¿Puede estar el régimen español detrás del malware "Careto/The Mask"?

DIARIO TURING :: 15/02/2014

‘Careto’ podría tener origen español o hispano, pues se han encontrado varios términos en castellano dentro del software

El malware espía extremadamente sofisticado que ha descubierto la firma de seguridad rusa Kaspersky ha sido bautizado como ‘Careto’. Esto es porque el término estaba incluido en algunos de los módulos del software.

Un detalle, junto a **la existencia de otras palabras en español**, que sugiere que los creadores son de habla hispana, algo muy poco habitual en ataques de este tipo. Los atacantes a veces dejan pistas falsas para que sea más difícil rastrearlos, pero no es habitual encontrar términos en castellano.

Sin embargo, los países infectados y la dispersión de las infecciones **se corresponden con los ejes de la política exterior española**. En total son 31 países, entre los cuales se encuentran nueve de Latinoamérica, con especial hincapié en Brasil, donde España cuenta con grandes inversiones en estos momentos. En el norte de África todos los países que lindan con el Mediterráneo han sido infectados por el malware. El caso más agudo es el de Marruecos, que es de largo la nación más afectada por 'Careto'. Europa también está presente, son siete los estados que figuran en la lista de Kaspersky.

Han sido 31 países los infectados, con desigual suerte, como se puede ver en la gráfica

Otras regiones de importancia estratégica para España están reflejadas en el ataque, como Estados Unidos, países de Oriente Medio y China. Un dato que también podría ser revelador es que Gibraltar se encuentra en la lista, como apunta el especialista en seguridad Bruce Schneier en su blog, quien asimismo sugiere que pronto los países empezarán a infectar a otros con los que no tienen relación para alentar la confusión. La lista completa la componen Argelia, Argentina, Bélgica, Bolivia , Brasil , China, Colombia, Costa Rica, Cuba , Egipto, Francia , Alemania, Gibraltar, Guatemala, Irán , Irak, Libia, Malasia , Marruecos, México, Noruega, Pakistán, Polonia, Sudáfrica, España, Suiza, Túnez, Turquía, Reino Unido, Estados Unidos y Venezuela.

Los investigadores descubrieron la existencia de ‘ Careto’ el año pasado. Desde entonces han ido desgranando su funcionamiento y su amplitud. **Las muestras más antiguas del malware espía se detectaron en 2007**. En total son 380 víctimas, equipos informáticos, con 1.000 IPs diferentes las que se han visto afectadas por ‘Careto’. El malware interviene todos los canales de comunicación de un equipo, con lo que toda la información que se mueve queda expuesta. El malware está orientado a la captación de los datos más críticos, como las contraseñas, configuraciones VPN o claves SSH, que permiten la entrada a servidores SSH, con seguridad adicional. Los archivos RDP, que ofrecen acceso a máquinas

reservadas, también se han visto afectados hasta el pasado mes de enero, cuando el servidor de comando y control utilizado por los atacantes cesó su actividad.

“[El malware] permite desde **grabar conversaciones de Skype, ver todo lo que tecleas, sacar pantallazos**, robar archivos, instalar cualquier cosa en tu equipo, en fin, todo un arsenal para espiar”, indica Vicente Díaz, analista senior de malware en Kaspersky.

*El termino '*careto*' está presente en algunos de los módulos del malware*

'The Mask' **se ha introducido en instituciones gubernamentales, legaciones diplomáticas o embajadas**. Sin embargo, también se ha encontrado en los llamados sistemas críticos (aquellas instalaciones cuyo funcionamiento es necesario para la zona donde se emplazan), como las compañías de energía, incluidas las de petróleo y gas. Incluso constan como objetivos organizaciones dedicadas a la investigación y grupos activistas, lo que da una idea del afán de control de los atacantes. Vicente Díaz destaca que se trata de objetivos selectivos con perfiles cuidadosamente escogidos.

Uno de los malware espía más sofisticados La infección de ‘Careto’ se producía a partir de un ataque de phishing, el envío de mensajes de correo electrónico con enlaces a un sitio malicioso, camuflado bajo una redirección que se efectuaba a algún portal conocido, como YouTube, tras haber instalado el malware. Para confundir a los usuarios se han utilizado subdominios que simulaban secciones de los principales periódicos de España, así como otros internacionales, entre los que están ‘The Guardian’ o ‘The Washington Post’.

Pero la verdadera sofisticación se advierte en la complejidad de las herramientas utilizadas. Los atacantes se sirven de exploits punteros, un rootkit y un bootkit. Kaspersky ha descubierto que al menos se utilizó una vulnerabilidad de Adobe Flash Player, presente en las versiones 10.3 y 11.2. Una falla que Adobe solucionó en abril de 2012, según indica la compañía. La detección del malware se ha calificado como extremadamente difícil.

“Hacer un ranking de sofisticación resulta complicado. No obstante, este código malicioso realmente era muy alucinante. A nivel técnico era muy escurridizo y hacía una serie de cosas muy originales”, afirma Díaz. **Existen versiones de ‘Careto’ para Mac OS X y para Linux**, mientras que los investigadores juzgan como probables otras para Android y iOS. La variedad de sistemas operativos que soporta se debe a que el malware está destinado al equipo de una víctima específica, con lo que los atacantes se aseguran más posibilidades de éxito.

Aunque la atribución es complicada, desde la firma de seguridad rusa apuntan una serie de razones que sugieren el patrocinio de una entidad estatal. El tipo de víctimas y su carácter selectivo invita a pensar en labores de inteligencia. En una nota de prensa, el director del equipo de investigación y análisis global de Kaspersky Lab, Costin Raiu, expone así las pistas. “Se ha observado un alto grado de profesionalidad en los procedimientos operativos del grupo que está detrás de este ataque: desde la gestión de la infraestructura, el cierre de la operación, evitando las miradas curiosas a través de las reglas de acceso, y la limpieza en lugar de la eliminación de los archivos de registro”, comenta, aclarando que **este nivel operacional no es habitual en grupos dedicados al cibercrimen**.

Imágenes: Kaspersky

_____

https://www.lahaine.org/mm_ss_est_esp.php/horario-y-actividades-de-birosta-en-zara