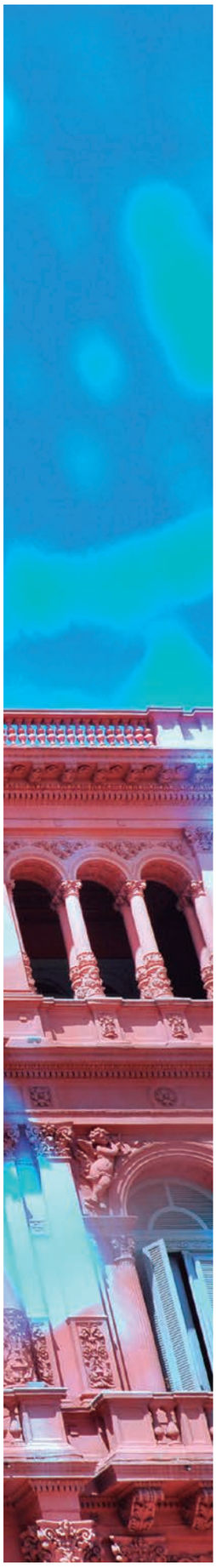
ARGENTINA BAJO ATAQUE

El avance de las amenazas informáticas también afecta al país. Con números que no paran de crecer, las empresas y el Gobierno están bajo el asedio de criminales digitales. Secuestro de datos, filtraciones, ejércitos de botnets, minado de criptomonedas y ataques a la infraestructura están en el menú del día. La posición del país en el mapa de la ciberguerra.

Por **Matías Castro**



Más información en
InfoTechnology.com

ndt

Están ahí, pero no los ves. De eso se trata. Están, pero no están. Así que cuidá tu infraestructura, tus datos, tus credenciales. Cuidá los ahorros. Porque están ahí, van a estar siempre ahí. ¿Chorros?, no, no, eso es para la gilada. Son crackers, exploiters, script kiddies, bandas de ransomware, hackers maliciosos, negadores de servicio, podría decirse parafraseando a la película argentina *9 Reinas*. Así es como se mueven hoy los actores maliciosos que tienen a la Argentina bajo asedio, específicamente, a todo su entramado tecnológico. Es una guerra sin cuartel ni armas convencionales, con un botín más que tentador: para finales de 2021 se espera que el ciberdelito le cueste al mundo unos US$ 6.000 millones, cifra ascenderá a US$ 10.500 millones para 2025 según proyecciones de la firma PacketLabs. Pero el precio del botín no viene solo, sino que es consecuencia y a su vez motivo del aumento general de los ciberataques en el mundo. Según el informe global anual de CheckPoint, un proveedor global de soluciones de ciberseguridad, se vieron casos llamativos, como el ataque a la compañía de infraestructura SolarWinds a principios de año, o la explotación de la debilidad en **Apache Log4j.** Según el informe, en 2021 las empresas experimentaron un 50 por ciento más de ciberataques semanales que en 2020 con picos de hasta 900 ataques semanales por organización. Los blancos fueron educación e investigación, con 1.605 ataques semanales (un 75 por ciento de aumento) seguido por los Estados y su rama militar con 1.136 ataques semanales (47 por ciento de aumento) y el ámbito de las comunicaciones con 1.079 ataques semanales (51 por ciento de aumento). Estos datos no se desinflan al localizarlos en la Argentina. Según un estudio de la multinacional Fortinet, se detectó un aumento constante de amenazas durante el año pasado con más de 289.000 millones de amenazas cibernéticas en América latina y el Caribe, un 600 por ciento superior a lo registrado en 2020 y de las cuales 3.200 millones apuntaron hacia el país.

