Los ciberataques, otra poderosa arma en el conflicto entre Rusia y Ucrania

28/02/2022

A medida que las ciudades de Ucrania son objeto de fuertes ataques con misiles por parte de Rusia y las tropas avanzan por el país, una contienda subterránea y menos visible está también afectando duramente a Kiev.

Se trata de una serie de ataques cibernéticos a varios sitios web de los departamentos gubernamentales y bancarios de este país, que en ocasiones han llevado al colapso total de su sistema.

Uno de los más recientes –y sofisticados– ocurrió este miércoles, en la antesala a la invasión rusa, solo horas antes de que Vladimir Putin anunciara una «operación militar especial» que acabó convirtiéndose en una invasión.

Funcionarios de seguridad acusaron al Kremlin de estar detrás de la ofensiva –que afectó a los sitios web del Parlamento,

del Servicio de Seguridad y del ministerio de Relaciones Exteriores de Ucrania, entre otros– y dijeron que los piratas informáticos «ya no intentan ocultar su identidad».

Además, indicaron que esta vez los ataques estaban «en un nivel completamente diferente», con el empleo de nuevas tácticas y una capacidad de sabotaje que no se había visto antes.

Los ciberataques son un arma poderosa: pueden paralizar la infraestructura de un país, afectando los servicios de agua, electricidad y telecomunicaciones, entre otras cosas.

Sin duda son una herramienta que, en este caso, podría servir para debilitar aún más a una Ucrania que intenta hacer frente al gigantesco poder militar y de inteligencia ruso.

¿Qué tipo de ataques han afectado a Ucrania?

Los últimos ciberataques registrados en Ucrania han tenido una característica en común: han sido calificados como ataques de «denegación de servicio» (DDoS por sus siglas en inglés).

Este tipo de ofensiva emplea bots–una herramienta digital que se usa para realizar tareas repetitivas, predefinidas y automatizadas– para inundar un servicio en línea, abrumándolo hasta que falla, se bloquea e impide el acceso de usuarios legítimos.

«Básicamente, los atacantes sobrecargan un servicio o un sitio web con más tráfico del que pueden manejar», le explica a BBC Mundo Richard Smith, director del Instituto de Tecnología Cibernética de la Universidad de Montfort, en Reino Unido.

«**La red de bots es controlada de forma remota y los propietarios probablemente desconocen por completo que tienen un software malicioso en sus sistemas**», agrega.

Pero, además, se descubrió que Ucrania había sido objeto de otro tipo de ataque: a través de la instalación de un malware

(o programa malicioso) llamado «wiper» (limpiador, en español), lograron destruir los datos de distintos sistemas.

«Lo que hizo fue eliminar el registro de arranque de los dispositivos. Eso significa que luego no pueden iniciarse; tienes que empezar completamente desde cero y reinstalar todo. Con ello, se necesita aún más tiempo para poder volver a la capacidad operativa total», indica Smith.

Los expertos en seguridad cibernética de las compañías ESET y Symantec llamaron a este virus «HermeticWiper», asegurando que se había instalado en cientos de computadores en el país.

Además, señalaron que el software malicioso se creó el 28 de diciembre de 2021, lo que implica que el ataque pudo haber sido planeado desde entonces.

En enero, Ucrania ya había sido víctima de varios ataques cibernéticos.

Algunos sitios web afectados fueron reemplazados por una advertencia que decía que «se preparen para lo peor».

Confusión y caos

A pesar de que Ucrania, Estados Unidos y otras potencias occidentales han responsabilizado directamente a la Dirección Principal de Inteligencia de Rusia (GRU) de estos ataques, el Kremlin ha negado su participación, calificando las acusaciones de «rusofóbicas».

Y, hasta el momento, ha sido difícil comprobar que el país liderado por Vladimir Putin está realmente detrás de la ofensiva cibernética.

«No hay forma de probarlo. La atribución suele ser muy difícil en estos casos porque no necesariamente se lanzan los ataques desde servidores en su propio territorio», indica Smith.

«No es imposible, pero el nivel de pruebas que puedes llegar a

tener probablemente no serían suficientes en un tribunal de justicia internacional, por ejemplo», añade.

Pero expertos aseguran que, en los últimos años, Rusia ha demostrado ser experta en atacar el ámbito cibernético de los países.

«El 58% de los ataques contra la infraestructura de los gobiernos de Estados Unidos y Reino Unido se atribuyeron el año pasado a Rusia o, digamos, a grupos que actúan por Rusia», dice Smith.

Y es que los ciberataques han demostrado ser una herramienta eficiente a la hora de debilitar al enemigo.

El académico Richard Smith cree que es un tipo de ofensiva que en este momento del conflicto entre Rusia y Ucrania está siendo muy importante, sobretodo en el ámbito de la propaganda, «intentando reducir el espíritu del pueblo ucraniano».

«También confundiendo y generando caos al hacer que los sistemas fallen», indica.

En enero, las autoridades ucranianas señalaron a través de un comunicado que el objetivo de los ciberataques «no es solamente intimidar a la sociedad», sino además «desestabilizar la situación» con «falsas informaciones sobre la vulnerabilidad de las infraestructuras informáticas del Estado».

«Guerra híbrida»

Los ataques de «denegación de servicio» (DDoS) ya se habían registrado en el pasado.

Estas ofensivas afectaron a Georgia y Crimea durante las incursiones de 2008 y 2014, respectivamente.

En 2015 y 2016, en tanto, la Unión Europea, Reino Unido y

Ucrania culparon a los piratas informáticos del gobierno ruso de los ataques a las subestaciones eléctricas que provocaron cortes de energía generalizados.

Lo anterior corresponde a las llamadas tácticas de «guerra híbrida» de Rusia, un concepto que fue utilizado por primera vez a principios de los años 2000 y que tiene que ver con la implementación de una estrategia (o varias) de confrontación que no pasa necesariamente por un combate de tipo militar.

Así lo explicó a BBC Mundo Antonio Alonso Marcos, profesor de Relaciones Internacionales de la Universidad San Pablo CEU, en España.

«Un país puede utilizar medios que vayan minando la seguridad y la estabilidad de otro país. Y no son medios militares, sino, por ejemplo, ciberataques o el lanzamiento de una oleada masiva de tuits que vayan en contra de la posición de un gobierno determinado. A eso se le denomina guerra híbrida», dice.

Este tipo de agresiones son cada vez más comunes y muchas veces pueden tener resultados tanto o más peligrosas que los ataques directos con misiles.

Por eso, el apoyo de la infraestructura cibernética ha sido reconocido como un aspecto importante de la ayuda internacional.

Ahora, diversos países de la Unión Europea, entre ellos, Países Bajos, Polonia, Estonia y Croacia, están enviando a Ucrania expertos en seguridad cibernética para ayudarlos a enfrentar estas amenazas.

BBC News Mundo

@norbertparedes