12-03-2014

Rusia y Ucrania ya están en ciberguerra

Miguel Ángel Criado
Cuarto Poder

Mientras la calma tensa se mantiene en la península de Crimea, las hostilidades entre Ucrania y Rusia han estallado en internet. Informes de varias empresas de seguridad han descubierto la existencia de virus informáticos en redes y ordenadores ucranianos. Aunque no señalan al Gobierno ruso, su código es tan sofisticado que no puede ser obra de aficionados sino de alguien con conexiones en alguna "agencia de inteligencia". Lo más llamativo es que, sea quien sea el que los ha creado, lleva espiando desde hace años.

Desde que la crisis en Ucrania diera un giro inesperado con el traslado del conflicto de la europeísta Kiev a la rusófila Crimea, *hackers* de Rusia y Ucrania están atacando redes y webs del otro lado. Unos y otros se dedican a colarse en páginas oficiales o de medios de comunicación, alterando su contenido. Hasta miembros del colectivo Anonymous se han puesto del lado de los ucranianos y han lanzado varios ataques contra servidores de empresas y la administración rusa con su #OpRussia.

Pero son fuegos de artificio si se compara con lo que han descubierto una empresa de seguridad informática alemana y otra de inteligencia militar británica. La primera, G DATA, publicaba ya antes de que las tropas rusas rodearan las bases militares ucranianas un informe sobre un software malicioso muy complejo y programado para robar información confidencial. Lo han bautizado con el nombre de Uroburos, en referencia a una serpiente que se muerde su propia cola y que aparece en varias mitologías. Los técnicos de la compañía germana encontraron ese nombre en el código del virus, aunque el original en griego sería Uróboros.

Uroburos es lo que los expertos en seguridad informática llaman un *rootkit*, un conjunto de herramientas que se integran en el núcleo del sistema atacado que entrega el control de la máquina al atacante y lo hace manteniendo su presencia oculta. En su caso, está diseñado para grabar archivos y tráfico del ordenador y enviarlo a servidores controlados por su creador. Por lo visto, tiene la capacidad de infectar a otros equipos que no estén conectados a internet a través de la red interna de la organización a la que pertenece.

"Debido a la complejidad de este malware y las posibles técnicas de espionaje que usa, creemos que este *rootkit* tiene como objetivo a gobiernos, centros de investigación y/o grandes empresas", escribían sus descubridores en el blog oficial de la compañía. Para los expertos alemanes, crear Uroburos exige mucha inversión. "El equipo de desarrollo que está detrás de este malware incluye expertos en informática altamente cualificados, como se puede deducir de la avanzada estrcutura y diseño del rootkit", añaden.

Lo que también han descubierto es que este virus no es una creación al calor del conflicto en Ucrania. Al menos lleva oculto tres años. En cuanto a su origen, en G DATA apuntan a Rusia. Además de que este idioma aparece en algunas líneas de código (cualquiera lo podría haber puesto ahí), hay detalles técnicos que refuerzan la pista rusa. Los nombres de los archivos, la clave de cifrado o su comportamiento revelan que quien haya creado Uroburos también diseñó Agent.BTZ, un virus que protagonizó en 2008 uno de los ciberataques más serios que han soportado las redes militares de Estados Unidos. Ya entonces se acusó a Rusia de estar detrás.

La división de inteligencia aplicada de BAE Systems, empresa británica que fabrica tanto avanzados aviones no tripulados como complejos sistemas de guerra electrónica, también ha detectado la presencia de un amplio programa de espionaje informático al que han bautizado como The Snake Campaign (La Campaña de la Serpiente, en inglés). Según su propio informe, Uroburos sería un componente más de este ataque.

Esta serpiente llevaría espiando al menos desde 2005 y, tanto el ataque de 2008 contra Estados Unidos como los que están sufriendo ahora las redes ucranianas formarían parte de la misma operación con un mismo virus con diversas variantes. De hecho, otro virus llamado Turla, diseñado para atacar redes oficiales de países de la OTAN, presenta muchas similitudes con Agent.BTZ, cuentan desde *Reuters*.

Por supuesto, que un virus parezca proceder de Rusia no significa que haya sido creado por las autoridades rusas y menos aún que lo estén usando para espiar a sus vecinos. Pero en el informe de BAE Systems (PDF) hay una gráfica muy reveladora. La primera muestra de una de las variantes del virus de la serpiente que han analizado procede de Ucrania. Aunque también tienen casos de infección en países occidentales, la mayoría de las infecciones reportadas proceden de Lituania, Georgia y Ucrania, tres antiguos miembros de la Unión Soviética y ahora vecinos temerosos del expansionismo ruso. De hecho, más del 60% de las muestras proceden de Ucrania y en lo que va de 2014, hay mas ataques detectados que en los cuatro años anteriores.

Rusia negará estar detrás de la serpiente y sus distintas cabezas. Ya negó estarlo tras Agent.BTZ. También rechazó haber organizado el ataque cibernético sufrido por Estonia en 2007, aunque se demostró que procedía de territorio ruso. Tampoco reconoció ninguna responsabilidad en el apagón informático que sufrieron las redes de telecomunicaciones de Georgia durante la guerra que les enfrentó por Osetia del Sur en 2008. Ahora también niega que las tropas que rodean las bases ucranianas sean suyas.

Lo peor es que, según los informes, estos virus están diseñados para espiar y recabar información pero también podrían contener instrucciones para destruir las redes que han infectado si fuera necesario. Como dicen desde G DATA: "Creemos que el equipo tras Uroburos ha seguido trabajando en variantes aún más avanzadas que aún no han sido descubiertas". Algo así supondría pasar del simple espionaje a la ciberguerra.

Fuente: http://www.cuartopoder.es/mecanicamente/rusia-y-ucrania-ya-estan-en-ciberguerra/3903