Nº3 El papel de los ciberataques en la guerra de Ucrania

"Soy perfectamente consciente de que si Rusia, como estado-nación, decidiera atacar las infraestructuras nacionales norteamericanas, incluyendo aquella de la que soy responsable, no tendría muchas posibilidades de pararla.

¿El gran estado-nación, Rusia, contra Peter? Pierdo seguro."

Peter Fletcher
CISO San José Water Company [1]

1. ¿Ciberguerra?

Pero ¿estamos en el escenario de ciberguerra que describe Peter Fletcher? Probablemente (todavía) no. Según diversos analistas, **el Kremlin ha evitado hasta ahora los ciberataques a los Estados Unidos y otros países de la OTAN por miedo a posibles represalias** amparadas por la legalidad internacional ya que, según el Manual de Tallinn [2], un documento académico creado a instancias de la OTAN que detalla cómo se aplica el derecho internacional en caso de guerra cibernética, un estado atacado podría legalmente defenderse de dichos ataques y lanzar diferentes tipos de contraataques incluyendo el uso de "represalias cinéticas", es decir bombas.

Lo cual trae a colación esa borrosa frontera entre la "ciberdelincuencia" o recibir "ciberataques" y la "ciberguerra" propiamente dicha. En cualquier caso, los recursos de las compañías y los de los Estados que las acogen deben estar en continua colaboración, pero, sin duda, en el caso de guerra, del tipo que sea, los Estados deben tomar el liderazgo.

La Rusia de Vladimir Putin ha demostrado una y otra vez que no tiene reparos en atacar infraestructuras críticas y causar considerables daños colaterales mediante actos de ciberagresión, por lo que no es difícil imaginar que un ciberataque a gran escala contra instituciones financieras o cualquier otra infraestructura crítica en países de la OTAN esté a la vuelta de la esquina. Y que esto termine en una escalada que arrastre a una tercera guerra mundial.

El propio Centro Nacional de Inteligencia (CNI), [3], está **alertando de la posibilidad de que "en los próximos días" grupos de hackers asociados a los servicios de inteligencia rusos lancen ataques cibernéticos contra objetivos españoles**. Por ello Margarita Robles, ministra de Defensa, ha aumentado el nivel de alerta cibernética a tres (sobre cinco), tras detectar un incremento de la actividad procedente de Rusia al inicio de la invasión de Ucrania y ha creado un comité de ciberseguridad dirigido por el Centro Criptológico Nacional bajo el paraguas del Comité de Crisis activado en la Moncloa a raíz de la guerra.

Un ejemplo de esta urgencia es la aprobación de las medidas para garantizar la ciberseguridad de las redes 5G, que el Gobierno decidió aprobar el pasado 5 de abril mediante la fórmula de Real Decreto-ley como consecuencia de la guerra en Ucrania en vez de mediante la vía de Proyecto de Ley, como estaba contemplado inicialmente.

Javier Candau, Jefe del Departamento de ciberseguridad del Centro Criptológico Nacional, con quien nos hemos puesto en contacto para la redacción de este boletín, nos comenta:

"Aunque las tensiones entre Rusia y Ucrania tienen altos y bajos, se recomienda a las empresas que no relajen su nivel de alerta ya que el conflicto en el ciberespacio podría abrirse a los países de la OTAN en cualquier momento.

Sigue existiendo la posibilidad real de que el Gobierno de Rusia patrocine directamente un ciberataque destructivo contra el gobierno, infraestructuras críticas o empresas de sectores estratégicos en España."

Nº3 El papel de los ciberataques en la guerra de Ucrania

Según el informe detallado en [4], se contemplan tres supuestos de ciberataque de gravedad incremental [también desarrollado en 5]:

a) Ataque directo a la soberanía de un país de la OTAN, por ejemplo, a una infraestructura digital militar pero también a una red eléctrica nacional u otra infraestructura crítica.

b) Agresión cibernética que impida que el país actúe legal y libremente en la escena internacional: interferencia en los derechos de voto dentro de la Alianza o en el despliegue de tropas en la Europa del Este.

c) Ataque que ocasione daños físicos o personales incluyendo la muerte de personas. Eso igualaría la gravedad del atentado al del uso de armas cinéticas y, por lo tanto, activaría el artículo 5 de la Alianza Atlántica por el que sus miembros deberían acudir en defensa del país atacado con todo tipo de medios a su alcance.