Pero además, la naturaleza de las ofensivas cambió. "Según el último informe de la Dirección Nacional de Ciberseguridad se registró un aumento interanual del 261 por ciento. Por supuesto que no son datos que sorprendan, ni tampoco que entre los incidentes más reportados se encuentren los relacionados con acciones de ransomware y phishing. Pero la profesionalización de los atacantes conlleva una sofisticación de sus técnicas, además de una inmediatez para detectar oportunidades que debe ser evaluada para plantear planes asertivos", explica Sebastián Stranieri, fundador de la firma argentina de seguridad informática VU. "Si bien las amenazas que vemos a diario no son nuevas, estas evolucionan y se sofistican a cada segundo, pero sobre todo están disponibles online para que prácticamente cualquier usuario pueda darles uso y generar una nueva. Así, se dirigen a targets más específicos o masivos, según el objetivo", agrega el especialista. Por caso, durante el tercer trimestre de 2021 tuvo lugar el mayor ataque de denegación de servicio distribuido de la historia (DDoS, por sus siglas en inglés, que utiliza técnicas como la Inundación SYN, que genera varias peticiones abiertas en un servidor, hasta saturarlo) que provino de una variante de la reconocida botnet Mirai, dirigida a dispositivos IoT. La potencia del ataque llegó al Tbps (Terabits por segundo) con picos de hasta 1,2 Tbps. Fortinet detectó que el ataque llegó a territorio local e incluso en Brasil se dio el 10 por ciento de estos ataques (unos 500.000 millones de intentos de DDoS). Según la firma Kaspersky, la Argentina fue atacada, especialmente, por ransomware dirigido como Conti, Darkside, Lockbit, Ransomexx, Revil, Ryuk y Wastedlocker lo que evidencia la complejización de los ataques: ya no se trata de disparar a ciegas, sino con precisión de francotirador. "Más tecnología disponible, más personas volcándose a trabajar o comprar online, da como resultado una incalculable cantidad de datos", clarifica Stranieri. De hecho, un informe de la empresa F5 da cuenta de que si bien la Argentina tiene solo un 0,3 por ciento de las 4.000 millones de IPs públicas asignadas en el mundo, el tráfico de ataques y escaneo de vulnerabilidades fue diez veces superior (2,9 por ciento) en el período de julio a septiembre de 2021. A su vez, los tres puertos más atacados y con mayor escaneos de vulnerabilidades siguen siendo los puertos 5.900, 22 y 3.389: aquellos más comunes en los accesos remotos. Incluso el phishing, la versión digital del cuento del tío, se profesionalizó. "Los últimos sucesos en diferentes países demuestran que ni la Argentina ni ningún país está preparado. Esto es porque, por ejemplo, el phishing apela a los sentimientos de la persona de modo que si el filtro de anti-phishing no funciona, la persona se

También llamada Log4Shell o LogJam fue una vulnerabilidad de día cero en la Interfaz de Nombrado y Directorio de Java que permitió ejecutar código arbitrario de forma remota.

US$ 3.900 M

es la pérdida promedio en na empresa por cada brecha de seguridad.

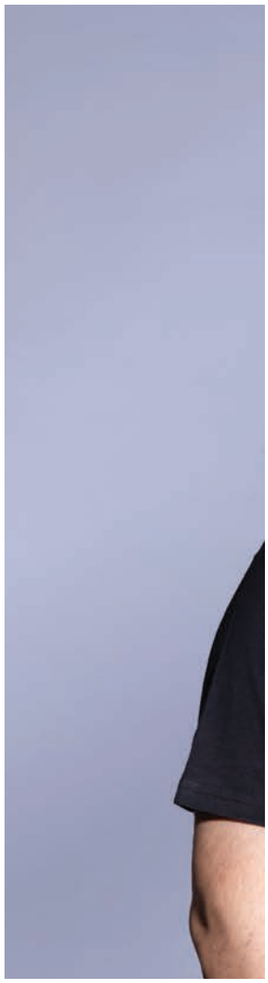
Malware que usa un motor de código para mutar pero sin cambiar su algoritmo original: modifica su payload pero no su semántica (funcionalidad). Es más difícil de detectar.

US$ 6.000 M
es lo que le costará al mundo el cibercrimen para finales de este año.

sintió impulsada a darle clic y es una caída limpia. Los phishing dirigidos son fabricados de tal forma que no habrá detección. Entonces, al final es el atacante versus la víctima, cara a cara, donde la decisión reside en si la víctima está suficientemente motivada a dar clic", explica Dmitry Bestuzhev, director del Equipo Global de Investigación y Análisis en América latina para Kaspersky, en referencia a los spear phishing más sofisticados que utilizan una miríada de datos de acceso público (como redes sociales) y información interna de la empresa (previamente vulnerada e investigada) para diseñar phishings con precisión quirúrgica.
El mandato darwiniano de adaptación obligó a los phishings a dejar atrás al mítico príncipe nigeriano y a generar anzuelos con nombres reales, fechas exactas y perfilados para cada víctima.
"Estamos cada vez peor porque los ataques están siendo un negocio cada vez mayor. La evolución de la tecnología hoy permite llegar cada vez más lejos y profundo", resume Gery Coronel, Country Manager para América del sur en Checkpoint. La progresión del malware, que pasó de virus que infectaban directamente las PC y los subsecuentes antivirus que desarrollaron las primeras compañías de seguridad, hasta los firewall que llegaron de la mano de internet junto a las protecciones de IPS para agentes intrusivos, hoy son moneda común en cualquier organización. Sin embargo, "la nueva generación, la sexta, no se parece a las anteriores. Hoy se ven ataques **polimórficos,** multivectoriales y a gran escala que afectan a toda la superficie de la empresa. Antes se apuntaba a los servidores o los data centers, pero hoy hay accesos remotos, redes mobile, infraestructura en la nube. Esto generó que de 2020 a 2021 los ataques crecieran 20 por ciento, un número preocupante", agrega Coronel.

