Regin, El Software Malicioso Que Espía Gobiernos Y Grandes Empresas

El espionaje cada vez tiene pasos agigantados, avanzando en la mejora del **código para cada malware** o software de espionaje. Recientemente se ha **descubierto una pieza avanzada de malware**, que ha estado en uso desde el 2008 para espiar a gobiernos, empresas e individuos, dijo Symantec en un informe publicado el domingo.

La **herramienta de ciberespionaje Regin**, usa varias funciones de ocultación para impedir la detección la cual requiere una importante inversión de tiempo y recursos, lo que sugiere que es el codigo sea producto de una alianza de un Estado o nación, según Symantec, sin sugerir en qué país estaba detrás de él. El **diseño del software malicioso** hace que sea muy adecuado para la vigilancia masiva a largo plazo, ha dicho la compañía.

«Los desarrolladores de Regin han realizado un esfuerzo considerable y esto se ve en que el malware es poco visible. Su carácter discreto significa que potencialmente puede ser utilizado en campañas de espionaje que duran varios años», dijo la compañía en un comunicado. «Incluso cuando se detecta

su presencia, es muy difícil determinar lo que está haciendo.»

La naturaleza altamente personalizable de Regin permite una amplia gama de capacidades de acceso remotos, incluyendo el robo de contraseñas y de datos, entre otras funciones como la captura de pantalla y de eventos de los computadores infectados. Otras infecciones que se lograron identificar son el monitoreo del tráfico de la red y análisis de **bases de datos de correo electrónico Exchange**.

Algunos de los **principales objetivos de Regin** incluyen proveedores de servicios de Internet y empresas de telecomunicaciones, donde al parecer el complejo software se utiliza para controlar las llamadas y comunicaciones direccionadas mediante la infraestructura de las empresas. Otros objetivos incluyen empresas de los sectores de líneas aéreas, energía, hospitales y centros de investigación, dijo Symantec.

Los objetivos del malware son geográficamente diversos, dijo Symantec, la observación de más de la mitad de las infecciones se han visto en Rusia y Arabia Saudita. Entre los demás países destinatarios son Irlanda, México y la India. Regin **se compone de cinco etapas de ataque** que están ocultos y cifrados, con la excepción de la primera etapa, que se inicia una cadena de dominó para descifrar y ejecuta la siguiente etapa. Cada etapa individual contiene **poca información sobre la estructura de malware**. Las cinco etapas tuvieron que ser adquiridas para analizar la amenaza planteada por el malware.

Finalmente

El ciberespionaje es un tema sensible, a menudo poniendo en riesgo las relaciones diplomáticas entre los países. Los EE.UU. y China han peleado durante años por **acusaciones sobre espionaje electrónico.** Los EE.UU. han acusado al Gobierno de China y militar de la participación en ciberespionaje generalizado dirigido a redes del gobierno de Estados Unidos y negocios de computación. China ha negado los cargos y acusó a los EE.UU. de comportamiento similar dirigido su propia infraestructura.

Sin duda este tipo de competencia tecnológica, ha llevado al desarrollo de grandes programas de espionaje, tanto así que Regin ha estado funcional desde el 2008, y sin duda, lo mas preocupante son las diversas funciones que realiza este software malicioso.