El número de ciberataques ha crecido en todo el mundo durante el conflicto

El ciberespacio, otro campo de batalla

La invasión de Rusia a Ucrania ha tenido en paralelo a la contienda física otra en el espacio digital, que persigue inutilizar los sistemas y causar daños tanto en la operativa de las instituciones como de las empresas con el fin de paralizar Ucrania, influir en la opinión pública y destruir activos importantes. Los principales especialistas en seguridad han analizado este combate digital, las implicaciones que puede tener en nuestro país y cómo se pueden proteger tanto las entidades públicas como las empresas y ciudadanos.

Rosa Martín

El pasado 24 de febrero comenzó la invasión de Rusia a Ucrania y en paralelo se incrementó el número de ataques contra sitios del Gobierno ucraniano y otros organismos. La División de Inteligencia de Amenazas de Check Point Software Technologies, Check Point Research, detectó en los primeros tres días de la contienda un incremento de los ciberataques contra el Gobierno y el sector militar de Ucrania de un 196 %, frente al 4 % en los ataques a organizaciones rusas. Estos datos indican que la denominada "ciberguerra" es un factor que puede desestabilizar e inclinar la balanza para ganar la contienda. Los ciberataques que se han detectado se pueden dividir en función del atacante. Uno de ellos son los ataques del tipo APT (amenazas persistentes avanzadas), que tratan de conseguir ventajas a través del espionaje o sabotaje. Los actores de este tipo de amenazas tienen muchos recursos, conocimientos y actuarían como complemento al mundo real. "Los actores de amenazas Gamareddon, Cyclops Blink o PandoraBlade serían un claro ejemplo en este contexto, ya que se detectó un incremento significativo de su actividad coincidiendo con el desarrollo de la invasión", explica Dani Creu, analista de Seguridad en el GReAT (Equipo de Investigación y Análisis Global) de Kaspersky.

Wiper y otros ataques

Uno de los ataques principales registrados durante el conflicto es el del tipo Wiper, que consiste en *malware* específico para borrar datos e inutilizar sistemas. Borja Pérez, *country manager* de StormShield Iberia, señala que HermeticWiper se ha usado contra distintos organismos gubernamentales ucranianos como el Ministerio de Asuntos Exteriores o la Rada (su Parlamento). "Este *malware*, distribuido por GPO y dirigido contra el ordenador de la víctima, secuestra un *driver* legítimo de partición de disco para corromper particiones del sistema y ocasionar la pérdida de datos en la estación de trabajo o servidor. El objetivo es claro: la destrucción de datos", indica el directivo. Este *malware* tiene otra variante, llamada CaddyWiper, que intenta primero sobrescribir los datos de todos los directorios de usuario en todos los discos.

CrowdStrike Intelligence también ha detectado ataques por los actores VOODDOO BEAR y EMBER BEAR. A este último se le ha vinculado a ataques WhisperGate Wiper, mientras que al primero a una variedad de operaciones de alto perfil asociado al GRU (Departamento Centro de Inteligencia Ruso).

"Hemos visto también una convergencia entre los cibercriminales y los atacantes patrocinados por el estado. Este tipo de amenaza híbrida es algo que hemos observado en el pasado y que nuevamente se ha visto a lo largo del conflicto, multiplicando por tanto las capacidades de Rusia para realizar ciberataques tanto a Ucrania como a los países de la OTAN", confirma Miguel de Castro, de CrowdStrike.

Otro tipo de ataques son los efectuados por los grupos de cibercriminales, que suelen buscar un beneficio económico, que han puesto su conocimiento y herramientas a disposición de la fuerza militar. Y, además, se han visto otros ataques efectuados por grupos de *hacktivistas*, que se han posicionado a favor de Ucrania principalmente. Según apunta Nick Biassini, jefe de Divulgación en Cisco Talos, ha aumentado la participación de los *"cibervigilantes"* y otros actores que lanzan ataques a ambos lados del conflicto. "Esto ha suscitado una gran preocupación, ya que los atacantes con pocos conocimentos pueden inutilizar involuntariamente piezas claves de la infraestructura ucraniana".

"Desde CrowdStrike Intelligence se han observado ataques por parte de grupos patrocinados por el estado-nación de tipo destructivo tanto de despliegue de Wiper —*malware* específico que borra datos e inutiliza sistemas—como de ataques de denegación de servicio distribuido o también ataques de *defacement*, que modifican el contenido de páginas web y ataques a sistemas para obtener datos", detalla Miguel de Castro, ingeniero de ventas en CrowdStrike.

> Los ataques de denegación de servicio han sido frecuentes

Los expertos coinciden en señalar que los ataques de denegación de servicio han sido frecuentes, aunque han sido un "arma" habitual desde hace tiempo. John Shier, asesor senior de Seguridad en Sophos, ha señalado que "a pesar de que atribuir la autoría de los ataques DDoS es casi imposible por diseño, varias investigaciones han atribuido este tipo de ataques a actores vinculados con Rusia desde hace bastante tiempo y, al menos desde 2007, ha sido un *modus operandi* habitual".

