Fuente:
ITConnect

Dmitry Bestuzhev Director de Investigación y Análisis para Kaspersky Lab en América Latina @dimitribest, nos cuenta todo sobre Duqu 2.0

A nivel de seguridad, ¿qué novedades trae Duqu 2.0?

Duqu 2.0 es el master clase APT que hasta ahora no tiene competencia en el mercado, ya que no posee ningún mecanismo de persistencia en el sistema. Sin embargo, es capaz de sobrevivir y mutar entre las computadoras aun después de que estos sean parchados con las actualizaciones de Windows.

Duqu 2.0 existe únicamente en las memorias de las computadoras infectadas, su objetivo es arraigarse en los servidores como los Controladores de Dominios y así volver a infectar las computadoras reiniciadas.

Otra novedad es que Duqu 2.0 viene con tres exploits del día 0; uno de los cuales permite inmediatamente cargar sus drivers a nivel del kernel del sistema operativo, es decir saltar de la capa del usuario al kernel del sistema.

Los cibercriminales ¿se valieron de certificados digitales de Foxconn para armar este vector?

En realidad los actores detrás de este ataque han utilizado varios métodos tanto de infección inicial como de propagación posterior dentro de la red. Los certificados para firmar los binarios son parte de este ataque, son certificados válidos sustraídos de Foxconn – uno de los mayores productores de drivers y otros componentes importantes de los sistemas operativos a nivel mundial. Algunos gigantes de software y hardware también trabajan con Foxconn integrando sus soluciones en sus productos.

Una de las características de los ataques de Duqu 2.0 es que cada certificado fue utilizado una sola vez, es decir los atacantes no lo reciclaron – usaron un certificado diferente para cada ataque.

¿Qué impacto pudo tener Duqu 2.0 en los productos desarrollados por Foxconn?

En este momento debe de haber una investigación abierta. De parte nuestra, notificamos a Foxconn con suficiente tiempo de anticipación pero aún no hemos recibido respuesta alguna.

En general no es bueno que los certificados para firmar archivos sean sustraídos, ya que podrán ser

fácilmente utilizados para todo tipo del mal.

Si tomamos como base la curva evolutiva de Duqu 2.0 y la comparamos con el promedio de evolución de la industria de AV ¿es saldo es negativo para la industria?

No lo creo. Más bien es un reflejo de la realidad de que tenemos más actores de muy alto perfil y no solamente a los criminales cibernéticos clásicos que apuntan al dinero de las víctimas. Hoy prácticamente hay dos o tres compañías de anti-virus que de verdad pueden dar frente a los ataques del nivel de Duqu 2.0. Las demás compañías no han podido desarrollar suficiente experiencia técnica para estar a nivel de esta tendencia y aquí me refiero tanto a la capacidad científica, como tecnológica.

Las reglas tradicionales de seguridad ¿sirven para este nivel de sofisticación, o hay que reescribirlas?

Hay que recordar cómo encontramos esta amenaza. Fue exactamente en nuestra propia red al hacer pruebas con una nueva solución de Kaspersky que se llama internamente Anti-APT. Por supuesto esta solución no es el mismo producto que tienen los usuarios en sus computadores en casa. El método de protección puede variar y su enfoque netamente depende del actor detrás de ello. Si hablamos en general, el monitoreo del tráfico saliente es un factor muy importante. Lo que se debe mirar especialmente son las solicitudes DNS.

A pesar de que hoy en día existan algunas soluciones orientadas a la detección de las APTs, estas no serían eficaces contra Duqu 2.0; esto se debe a que en el disco duro no se registran ninguna anomalía.

Pues, las soluciones que trabajen con los objetos ubicados en el disco duro de las víctimas, serán bastante limitadas.

¿Qué experiencia nos deja Duqu 2.0?

Hay varias lecciones. La primera es que es una muy mala idea atacar a una compañía de seguridad. Siempre encontraremos al atacante y lo pondremos al descubierto. La segunda es que los actores de los ataques dirigidos están más avanzados de lo que la industria creía. La tercera es que nadie está a salvo. La cuarta es que con solamente compartir la información y no callar los hechos se puede dar frente a estos ataques. No es bueno ocultar los incidentes sino revelarnos haciéndolo de una manera responsable. La quinta es que el mismo actor puede tener varias operaciones paralelas; una va de mano con los aliados, mientras que otra va en contra de esos mismos aliados sin que los aliados lo sepan. Llegamos a un punto cuando no se puede confiar en absolutamente nadie.

Este cambio de concepto arquitectónico en la construcción de un malware ¿acelera el motor de innovación del cibercrimen? ¿Cómo compensamos estos niveles de cambio?

En cierto sentido sí, pues toda la información o casi toda llega a ser pública. Por supuesto hay que contemplar la posibilidad de que las mismas técnicas pueden ser recicladas; pero hay que recordar que los mismos niveles de sofisticación no se logran solamente por tener una idea sino que hay que contar con un presupuesto bastante grande. Por ejemplo, los actores detrás del Duqu 2.0 han invertido en este ataque por lo menos unos 10 millones de dólares. Esta es una cifra no necesariamente alcanzable para todo tipo de atacante.

¿Qué recomendaciones le daría a un CIO para comprar que sus sistemas están libres de Duqu 2.0?

Lo más fácil es usar una demo de Kaspersky para revisar todos los sistemas. Todos nuestros productos detectan todas las modificaciones de Duqu 2.0. El demo viene con una validez de 30 días y permite revisar los sistemas basados en Windows, OSX, Linux, Android y otros.

También se puede utilizar los Indicadores de compromiso publicados en nuestros blogs en www.securelist.com [1] y usarlos con su software de preferencia para buscar la presencia de Duqu 2.0 en el sistema.

Finalmente, como una medida drástica de seguridad, se podría apagar toda la red de golpe, esto podría hacer que el Duqu 2.0 muera en la red. Si uno apta por este proceso, debe entender que este debe ser de golpe al mismo tiempo, porque si no, Duqu 2.0 se quedará igualmente en la red.

Disponible en: http://itclat.com/2015/06/17/duqu-10000/ [2]

Links
[1] http://www.securelist.com
[2] http://itclat.com/2015/06/17/duqu-10000/