2. Contexto

En las primeras semanas de un año marcado por el conflicto militar con Rusia, **Ucrania ha sufrido ya varios ciberataques dirigidos a infraestructuras críticas para el país**. En un escenario de fuerte tensión, con Joe Biden, presidente de Estados Unidos, y la OTAN advirtiendo sobre la inminencia de un ciberataque ruso, los analistas recuerdan la nutrida historia de ataques informáticos que ha sufrido Ucrania en los últimos años, sin evidencias de su autoría, pero con Rusia como principal sospechoso.

Sobre todo, **preocupan los paralelismos con el que está considerado el ataque cibernético más destructivo de la historia, NotPetya**. Dirigido por Rusia hacia Ucrania en 2017, que se expandió más allá de sus objetivos iniciales y provocó pérdidas por 10.000 millones de dólares, con impacto en el mundo entero.

Es fácil entender por qué Ucrania ha sido y es un objetivo atractivo para poner a prueba las capacidades de los ciberataques. El país tiene una infraestructura similar a la que se encuentra en Europa Occidental y América del Norte. Pero a diferencia de los Estados Unidos, el Reino Unido y la Unión Europea, Ucrania tiene recursos más limitados para contraatacar. Si bien Rusia es el sospechoso obvio, es posible que otros países, como Irán, Corea del Norte o China, también hayan estado probando sus propias armas cibernéticas en Ucrania.

Estos son algunos de los ataques que más temen los expertos:

- BlackEnergy: En 2015, la red eléctrica de Ucrania se vio interrumpida por un ciberataque llamado BlackEnergy, que causó un apagón a corto plazo para 80.000 clientes de una empresa de servicios públicos en el oeste de Ucrania. Casi exactamente un año después, otro ciberataque conocido como Industroyer dejó sin energía eléctrica durante aproximadamente una hora a casi una quinta parte de Kiev, la capital de Ucrania.
- NotPetya: Se cree que NotPetya es el ciberataque más costoso de la historia y las autoridades de EE.UU., Reino Unido y la UE culparon a un grupo de hackers militares rusos. El software destructivo se ocultó en una actualización de un popular software de contabilidad utilizado en Ucrania, pero se extendió por todo el mundo destruyendo los sistemas informáticos de miles de empresas y causando daños por aproximadamente 10.000 millones de dólares.
- Colonial Pipeline: En mayo de 2021 se declaró el estado de emergencia en varios estados de EE.UU. después de que un grupo de hackers causara el cierre del gasoducto Colonial Pipeline que transporta el 45% del suministro de gasolina y diésel de la costa este de EE.UU. lo cual desencadenó el pánico en las gasolineras. El ciberataque no fue obra de hackers del gobierno ruso, sino del grupo de ransomware DarkSide, que se cree que tiene su base de operaciones en Rusia. La empresa del gasoducto admitió haberles pagado a los criminales 4,4 millones de dólares en bitcoins, difíciles de rastrear, a cambio de volver a poner en funcionamiento los sistemas informáticos.

Nº3 El papel de los ciberataques en la guerra de Ucrania

3. Y empezó la guerra

La **mayoría de los escenarios simulados sobre una invasión rusa, planteaban una gran guerra híbrida** que comenzaría con ciberataques abrumadores que aniquilarían el acceso a internet, y tal vez la red eléctrica, en Ucrania. Hasta el momento, eso no ha ocurrido y está sorprendiendo la escasa actividad cibernética aparente que está sucediendo.

A finales del año pasado, Estados Unidos y Gran Bretaña enviaron expertos a Ucrania para ayudar a su gobierno a prepararse para este gran ataque cibernético que se creía sería la salva inicial de Vladimir Putin durante la invasión. Se dijo que la red eléctrica de Ucrania era un objetivo particularmente atractivo para los piratas informáticos rusos, quienes lograron hacerla caer por breves períodos dos veces antes.