¿Cui Bono?

Para entender el estado de situación hay que seguir el viejo adagio latín que insta a preguntarse quiénes están ganando con esto y por qué. "Hay tres motores que mueven los incidentes. Uno es el monetario, tener ganancias, cuya máxima expresión es el ransomware o la venta de información y de propiedad intelectual de empresas como también de datos personales que tengan esas compañías. Por otro lado, están los ataques orientados o influenciados por los Estados que son los más difíciles de probar, y tienen más que ver con la defensa del ciberespacio; tanto ofensiva como defensivamente. Aquí se busca dañar a un gobierno. Por último, el hacktivismo, que no está directamente relacionado con hacer daño,sino con ataques de baja complejidad, como DDoS o un wipeout masivo", explica Gonzalo García, vicepresidente de Fortinet para América del sur. Según los especialistas, en el país hay "de todo" aunque con intensidades de ataques diferentes. "La Argentina es representativa de la muestra mundial y las intenciones de los ciberdelincuentes se conocen por sus efectos más que de manera explícita. Hace un tiempo el ransom se apuntaba hacia usuarios individuales pidiendo US$ 200 por archivos de trabajo o fotografías familiares. Hoy, el espacio económico es tan grande que se secuestra información gubernamental y de empresas por valores de miles de millones de dólares. Incluso, el software malicioso se vende como ransomware as a service, que incluye también manuales de operaciones, formas de lavar el dinero y hasta indicaciones para llevar a cabo la negociación", se explaya Coronel. En el mismo sentido, Stranieri comenta que "en 2020 se superó el récord de costos asociados a ciberataques. En todo el mundo, se estima que las pérdidas económicas pueden alcanzar un trillón de dólares, con un promedio de US$ 3.900 millones por cada brecha de seguridad. Además, estudios promedian que el valor estimado de las primas de seguros cibernéticos en todo el mundo ascenderá a US$ 20.000 millones para 2025". En el país hay algunos casos testigos: en julio de 2020, la división local de Telecom sufrió un ataque de dispersión global a sus sistemas que culminó en un pedido de rescate de US$ 7.500 millones en la criptomoneda Monero. Según diversas fuentes y documentos filtrados, se trató de una operación exitosa de phishing a través del call center de la compañía que consiguió credenciales de usuarios con privilegios de acceso. Se cree que el grupo responsable del deploy del payload malicioso fue el grupo ruso Revil (o Sodinokibi) que fue desmantelado a principios de este año por el Estado ruso. La narrativa oficial es que la compañía pudo contener el ataque sin daño a las infraestructuras críticas, aunque no ofrecieron mayores detalles ante la consulta de este medio. En noviembre de ese mismo año, se conoció que Cencosud (específicamente sus cadenas Jumbo, Easy, Paris y Santa Isabel) cayó víctima de un exitoso ataque de ransomware con **Egregor,** otro en ese entonces popular servicio de ransom-as-a-service. En una escena dantesca, tras el ataque, las máquinas de facturación de los locales emitieron la nota de rescate con las indicaciones para el pago y la comunicación con el grupo atacante. Los expertos coinciden en que esta curiosa escena se dio por la falta de segmentación de las redes operacionales y administrativas de la compañía (según estimaciones en off the record del sector, la ausencia de microsegmentación permitió que fueran afectados hasta el 80 por ciento de los sistemas).



El malware utiliza un esquema de cifrado de archivos híbrido basado en el cifrado de flujo ChaCha y el cifrado asimétrico RSA. La clave pública maestra RSA-2048 de los delincuentes está incrustada en el cuerpo del troyano.

