Texto
R. Contreras

LA INVASIÓN RUSA DE UCRANIA DESATA UNA OLA DE ATAQUES SIN PRECEDENTES

La ciberguerra **muestra sus fauces**

Es como ese lago plácido en el que los cisnes se deslizan por sus tranquilas aguas, pero por debajo sus palmas patalean en un espacio turbio de lodo y remolinos violentos. Así, la ciberguerra ha ido operando bajo el desconocimiento de la inmensa mayoría, bajo una aparente calma chicha, saboteando centrales nucleares, tumbando estructuras críticas, colapsando países… Desde 2013, justo antes de la anexión rusa de Crimea, el conocido grupo Gamaredon viene dirigiendo sus campañas contra funcionarios y organizaciones del gobierno ucraniano. En diciembre de 2015, se produce un ataque sobre la empresa UKranian Kyivoblenergo que provoca un corte de suministro para más de 225.000 clientes entre una y seis horas en un crudo invierno. En junio de 2017, un malware genera fallos de funcionamiento generalizados en todo tipo de empresas e instituciones ucranianas, incluyendo bancos, ministerios, diarios y empresas de electricidad.

Ray Canzanese, director de Netskope Threat Labs, es conocedor de esta larga carrera de sabotajes: "Esta ciberguerra entre ambos países ya se estaba librando desde mucho antes, incluso años, como parte del conflicto geopolítico en Ucrania. Ya en enero de 2022, Netskope Threat Labs monitorizó diversas campañas de malware, entre ellas la de WhisperGate, que borraba archivos y corrompía discos de los sistemas ucranianos".

Los wipers o borradores de información

Los anteriores wipers rusos -hubo al menos tres, dirigidos a sistemas en Ucrania desde enero- no iban acompañados de este software adicional diseñado para propagarlos de forma autónoma. Un malware con estas características de 'gusano' estuvo detrás del devastador ataque NotPetya en 2017, el ciberataque más dañino de la historia.

Atribuido al Estado ruso, NotPetya infligió daños por valor de miles de millones de dólares a empresas como Maersk, FedEx e incluso Rosneft, la compañía petrolera rusa, aunque su objetivo era Ucrania. "Y es que todos los expertos en ciberseguridad coincidimos en que Rusia se está preparando para el próximo NotPetya", puntualiza el experto Ray Canzanese.

Con relación a los tres ataques encadenados (HermeticWiper, IsaacWiper, CaddyWiper), Josep Albors, Awareness & Research de ESET España, comenta que "es algo sin precedentes en la historia relacionada con los ciberataques en Ucrania que venimos analizando desde hace años. CaddyWiper tan solo sería el último de una serie de ciberataques que se han dedicado a atacar a objetivos de todo tipo durante los últimos ocho años, incluyendo ataques a centrales de distribución eléctrica en 2015 (BlackEnergy) y 2016 (Industroyer) o el conocido incidente provocado por NotPetya en 2017".

Comienzan las hostilidades

Todo estaba preparado para entrar en campaña; mientras los rusos engrasaban su maquinaria bélica, grupos de cibercriminales, amparados por el estado, se lanzaron a desbaratar las defensas ucranianas, bloqueando sus ministerios más estratégicos (Defensa, Interior, Gabinete de Ministros…) con ataques masivos de DDoS, dejando paralizados sus accesos durante unas horas.

Los informes de Estados Unidos apuntan a la GRU (Glávnoye Razvédyvatelnoye Upravlenie) como principal orquestadora de los ataques. Esta legendaria agencia de inteligencia (fundada por Trosky en 1918) estaría vinculada con el hackeo electoral de Estados Unidos y con otras operaciones en el extranjero. Gabriel Zurdo, CEO de BTR, explica la conexión existente entre la agencia y UNC1151, "un grupo vinculado a los servicios especiales de la República de Bielorrusia, también conocido como Ghostwriter y supuestamente responsable del espionaje directo y la obtención de información confidencial para disidentes, medios de comunicación y periodistas bielorrusos e igual situación en relación a las elecciones en Alemania".

A Sandworm, otro grupo que amenaza históricamente a Ucrania, le atribuyen los ciberataques a los Juegos Olímpicos de invierno de 2018.

Lo que parecía ser un paseo militar no lo fue, de la misma manera tampoco fueron los ciberataques propiciados desde las líneas rusas. Y los invasores no valoraron lo suficiente que su víctima propiciatoria estaba versada en estas lides virtuales y contaba, además, del respaldo estadounidense, con el apoyo de la comunidad internacional de hackers, que inmediatamente lanzaron una cruzada contra Putin con Anonymous como el principal abanderado.

