El papel del ciberconflicto en Ucrania sigue siendo una incógnita un año después

La invasión de Ucrania nos ha hecho testigos de operaciones cibernéticas destructivas, de influencia y de recopilación de inteligencia, pero de momento, no de la ciberguerra que algunos esperaban hace un año

Hace algo más de un año que comenzó la invasión de Ucrania y una de las incertidumbres que nos han acompañado desde entonces, y que se suma a las humanitarias, políticas o económicas, tiene relación con la ciberseguridad. Y es que los primeros signos de esta invasión se dieron en el ciberespacio. Desde entonces se han observado multitud de ciberataques a las infraestructuras ucranianas y a las de sus aliados, de distintos tipos y con diferentes objetivos. Pero la frecuencia de estos ataques, y sobre todo, sus impactos, no han sido los que cabía esperar en un principio. Parece que esto tiene que ver, a partes iguales, con una falta de organización desde el punto de vista ofensivo en el bando ruso y con unas altas capacidades defensivas en el bando ucraniano (tanto propias, como por parte de todos sus aliados). Pero hay que tener en cuenta que no tenemos toda la información y que no está nada claro cómo va a evolucionar el conflicto en los próximos meses. Tenemos que estar preparados.

Hace años que se considera el ciberespacio como un espacio más en el que puede desarrollarse el conflicto bélico más allá de los tradicionales tierra, mar y aire. Hay que tener en cuenta que Rusia es una de las potencias mundiales en ciberseguridad. ¿Qué sabemos de lo ocurrido hasta el momento? ¿Ha afectado sólo a Ucrania o también a otros países?

Primera ola de ataques destructivos

Rusia y sus socios habituales fueron muy activos en las semanas previas a la invasión terrestre. El número de ciberataques a sistemas ucranianos aumentó espectacularmente, lo que fue un claro indicador de que las hostilidades habían pasado a un nuevo nivel. En aquel entonces no se sabía si todo iba a quedar en un conflicto híbrido o de “paz formal” o si, por el contrario, terminaría siendo un conflicto bélico tradicional.

> En estos momentos muchos aspectos de todos estos ataques, y de otros que no se han hecho públicos, son desconocidos para el público general

Los ataques de esta primera fase fueron destructivos, casi siempre dirigidos a provocar impactos en la integridad y en la disponibilidad de los sistemas y aplicaciones ofrecidos por las administraciones públicas ucranianas y por sus empresas más importantes. *Software* malicioso de tipo *wiper* (*WhisperGate*, *HermeticWiper*) que borraba bases de datos completas, o denegaciones de servicio volumétricas que impedían que las páginas web gubernamentales o de bancos dieran servicio a sus usuarios legítimos, fueron

los patrones más repetidos.

En ese momento las administraciones ucranianas se movilizaron de manera masiva para poner a salvo los datos de sus ciudadanos, realizando copias de toda la información sensible que manejaban en servicios en la nube cuyos centros de datos no corrieran peligro si se producía una invasión. Y ofreciendo los servicios esenciales también desde centros de datos deslocalizados que no se vieran afectados por potenciales cortes de luz, destrucción de edificios, etc. Diferentes proveedores tecnológicos y socios de la OTAN ofrecieron su ayuda para realizar estas operaciones de la forma más rápida y eficiente que fuera posible.

Una vez comenzada la invasión terrestre, se esperaba una ola de ciberataques a infraestructuras críticas en Ucrania como centrales nucleares o eléctricas, potabilizadoras y depuradoras de agua, centros de distribución de gas, antenas y torres de comunicaciones, ferrocarriles, etc. Pero en un escenario de conflicto bélico terrestre la mayor parte de estos ataques se realizaron mediante bombardeos físicos y no mediante los sofisticados ciberataques que se había previsto. Afortunadamente tampoco se observó el pico de ciberataques esperado en países de la OTAN que apoyaron a Ucrania y que hubiera escalado el conflicto desde sus fases iniciales.

Segunda ola de desinformación

Justo al comenzar la invasión terrestre se observó cómo gran parte de los recursos rusos se destinaban a la propaganda y a la influencia, algo habitual en todos los conflictos bélicos, pero que en este caso se daba casi por completo en el ámbito digital. Las operaciones rusas iban dirigidas, por un lado, a evitar la oposición doméstica y transmitir el mensaje oficial en Rusia. Por otro lado, a crear confusión en Ucrania, generar desconfianza en el gobierno legítimo y provocar división entre los socios de la OTAN.

Estas operaciones se han realizado desde diferentes medios rusos, pero también creando plataformas y cuentas específicas en redes sociales para ello. En muchos casos se ha pagado a terceros para que las mantengan y administren. De hecho, una de las conclusiones que se puede extraer de lo observado en este último año es que, al igual que ha ocurrido con las fuerzas militares, las fuerzas ciber empleadas por Rusia en esta invasión no han sido siempre propias. En muchos casos el gobierno ruso ha financiado a mafias y cibercriminales para que llevaran a cabo las diferentes operaciones como mercenarios, aprovechando para ello los conocimientos que tenían de su actividad tradicional antes de la guerra. Es el caso de diferentes mafias de *ransomware* o de propietarios de *botnets*. Incluso ha habido grupos que han apoyado estas campañas por motivos ideológicos, sin necesidad de un incentivo económico significativo.