Foto: Gentileza VU.

LOS 6 PEORES CIBERATAQUES DEL AÑO

1. SolarWinds: la compañía de software fue víctima de un malware que contaminó una de sus actualizaciones y generó un efecto en cadena que infectó a otras 18.000 empresas.

2. Microsoft Exchange Server: un grupo de delincuentes encontraron cuatro vulnerabilidades en el software que funciona como back end para sistemas de mensajes y ejecutaron cuatro ataques de día cero. Un total de 30.000 organizaciones públicas y privadas fueron víctimas en los Estados Unidos y 60.000 a escala global.

3. Colonial Pipeline: el sistema de oleoductos de productos refinados más grande de los Estados Unidos fue víctima del ransomware DarkSide y debieron interrumpir todos sus procesos de distribución, lo que generó escasez de combustibles en una parte del país. La firma pagó un total de US$ 5 millones al grupo de hackers.

4. JBS: la compañía dedicada a la carne fue hackeada por el grupo de ransomware REvil y debió paralizar todas sus operaciones por varios días seguidos. Pagaron US$ 11 millones por el rescate y, según la firma, que ni sus datos ni los de sus clientes resultaron comprometidos.

5. Kaseya: la empresa de software de gestión informática también cayó en un ataque de REvil, al igual que JBS, y negó el pago de US$ 70 millones. Dicho ransomware se expandió a agencias gubernamentales y a pequeñas empresas que usaban el sistema de Kaseya, y un total de 1.500 negocios debieron frenar sus operaciones.

6. Twitch: la compañía de transmisión de videos en vivo sufrió una fuga de datos y los ciberdelincuentes filtraron un torrent de 125 GB con datos, documentos, el código fuente de la empresa y hasta sus propias herramientas para hackear.

Fuente: Fluid Attacks, 2021.

"LAS AMENAZAS QUE VEMOS A DIARIO NO SON NUEVAS, PERO EVOLUCIONAN."

SEBASTIÁN STRANIERI,
CEO de VU.

En el mismo sentido, la ausencia de una política de Domains Keys Identified Mail hizo más vulnerable aún el proceso de validación de correos electrónicos dentro de una corporación con alta diversidad comercial. La nota amenazaba con que si no se paga un rescate en tres días, los datos robados se harán públicos. Los atacantes pidieron una suma final de US$ 4 millones por la llave de desencriptación y como pago por su silencio respecto al hackeo. La decisión de la empresa fue no pagar y los hackers cumplieron con su parte: a las 72 horas del pedido de rescate, los datos fueron subidos a la web. Las ramificaciones de esto se verán más adelante. El último caso resonante fue el de MercadoLibre. Según confirmó la empresa, sufrió un episodio de ciberdelincuencia y los hackers accedieron a los datos de 300.000 de sus usuarios junto a parte del código fuente de la empresa. Lapsus$, el grupo de hacking que se adjudicó el ataque, aún no liberó los datos, ya que pondero varios leaks de otras empresas en su canal de Telegram y la empresa de origen argentino no salió elegida (antes se liberaron datos del fabricante de hardware Nvidia y de la empresa de telecomunicaciones Vodafone). Se cree que este grupo tiene su sede en Brasil y está en la mira de los investigadores de seguridad desde 2020, pero ganó notoriedad el año pasado cuando se atribuyó el mérito de atacar al Ministerio de Salud de Brasil. También han hackeado a otras empresas que operan en Brasil o son de habla

Funciona como una firma digital de seguridad que permite al receptor confirmar que un correo electrónico fue indefectiblemente enviado y autorizado por el dueño de ese dominio.

Para cada conexión de sistema a sistema se debe decidir si cualquiera de los lados de la conexión confiará en el otro y en qué medida. Las "zonas de confianza" son áreas donde las conexiones se consideran entre si con el mismo nivel de confianza.

portuguesa como Impresa, Claro, Embratel, NET, y Localiza. En el caso de Mercado Libre, no está claro a qué se refieren con "código fuente", aunque podría tratarse de un caso similar al de Samsung, donde se robaron ciertas piezas de software usadas para autenticar procesos internos de los teléfonos inteligentes, como ser el caso de las Trusted Applets (AT) o Trusted Zones (Trusted execution environment o TEE, en inglés). Según la empresa, su análisis forense no arroja que hayan sido comprometidos datos de los sistemas de pago.