Una opinión similar mantiene Ramiro Céspedes, *Threat Intelligence Enginieer* de Threat-

España, ¿objetivo?

Los especialistas opinan que nuestro país no es un objetivo prioritario en este conflicto digital, pero al formar parte de la Unión Europea, que está apoyando a Ucrania, podría ser atacada. Sergio Bravo, de Bitdefender, indica que el riesgo de sufrir un ataque no es el mismo en todas las organizaciones y depende de la relación con Ucrania.

Actualmente no existe un registro oficial de campañas dirigidas de grupos pro-rusos contra España, pero sí que se han tomado algunas medidas, según les consta a los expertos. "En el ciberespacio no hay límites o fronteras por lo que una herramienta que fue diseñada para realizar un ataque a Ucrania podría ser utilizada contra España", argumenta el *Threat Intelingence engineer* de ThreatQuotient.

Albors, de ESET, recalca que nuestro país cuenta con un Centro Nacional de Protección de Infraestructuras Críticas, un Centro Criptológico Nacional, INCIBE y distintos CERT profesionales que velan por la seguridad de las empresas tanto públicas como privadas. "Esto no significa que no seamos vulnerables, pero las puntuaciones obtenidas en las pruebas que realiza el índice de ciberseguridad global nos deja en los primeros puestos. El principal problema se encuentra en que no se destinan los suficientes recursos para detectar y bloquear ataques comunes que pueden ser evitados aplicando medidas de seguridad básicas".

Quotient, quien señala que el gobierno ruso lleva años financiando y patrocinando de manera directa e indirecta a múltiples agrupaciones que llevan adelante operaciones en el ciberespacio. El gobierno ucraniano también reaccionó durante los primeros días solicitando la participación de voluntarios para formar un ciberejército. "Los principales ataques llevados a cabo por este grupo han sido ataques de denegación de servicio (DDoS) contra sitios web del gobierno de Rusia y contra desarrolladores rusos en plataformas como GitHub. Las acciones de este grupo han estado más enfocadas en el volumen que en la precisión, pero aun así han logrado comprometer diferentes activos del gobierno ruso", añade.

Para Josep Albors, director de investigación y concienciación de ESET España, también han

sido relevantes los ataques dirigidos a infraestructuras críticas como los ISP y las conexiones satelitales.

Miguel Ángel Fañanás, director de Europa Occidental en VU, cree que la contienda está desarrollando nuevas tácticas de ingeniería social, por lo que el panorama de los ataques está cambiando constantemente, aunque señala que en gran parte "apuntan a impactar el marco de la desinformación, teniendo el foco en los medios de noticias oficialistas de cada país".

Ataques más peligrosos

A la hora de determinar qué tipo de ataques son más peligrosos, los especialistas señalan que son los que consiguen sus objetivos. Para Sergio Bravo, *Iberia sales director* de Bitdefender, el Wiper es uno de los más dañinos porque "el cifrado de datos resulta irreversible". A su juicio, estos ataques están diseñados para causar el mayor daño posible, suelen ser oportunistas y no están dirigidos con precisión.

> "Todos los ataques dirigidos con estrategia son dañinos"

David Sancho, investigador senior de Amenazas y responsable del Equipo de Investigación de Trend Micro, opina que los ataques de DDoS y los de alteración de contenidos o "*defacement*" son los que crean más daño a corto plazo y se pueden hacer sin grandes conocimientos técnicos. "Son fáciles de realizar y difíciles de prevenir", resalta.

Mario García, director general de Check Point Software para España y Portugal, indica que "hablar de peligrosidad en ataques es muy relativo. Todos lo son. Dependiendo de la importancia del objetivo, en un momento puede

ser devastador y ocasionar muchos problemas directos e indirectos. Todos los ataques dirigidos con estrategia son dañinos".

Los expertos consideran también que los ataques a las infraestructuras críticas son especialmente dañinos; aunque hay que tener en cuenta que todos los ataques pueden tener distintas consecuencias. "La cuestión es que muchos ataques pueden llevar factores externos y efectos derivados más allá de la víctima original. Cada ataque exitoso puede suponer un riesgo secundario que no es obvio al principio. Afortunadamente, no todos los ataques tendrán consecuencias peligrosas, pero eso no significa que debamos ser benévolos con ellos", recalca Shier, de Sophos.

Céspedes, de TreatQuotient, apunta que otro tipo de ataques con importante repercusión son los de la desinformación porque "pueden infligir un serio daño en la moral de las tropas y ciudadanos de ambos bandos y podrían tener un impacto político muy alto".