Pero las cosas no sucedieron del modo esperado y Rusia invadió Ucrania a la antigua usanza. Hubo informes de un aumento en los ataques a sitios web ucranianos en los meses previos a la guerra, pero su impacto fue mínimo. Semanas después de los combates, la red eléctrica de Ucrania, sus sistemas de comunicaciones y otras infraestructuras críticas siguen funcionando en gran medida.

Entre otros problemas, los ciberataques son difíciles de apuntar y controlar, debido a la conectividad global de las redes informáticas. Un ataque viral dirigido a Ucrania podría escapar a sus vecinos de la OTAN, forzando un conflicto más amplio que Rusia podría querer evitar (Tallinn de nuevo). Las armas cibernéticas también son por naturaleza lentas y difíciles de usar. Es posible que los piratas informáticos deban pasar meses estudiando la infraestructura de un enemigo para poder atacarlo, pero el ataque puede desmoronarse en un instante si el enemigo descubre la intrusión.

El **primer ataque notificado en relación con la guerra tuvo lugar durante la noche del jueves 13 de enero** de 2022, cuando los ucranianos se encontraron muchas de las páginas web del Gobierno desfiguradas. Pero más allá de eso, y más discretamente, los atacantes habían insertado un programa destructivo dentro de los servidores de agencias ucranianas, una operación que fue descubierta por investigadores de Microsoft.

Este malware, conocido ahora como WhisperGate simulaba ser un ransomware, pero no había contraseña para recuperar nada. En realidad, **su objetivo era la destrucción de datos clave para dejar las máquinas inoperativas.** Expertos citados por el MIT Technology Review [6], señalaron que WhisperGate recuerda a NotPetya hasta en los procesos técnicos destructivos.

Un mes más tarde, **el 23 de febrero, el ministro de asuntos digitales del país confirmó otro ciberataque** con los mismos objetivos que el anterior: páginas web del Gobierno y bancos. Este ataque paralizó los sitios web del Gabinete de Ministros y de los ministerios de Energía, Deportes, Agricultura y Ecología. Aun así, las páginas web del Gobierno y del Ministerio de Defensa permanecieron en línea. El Ministro de Defensa ucraniano dijo en un tuit que habían recibido un volumen inusualmente alto de solicitudes para cargar la web, lo que sugiere que los atacantes estaban inundando los servidores con solicitudes ilegítimas en un intento de sobrecargarlos e impedir que los ciudadanos accedieran al sitio.

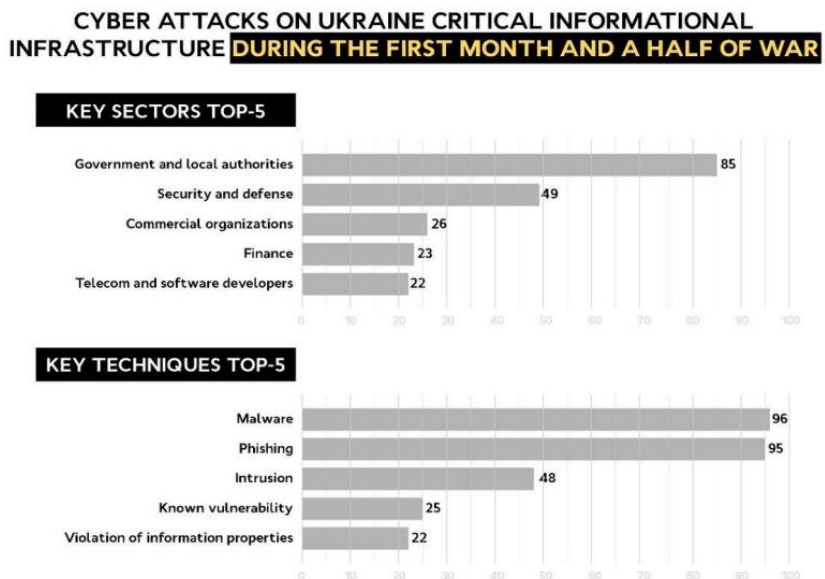

Figura 1. Sectores atacados y técnicas cibernéticas usadas contra Ucrania. Fuente: Gobierno de Ucrania

