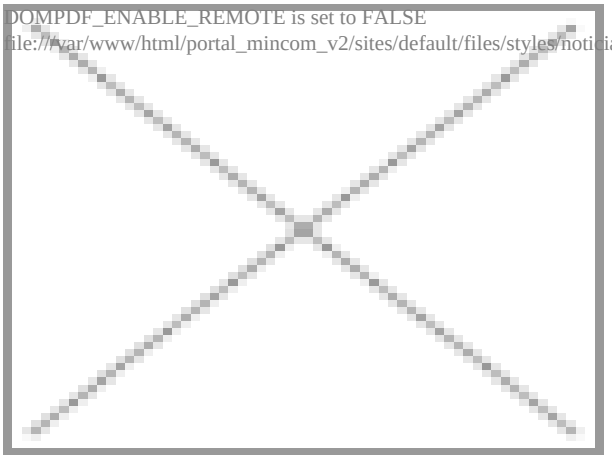
DOMPDF_ENABLE_REMOTE is set to FALSE
file:///var/www/html/portal_mincom_v2/sites/all/themes/mincom/logo.png

DOMPDF_ENABLE_REMOTE is set to FALSE
file:///var/www/html/portal_mincom_v2/sites/default/files/styles/noticias/public/ataque-verano-pc_hi.jpg



Fuente:
Computer World

Las infecciones de malware están relacionadas con los eventos P5+1 y los lugares de celebración de reuniones de alto nivel entre líderes mundiales, según Kaspersky Lab.

A principios de la primavera de 2015, Kaspersky Lab detectó una ciberintrusión que afectaba a varios de sus sistemas internos. A raíz de ello descubrieron una nueva plataforma de malware de uno de los actores más hábiles, misteriosos y poderosos del mundo APT.

Para la compañía, los ciberatacantes estaban seguros de que era imposible descubrir el ataque, ya que incluía algunas características únicas e invisibles para no dejar casi rastro. El ataque explota vulnerabilidades zero-day y tras la elevación a privilegios de administrador de dominio, el malware se propaga en la red a través de la instalación de paquetes MSI (Microsoft Software Installer), que son los archivos que los administradores de sistemas utilizan habitualmente para instalar software en equipos Windows en remoto. Además, no realizaba cambios en el disco de la víctima o en la configuración del sistema, lo que hacía muy difícil la detección. La filosofía y la forma de pensar del grupo Duqu 2.0 muestra una generación más avanzada, por delante de todo lo visto en el mundo APT.

"Espiar a las empresas de seguridad es una tendencia muy peligrosa. El software de seguridad es la última frontera de protección para las empresas y los clientes en el mundo actual, donde el hardware y la red pueden verse comprometidos. Por otra parte, antes o después, las tecnologías implementadas en los ataques dirigidos serán examinadas y utilizadas por los terroristas y delincuentes profesionales. Y eso es un escenario posible y de extrema gravedad", ha explicado Eugene Kaspersky, CEO de Kaspersky Lab.

La empresa no era el único objetivo de este atacante. Hay víctimas en países occidentales, así como en países de Oriente Medio y Asia. En particular, algunas de las nuevas infecciones entre 2014-2015 están vinculadas a los eventos P5+1 y lugares relacionados con las negociaciones con Irán sobre un acuerdo nuclear. El actor que está detrás de Duqu parece haber lanzado ataques en los lugares donde se produjeron estas negociaciones. Además, el grupo Duqu 2.0 lanzó un ataque similar relacionado con el 70 aniversario de la liberación de Auschwitz-Birkenau. A estas reuniones asistieron muchos dignatarios y políticos extranjeros.

Kaspersky Lab realizó una auditoría de seguridad inicial y un análisis del ataque. La auditoría incluyó la verificación del código fuente y la comprobación de la infraestructura corporativa. La auditoría está todavía en curso y se completará en unas pocas semanas. Además del robo de propiedad intelectual, no se detectaron

otros indicadores de actividad maliciosa. El análisis reveló que el principal objetivo de los atacantes era espiar las tecnologías de Kaspersky Lab, la investigación en curso y procesos internos. No se detectó interferencia con procesos o sistemas. Y la compañía garantiza que sus clientes y partners están seguros y que no hay impacto en sus productos, tecnologías y servicios.

Entre los detalles técnicos sobre Duqu 2.0, dados en el blog Securelist, destaca que el ataque fue cuidadosamente planeado y llevado a cabo por el mismo grupo que estaba detrás del infame ataque APT Duqu de 2011 y posiblemente es una campaña patrocinada por un estado. Kaspersky Lab cree que el objetivo principal del ataque era obtener información sobre las tecnologías más recientes de la compañía. Los atacantes estaban especialmente interesados ??en los detalles de las innovaciones de sus productos y la información a la que tuvieron acceso no es clave para el funcionamiento de los productos.

Los atacantes parecen haber explotado hasta tres vulnerabilidades zero-day. La última que quedaba (CVE-2015-2360) ha sido parcheada por Microsoft el 9 de junio de 2015 (MS15-061), cuando los expertos de Kaspersky Lab les informaron.

"Este ataque altamente sofisticado utiliza hasta tres exploits zero-day, algo muy sorprendente ya que los costes deben ser muy elevados. Para mantenerse oculto, el malware reside sólo en la memoria de kernel, por lo que las soluciones anti-malware podían tener problemas para detectarlo. Tampoco se conecta directamente a un servidor de comando y control para recibir instrucciones. En lugar de ello, los atacantes infectaron pasarelas de red y servidores de seguridad mediante la instalación de drivers maliciosos que dirigieron todo el tráfico de la red interna a los servidores de comando y control de los atacantes", ha afirmado Costin Raiu, director del Global Research and Analysis Team de Kaspersky Lab.

Los atacantes también mostraron un gran interés por las investigaciones actuales de Kaspersky Lab sobre ataques dirigidos avanzados; probablemente conscientes de la reputación de la compañía como una de las más avanzadas en la detección y lucha contra los ataques APT complejos. El programa malicioso utiliza un método avanzado para ocultar su presencia en el sistema: el código de Duqu 2.0 sólo existe en la memoria del equipo y trata de eliminar todos los rastros en el disco duro.

"Reportar este tipo de incidentes es la única forma de hacer que el mundo sea más seguro. Esto ayuda a mejorar el diseño de la seguridad de las infraestructuras de las empresas y envía una señal clara a los desarrolladores de este malware: todas las operaciones ilegales serán detenidas y procesadas", apunta Eugene Kaspersky.

Kaspersky Lab ha resuelto este incidente previniendo que un problema similar pueda suceder. La compañía se ha puesto en contacto con los correspondientes departamentos de policía en varios países solicitando que se lleven a cabo investigaciones oficiales sobre este ataque.
Además, la compañía subraya que estos resultados son sólo los preliminares de una primera fase de investigación, creen que este ataque ha tenido un alcance geográfico más amplio y muchos más objetivos, dada la información que han recogido.

Disponible en: http://www.computerworld.es/sociedad-de-la-informacion/la-plataforma-de-ataque-duqu-20-peligro-para-occidente-asia-y-oriente-medio [1]

Links
[1] http://www.computerworld.es/sociedad-de-la-informacion/la-plataforma-de-ataque-duqu-20-peligro-para-

occidente-asia-y-oriente-medio