Sector público y empresas

En este panorama de ciberataques los organismos del sector público y las empresas están en el punto de mira de los atacantes, pero el nivel de preparación para combatir estas amenazas no es siempre el adecuado y va unido al presupuesto de seguridad, según señalan los especialistas en ciberseguridad.

> "La seguridad es una inversióny no un gasto"

El Security Report 2022 de Check Point Software señala que los ciberataques a servicios públicos se incrementaron un 46 % en 2021, en comparación con 2020, registrándose 736 amenazas semanales por organización dentro de los servicios públicos a nivel mundial. Estos datos revelan que es necesario articular estrategias de seguridad y ser proactivos para combatir estas amenazas.

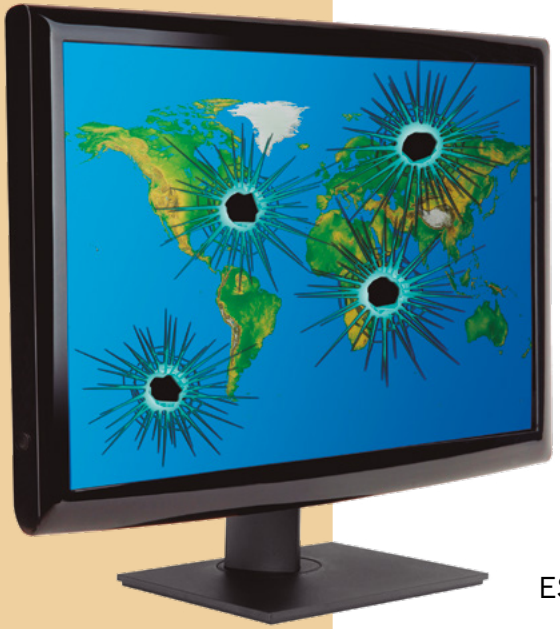
Los especialistas coinciden en señalar que mantenerse a salvo de un ataque es prácticamente imposible, pero que siempre hay que tomar medidas para dificultar estos ataques. "Detrás de cada amenaza siempre existe un humano y el conocimiento de sus intenciones, motivaciones, capacidades e infraestructura que aporta la inteligencia de amenazas es la única forma para tratar de ir un paso por delante de los atacantes", insiste Miguel de Castro, de CrodwStrike.

Biasini, de Cisco Talos, añade que, con independencia de la situación actual, "los sistemas heredados, la mala higiene de la ciberseguridad y el software obsoleto pueden tener impactos catastróficos en cualquier organización".

El analista de Seguridad en el GReAT de Kasperksy indica también que hay que considerar que la seguridad debe "considerarse como un proceso y no como un estado". Y, al mismo tiempo, destaca que "la seguridad es una inversión y no un gasto". Los especia-

Consejos de seguridad para el ciudadano

Los ciudadanos pueden ser víctimas de ciberdelincuentes que pueden aprovecharse de su solidaridad con los refugiados y los afectados por el conflicto mediante campañas de *phishing* y otras extorsiones. Los especialistas en ciberseguridad aconsejan estar alerta y mantener unas buenas prácticas para evitar caer en estafas. No se deben abrir correos de usuarios desconocidos, ni hacer clic en enlaces adjuntos y, por supuesto, no se tienen que facilitar datos a través de estos canales. Es recomendable contar con contraseñas robustas que combinen los números con las mayúsculas y los símbolos; y además cambiarlas cada cierto tiempo. Y, por supuesto, señalan que no es conveniente tomar parte en el conflicto participando en grupos de *hackers* porque posiblemente se estén cometiendo delitos graves.



listas creen que ahora es el mejor momento para que las empresas revisen sus planes de ciberseguridad, intensifiquen la búsqueda de vulnerabilidades, analicen sus accesos y registros, y elaboren un plan de crisis.

La recomendación de Cisco Talos es que las empresas y organizaciones con vínculos con Ucrania habiliten y examinen con cuidado sus registros, apliquen parches y, además de diseñar un plan de crisis, habiliten la autenticación multifactor.

Sophos también indica que es aconsejable monitorizar cualquier movimiento inusual en las redes a medida que avanza el conflicto, mientras que Check Point Software considera que, además de contar con un buen software de protección y de hacer *backup* de forma periódica, es imprescindible dar una formación en ciberseguridad a los empleados para que sean la primera barrera ante cualquier incidente.

Para ThreatQuotient las empresas deberían contar con un responsable de la estrategia de ciberseguridad y mejorar los sueldos de los especialistas para captar y retener talento en este apartado.

ESET recalca que es imprescindible, además de aplicar las medidas de seguridad consideradas básicas desde hace tiempo, realizar auditorías constantes para detectar posibles agujeros y solucionarlos a tiempo.

Bitdefender añade un consejo más: la revisión de la guía Shields UP, elaborada por la CISA (Agencia de Seguridad de Infraestructura y Ciberseguridad en Estados Unidos).