Estos últimos ciberataques en Ucrania tuvieron un impacto limitado. Fueron del tipo de denegación de servicio, DDoS (por sus siglas Distributed Denial of Service), una modalidad que consiste en dirigir una avalancha de peticiones simultáneas a un sitio web, lo que provoca que el servidor se bloquee o deje de funcionar en su intento de responder a más solicitudes de las que puede manejar, con lo que se impide el acceso a los usuarios legítimos.

Nº3 El papel de los ciberataques en la guerra de Ucrania

4. Máxima alerta

Durante años, Ucrania ha sido un campo de pruebas para los ciberataques rusos. Mientras las empresas y los países ven cómo avanza la guerra, deben prestar atención y **pensar en cómo prepararse si el conflicto se extiende fuera de las fronteras de Ucrania**. Algunos ciberataques, como los que van dirigidos a infraestructuras, pueden ser difíciles de prevenir, pero hay que estar en máxima alerta y tomar todas las medidas posibles.

A diferencia de los ataques convencionales, los ciberataques son difíciles de atribuir ya que en muchos casos se pueden lanzar desde un host involuntario. Por ejemplo, podrían tomar el control parcial de un ordenador particular, sin que el propietario lo supiera, y usarlo para iniciar una cadena de ciberataques. **Medidas simples, como tener una contraseña segura y no entrar en enlaces sospechosos, precauciones que, lamentablemente, en muchas ocasiones se pasan por alto, pueden ahorrar muchos problemas**.

El escenario actual de la ciberseguridad se caracteriza por las constantes oleadas de ciberataques de alta persistencia y sofisticación tecnológica, originados por atacantes que, además de los escenarios tradicionales, están explotando el crecimiento exponencial de la superficie de exposición que comporta el trabajo a distancia. En este sentido, el contexto de la guerra de Ucrania está siendo aprovechada por grupos cibercriminales para incrementar su actividad en todos los frentes.

De forma muy resumida, según el CCN-CERT [7], el modus operandi en muchas de las actuales campañas de distribución de malware puede resumirse en:

1. Fase de intrusión. Las principales vías de entrada que se están detectando por parte de los atacantes son el correo electrónico y los servicios no seguros expuestos. Habitualmente, en el caso del correo electrónico, se trata de correos dirigidos a una o varias víctimas con un documento malicioso adjunto o persuadiendo al usuario para que visite una web previamente comprometida. Una vez allí, una falsa actualización del navegador, la instalación de complementos o mecanismos similares logran la descarga de la primera etapa del malware.
2. Movimiento lateral. Una vez dentro de la organización, los atacantes buscan ganar persistencia y desactivar los sistemas de defensa. Asegurada la persistencia, la propagación del malware dentro de la organización se lleva a cabo utilizando diferentes tácticas/técnicas: explotando vulnerabilidades conocidas que ayuden al movimiento lateral del atacante, robando credenciales y creando nuevos usuarios de administración y deshabilitando cualquier sistema de protección implementado. El atacante puede estar mucho tiempo en esta fase y esperar al momento ideal para pasar a la siguiente y realizar la acción.
3. Explotación o colonización. Una vez obtenido el control sobre la infraestructura víctima y establecido contacto con su sistema de Comando y Control, el atacante envía las órdenes de descarga y detonación del malware elegido, o bien cualquier otro tipo de acción a realizar sobre la red o sistemas víctima: exfiltración de información, alteración o eliminación de datos, cifrado, etc.