<< En 2016, Obama declaró el ciberespacio como el cuarto escenario de guerra tras aire, mar y tierra. Con la caída del muro de Berlín y el auge de Internet, la guerra fría se sumergió en las procelosas aguas de la Dark Web. Desde entonces, se viene produciendo una guerra larvada, que se ha disparado con la invasión rusa.

A las ciberbarricadas

Los hackers se organizaron en Telegram bajo el nombre de 'Ejército de Ucrania' y se calcula que son más de 300.000 los que se han unido a la causa en respuesta al llamamiento de auxilio que realizó, a través de Twitter, Mykhailo Fedorov, viceprimer ministro del país y ministro de transformación digital de Ucrania.

Esta confederación espontánea asegura haber tumbado la web del Kremlin, publicando eslóganes contra la guerra en las páginas de inicio de medios de comunicación rusos y revelado información obtenida de grupos de piratería rivales.

Anonymous está implicado en la violación de Rosneft Deutschland, subsidiaria alemana de la matriz energética rusa que mostró su oposición a represalias contra la invasión, y que supuso el robo de 20 terabytes de datos. Anonymous también se atribuye la responsabilidad de ataques contra organizaciones rusas en los últimos días, incluso contra la televisión estatal y los servicios de transmisión con el fin de mostrar imágenes reales del conflicto a los ciudadanos rusos.

Con gran alcance mediático, el grupo TheAnonleaks, afiliado a Anonymous, logró hackear el Sistema de Identificación Automática (AIS) del yate de lujo de Putin, haciendo creer que se había estrellado en Ucrania y cambiando su destino a posteriori. Otro grupo de hackers afiliado a Anonymous logró el 1 de marzo deshabilitar el centro de control de la Agencia Espacial Rusa Roscosmos.

Sin embargo, este movimiento no es tan positivo como pueda parecer a primera vista, funcionarios de seguridad europeos denuncian que se han difuminado las líneas entre los hackers patrocinados por

LOS PRIMEROS NUEVE DÍAS DE CIBERCAMPAÑA

23 de febrero

- Se desata una ola de ataques DDoS contra varios Ministerios estratégicos ucranianos, como el de Defensa y el de Interior.
- ESET detecta un nuevo wiper (Hermetic Wiper, borrador de sistemas) que afecta a grupos financieros ucranianos.

24 de febrero

- El mismo día de la invasión, el Gabinete de Ministros de Ucrania permanece inaccesible durante varias horas.

25 de febrero

- Anonymous declara la guerra al gobierno ruso hackeando el yate de Vladimir Putin; el grupo Conti reacciona poco después mostrando su "pleno apoyo al gobierno ruso".
- Grupos de hackers organizados (cyberpartisans) tumban webs del gobierno ruso.

26 de febrero

- El ministro de Transformación Digital hace un llamamiento global a los expertos cibernéticos para unirse a su ejército virtual ucraniano.

27 de febrero

- El grupo de ransomware Lockbit 2.0. asegura desde la dark web que nunca atacará la infraestructura crítica de ningún país.

28 de febrero

- Partidarios hacktivistas de Ucrania hackearon estaciones de recarga de coches eléctricos para mostrar mensajes ofensivos contra el presidente Putin.

1 de marzo

- Grupo afín a Bielorrusia trata de causar el caos entre los refugiados ucranianos, utilizando el malware Sunseed.
- El grupo TheAnonleaks deshabilita el centro de control de la Agencia Espacial Rusa Roscosmos.

2 de marzo

- Medios de comunicación españoles sufren una oleada de ataques de malware proveniente de grupos rusos, revela Iberlayer.

3 de marzo

- Proofpoint identifica a un grupo de hackers alineados con China que ha intensificado su actividad contra entidades en Europa.

el estado y los aficionados patrióticos, por lo que resulta complejo determinar a los gobiernos qué grupo es el agresor y cómo responder. Participar en ataques cibernéticos desde suelo estadounidense o británico podría contravenir la ley de fraude y abuso informático o la ley de uso indebido de ordenadores, y constituir pena de cárcel.

