WannaCry, identificar los servidores remotos que el malware utiliza y revelar la localización de servidores ocultos en la red Tor que malware como WannaCry utilizan para recibir los pagos de los rescates de forma anónima. El objetivo es automatizar el análisis que hoy en día es altamente manual y desarrollar nuevas técnicas que permitan adaptarse a unos ataques que constantemente crecen en complejidad.

En conclusión, la batalla contra las vulnerabilidades y el malware requiere de diferentes tácticas y nuevas técnicas que permitan controlar y eliminar estos problemas a medio y largo plazo, evitando dar oportunidades a los atacantes. En el Instituto IMDEA Software investigamos para conseguir ese objetivo utilizando diversas aproximaciones que creemos podrán utilizarse en un futuro muy cercano para incrementar la protección de nuestros sistemas informáticos.

Fuente: Instituto IMDEA Software
Contacto: contacto@software.imdea.org
URL: http://www.software.imdea.org

Como ejemplo de nuestras líneas de investigación en **técnicas automáticas de detección y verificación de la ausencia de de vulnerabilidades en el software** algunos de nuestros investigadores fueron parte del equipo que descubrió la vulnerabilidad Freak que afectaba a los protocolos criptográficos SSL/TLS que se usan para proteger el tráfico Web.

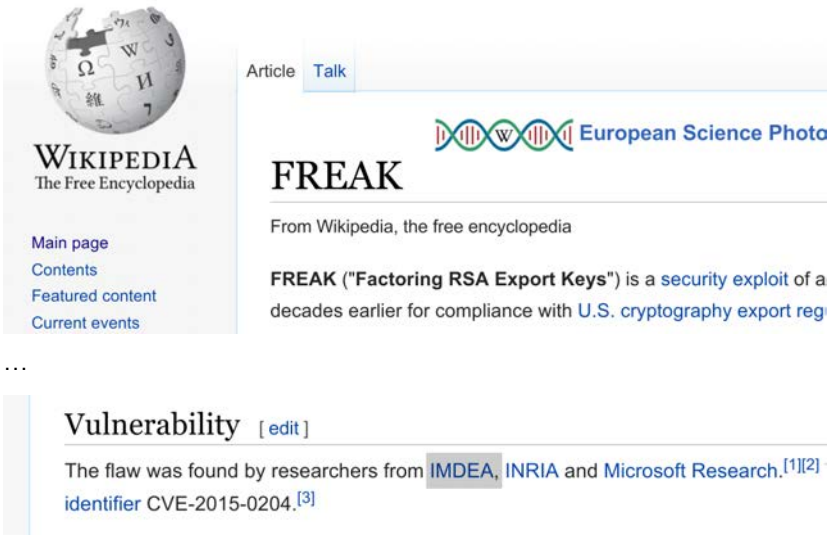
---

http://www.economist.com/news/science-and-technology/21645709-perils-deliberately-sabotaging-security-law-and-unintended-consequences

…

---

https://en.wikipedia.org/wiki/FREAK



…

---

https://arstechnica.com/security/2015/03/freak-flaw-in-android-and-apple-devices-cripples-https-crypto-protection

...

The research team behind FREAK included Karthikeyan Bhargavan, Antoine Delignat-Lavaud, and Jean-Karim Zinzindohoué of INRIA Paris-Rocquencourt; Cédric Fournet, Markulf Kohlweiss, and Santiago Zanella-Béguelin of Microsoft Research; Alfredo Pironti of Rome, Italy; and Pierre-Yves Strub, of IMDEA Software in Madrid, Spain. Stay tuned for updates to this post and additional coverage from Ars.