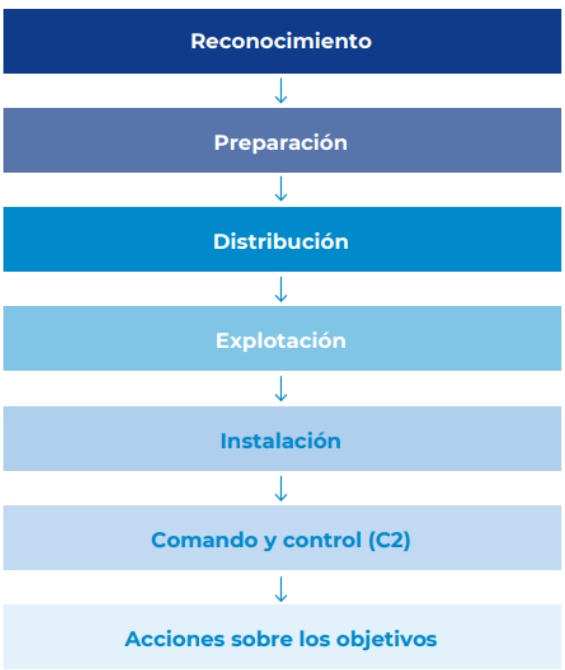

Figura 2. Ciclo de vida de la mayoría de las ciber amenazas. Fuente: Lockheed Martin, CCN-CERT [7]

Nº3 El papel de los ciberataques en la guerra de Ucrania

El necesario equilibrio entre la usabilidad y la seguridad en el uso de la tecnología y el manejo de información provoca que mantener un adecuado nivel de ciberseguridad en las organizaciones requiera una adecuada implicación de las personas.

Para lograr dicho objetivo, **resulta necesario la existencia y actualización de un plan estratégico de mejora del nivel de la cultura en ciberseguridad** que promueva los cambios en la conducta de las personas mediante la realización de acciones de concienciación y formación en ciberseguridad.

Además, prepararse para un ciberataque significa hacer todo lo posible para minimizar el daño potencial si el atacante consigue entra en nuestros sistemas. Esto incluye:

- Asegurarse de **que el software esté actualizado** en toda la organización y de que se hayan aplicado parches a las vulnerabilidades conocidas en versiones anteriores.
- **Tener un software antivirus** y de detección de malware eficaz.
- **Realizar copias de seguridad frecuentes** de los datos importantes, como documentos que solo se almacenan en un lugar, en caso de que se destruyan.

También vale la pena tomar medidas en su organización para minimizar el riesgo y prepararse para responder si ocurre lo peor. Esto incluye:

- **Buscar posibles vulnerabilidades en la cadena de suministro cibernética** y presionar a los proveedores de software de terceros para que prioricen la ciberseguridad.
- **Probar el plan de respuesta a incidentes**, incluyendo escenarios de ejecución y ejercicios de mesa, para asegurarse de que el plan sea sólido y que todos sepan lo que se supone que deben hacer en una crisis.

Por último, es importante remarcar que la interdependencia de nuestras empresas con aquellas que integran la cadena de suministros es cada vez más alta. La cantidad de productos y servicios que se contratan a terceros hacen que no podamos ignorar a nuestros proveedores en el análisis de los ciber riesgos que realizamos para nuestra organización.

REFERENCIAS

[1] THE NEW YORK TIMES. *US Says it secretly removed malware worldwide, pre-empting Russian cyberattacks. Kate Conger and David E. Sanger. 6 de Abril de 2022.* Link

[2] EL CONFIDENCIAL. *Cómo los hackers rusos pueden provocar la tercera guerra mundial. Jesús Díaz. 26 de marzo de 2022.* Link

[3] LA VANGUARDIA. *El CNI advierte que España es objetivo inminente de grupos de hackers rusos. 29 de marzo de 2022.* Link

[4] JUST SECURITY. *Expert backgrounder: NATO response options to potential Russia cyber attacks. Understanding the legal framework. Michael Smith. 24 de febrero de 2022.* Link

[5] NEXT VISIONS. *Terceros: el eslabón débil de la cadena. Roberto Heker. 4 de abril de 2022.* Link

[6] TECHNOLOGY REVIEW. *How a Russian cyberwar in Ukraine could ripple out globally. Patrick Howell O'Neill.. 21 de enero de 2022.* Link

[7] CCN-CERT. *Aproximación al marco de gobernanza de la ciberseguridad. Enero de 2022.* Link