Hasta la fecha, el gobierno ucraniano no ha salido mal parado frente a la ofensiva de sus vecinos. Los ataques DDoS y las operaciones 'limpiaparabrisas' no han surtido el efecto esperado por sus agresores y parece que las barreras de contención están siendo suficientes. No obstante, los ataques arrecian como demuestra Check Point en el siguiente balance: "En los tres primeros días de combate, aumentaron un asombroso 196%, con el Gobierno y el sector militar de Ucrania como objetivos. A partir de esa fecha, las ofensivas disminuyeron, reduciéndose un 50% en los últimos 7 días. Sin embargo, las amenazas a todas las industrias, no solo al sector gubernamental/militar, en Ucrania y Rusia, han aumentado hasta alcanzar el punto más alto desde el inicio del conflicto y 2022".

¿Internacionalización de la ciberguerra?

El riesgo añadido de toda conflagración es que salte las fronteras, y en la ciberguerra nunca se puede hablar de líneas de separación. Expertos de Proofpoint han captado un aumento de movimiento que afecta tanto a particulares como a empresas. Tras el inicio de la guerra la procedencia de direcciones IP de China se ha incrementado un 116% en los países de la OTAN y un 72% en todo el mundo, si bien resulta imposible atribuir los ciberataques a entidades chinas. Los ciberataques desde IP chinas a España fueron un 120% mayor que antes de la invasión, y un 124% mayor que las tres primeras semanas del conflicto.

En la misma tesitura, Iberlayer ha dado a conocer la fuerte campaña de malware proveniente de grupos de ciberdelincuentes rusos y dirigida a los principales grupos de comunicación españoles, tanto de prensa escrita, radio y televisión.

La verdad es la gran víctima

El senador de EEUU Hiram Johnson acuñó la famosa sentencia: "La primera víctima cuando llega la guerra es la verdad", y en este campo de batalla virtual se cumple el axioma. La desinformación ha sido una baza jugada con gran habilidad por las autoridades rusas maestras en el arte de las fakes news, que han convencido a la población que su país estaba amenazado por los países de la OTAN y que la incursión se circunscribe a la zona del Donbass. Para combatir toda esta sarta de infundios, la UE ha prohibido cualquier información de los medios estatales rusos Sputnik y Russia Today, por considerarlos "parte de la maquinaria de guerra rusa", medida muy discutida por los defensores de la libertad de expresión.

Y es que la censura es parte de este juego macabro. El regulador de telecomunicaciones Roskomnadzor ha vetado el servicio Google News en el país, acusando a la plataforma de difundir noticias falsas, proporcionando artículos y materiales con información inexacta sobre la "operación especial en Ucrania". La difusión de noticias falsas sobre la actividad militar se castiga con hasta 15 años de prisión según una nueva ley firmada por Putin. Rusia ya bloqueó a Meta, Instagram y Twitter como medidas quirúrgicas. Un tribunal acusó a Meta de "extremista" comparándolo con el Estado Talibán. Es difícil que la verdad pueda florecer en estas circunstancias tan complicadas; aunque anecdótico, puede ser un rayo de esperanza el hecho de que nada más anunciarse el cierre de Google News, muchos rusos se apresuraron a descargarse masivamente la Wikipedia por temor a que el operador Roskomnadzor cumpliera con sus amenazas de cerrar la enciclopedia online. ■

VÍCTOR GAYOSO, INVESTIGADOR EN EL ITEFI DEL CESIC

¿Vamos hacia un modelo de guerra híbrida, con diversos flancos invisibles?

El término 'guerra híbrida' hace referencia al hecho de que, en las guerras del siglo XXI, aparecen combinadas una componente militar y una componente menos visible pero también importante, las acciones a través de Internet. Estas acciones tienen un objetivo múltiple, incluyendo la obtención de información militar que pueda ser utilizada en el conflicto como planes de batalla o logísticos, recabar datos que puedan ser utilizados para desacreditar al enemigo (por ejemplo, datos asociados al número de víctimas civiles causadas por el bando contrario), generar información falsa para desestabilizar al enemigo provocando que el apoyo de sus ciudadanos al conflicto disminuya o finalmente la realización de ataques que bloqueen o destruyan algunos sistemas críticos del país (red eléctrica, sistema bancario, medios de comunicación, etc.). Dada la ubicuidad de la tecnología y más concretamente de Internet en nuestras vidas, es de esperar que esta componente de la guerra híbrida cobre cada vez más importancia, y precisamente por ello países como Rusia están intentando aislarse en Internet, lo que por otra parte genera muchas preguntas sobre la legitimidad o conveniencia para los propios ciudadanos de tomar medidas de este tipo.