Tercera ola de ataques dirigidos

En los últimos meses se ha observado un creciente número de ataques dirigidos a altos cargos del gobierno de Ucrania y de su ejército, así como de diferentes países miembros de la OTAN. Este tipo de ataques suelen intentar recabar información sensible sobre movimientos de tropas, estrategia militar, aprovisionamiento de bienes de primera necesidad y armamento, etc.

Prácticamente en todos los casos se ha tratado de ataques de *spear-phishing*, es decir, basados en emails ilegítimos construidos con mucho cuidado para que no levanten sospechas en sus víctimas y sean percibidos como legítimos y de confianza. Cuando estos ataques han tenido éxito, las credenciales de acceso de las víctimas se han visto comprometidas y esto ha permitido a los adversarios tener acceso a recursos críticos, casi siempre, datos.

Estos datos no siempre han estado relacionados con la recolección de inteligencia militar, en ocasiones, han sido utilizados en campañas de desprestigio tanto en Ucrania como en otros países aliados. Estas operaciones de *hack-and-leak* suelen filtrar información sobre las bajas entre los combatientes ucranianos, las dudas de los diferentes gobiernos a la hora de enviar armamento a Ucrania, las discusiones internas acerca de estrategia

militar o negociaciones de paz, etc.

Otros patrones de ataque

Además de los ataques ya mencionados, se han observado otros que merece la pena mencionar por su novedad o sofisticación, casi todos ellos relacionados con las infraestructuras de telecomunicaciones. El primero fue el ataque a Viasat una hora antes de que comenzara la invasión. Se trata de una compañía estadounidense en la que confiaba el ejército ucraniano para disponer de enlaces de comunicación vía satélite. El ejército ruso empleó un *malware* denominado AcidRain para inutilizar completamente miles de terminales de comunicaciones de la red KA-SAT, tanto *routers* como *módems*. Este ataque afectó también a otras infraestructuras europeas, por ejemplo, a turbinas de generación de energía eólica.

> Diferentes analistas han predicho que en este año 2023 se observará una escalada en los ciberataques llevados a cabo por Rusia

El segundo se está repitiendo mucho en los últimos meses y se basa en el secuestro de sesiones BGP (*Border Gateway Protocol*). Este tipo de ataques permiten pervertir el uso de los protocolos de enrutamiento en los que se basa Internet, de manera que se consiga que los enrutadores escojan para el tráfico de red rutas maliciosas que atraviesen dispositivos controlados por el atacante. Esto le permite espiar el tráfico o directamente, eliminarlo y provocar así denegaciones de servicio. Se calcula que alrededor del 15% de la infraestructura de Internet se ha destruido en Ucrania por culpa del conflicto bélico y este hecho también facilita a los atacantes rusos redirigir el tráfico a través de su propia infraestructura.

Conclusiones

En estos momentos muchos aspectos de todos estos ataques, y de otros que no se han hecho públicos, son desconocidos para el público general. Pero parece que Ucrania y sus aliados (tanto gobiernos de naciones de la OTAN como grandes empresas tecnológicas, casi siempre estadounidenses) han sido capaces de defender sus infraestructuras mejor de lo que se esperaba inicialmente. O al menos, han sido capaces de responder y recuperarse en plazos razonables que han evitado impactos catastróficos en la mayor parte de los casos. Hay que recordar que, por desgracia, Ucrania ya tenía años de experiencia como víctima de los ciberataques rusos.

Diferentes analistas han predicho que en este año 2023 se observará una escalada en los ciberataques llevados a cabo por Rusia, tanto en número como en alcance y en víctimas potenciales. Por ejemplo, pueden ser una herramienta muy potente para llegar a zonas de Ucrania que ahora mismo están lejos del conflicto bélico tradicional, en un momento en el que parece que las fuerzas rusas están estancadas en el este del país. También pueden ser coordinados con ataques tradicionales en forma de amenaza híbrida, algo que hasta el momento apenas se ha observado (sólo al comienzo de la invasión con AcidRain), probablemente porque el mismo ejército ruso no había tenido tiempo suficiente para planificar la invasión.

Es decir, las previsiones avanzan que el impacto de los ciberataques en las operaciones militares será mayor de aquí en adelante, dado que las fuerzas rusas han tenido tiempo de organizarse y de planificar sus

siguientes pasos. Pero tendremos que esperar para ver si esto se confirma, porque las capacidades reales del ejército ruso en el ámbito ciber son hoy en día una incógnita, así como su voluntad real de escalar el conflicto de manera intencionada, o no intencionada, a infraestructuras fuera de la frontera de Ucrania.

Geers, K./ NATO Cooperative Cyber Defence Centre of Excellence – CCDCOE: «Cyber war in perspective: Russian aggression against Ukraine», 2015. Disponible en: https://ccdcoe.org/uploads/2018/10/CyberWarinPerspective_full_book.pdf

Google's Threat Analysis Group (TAG) y Mandiant: «Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape», 2023. Disponible en: https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/

Lin, H.: «Russian Cyber Operations in the Invasion of Ukraine» en *The Cyber Defense Review,* 2022. Disponible en: https://www.jstor.org/stable/48703290

Watts, C.: «Is Russia regrouping for renewed cyberwar?» en *Microsoft On the Issues,* 2023. Disponible en: https://blogs.microsoft.com/on-the-issues/2023/03/15/russia-ukraine-cyberwarfare-threat-intelligence-center/