"Un ransomware ejecuta un código en algún dispositivo y luego cuando gana control se propaga lateralmente dentro de la organización y busca cómo hacerlo a escala y con velocidad mientras que las empresas tienen controles más sigilosos respecto a esto pero se empiezan a utilizar herramientas de IA con ataques más automatizados. La forma de implantar el ransom cambió y la velocidad cambió", resume García y agrega: "antes, desde la vulneración y el movimiento lateral hasta la detección podían pasar de seis a ocho meses pero ya no se trabaja oculto tanto tiempo. Se busca hacer rápido y acelerar la técnica de ataque con la sofisticación que provee el uso de IA". En sintonía, Alejandro Botter, gerente de ingeniería de seguridad para América del sur en Checkpoint, explica que hoy el ransomware contempla una triple extorsión: "La primera de ellas es pedir rescate por los datos encriptados, con un buen backup se podía salvar parte del problema pero luego llegó la doble y triple extorsión. El malware primero infecta la red, por phishing, archivo malicioso o un dispositivo externo comprometido, y se esparce y mueve lateralmente para buscar robar archivos de alto impacto. Luego es que se cifran los sistemas y se roba el acceso al usuario legítimo. Entonces, se extorsiona con el acceso a los equipos y con la liberación de los datos. Por último, usando esos mismos, se extorsiona a los propietarios de esos datos. Por ejemplo, en un ataque a un hospital se puede extorsionar al dueño de los datos del registro médico, directamente". En el caso de la Argentina, ¿se trata de un blanco específico?, ¿es un país que esté en la mira de los atacantes, siendo que su potencial beneficio económico es menor que en el de las grandes multinacionales del primer mundo? "La información siempre es valiosa y siempre habrá un comprador. Que no siempre está fuera de la Argentina. La huella digital de un usuario, que incluye medios de pago, información financiera, contraseñas y correos electrónicos, siempre tiene valor. Datos argentinos en la dark web hubo y habrá en el futuro a la venta", reconoce García.

Ábrete sésamo

Vale la pena, entonces, preguntarse cómo es que los agentes maliciosos logran efectivamente penetrar en los sistemas corporativos. Tanto desde la visión de los especialistas como al analizar los propios ataques, emerge un patrón claro: hay dos grandes categorías de ataques en el país. Por un lado, los phishing y por el otro los malware. Según datos de la empresa Global Data Systems (GDS), los ataques de phishing son responsables de más del 93 por ciento de las violaciones de datos comerciales a empresas. García, sin embargo, profundiza en este aspecto y explica cuál es la verdadera razón de la prevalencia del phishing sobre otros ataques: "Si el sistema ya tiene un exploit conocido, si tus puertos aparecen como vulnerables en Shodan, si ya

Un buscador de dispositivos de acceso público enfocado en servicios HTTP, HTTPS, FTP, SSH, Telnet, SNMP y SIP. Permite encontrar puertos abiertos en dispositivos IoT y en terminales Scada.

Foto: **Gentileza Kaspersky.**

"AL FINAL ES EL ATACANTE VERSUS LA VÍCTIMA, CARA A CARA."

DMITRY BESTUZHEV,,
director del Equipo global de investigación y análisis en América latina para Kaspersky.

APUNTEN CONTRA EL GOBIERNO

Los incidentes de ciberseguridad no se limitan a las empresas. El Estado es uno de los blancos predilectos de los cibercriminales y así lo evidencian las filtraciones y hackeos que los gobiernos vienen sufriendo desde hace años. Cómo piensa el Estado defenderse y cuáles son las brechas que aún quedan por cerrar.

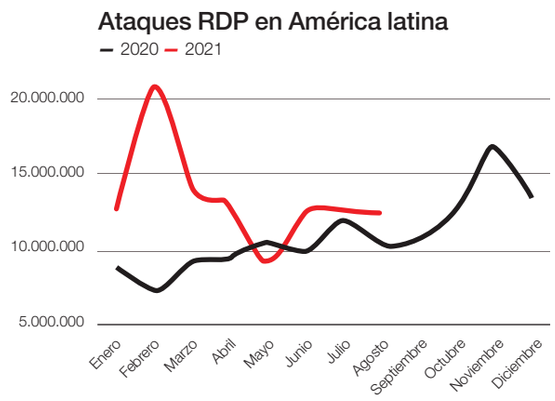
El pasado 11 de marzo el grupo de ransomware Vice Society publicó los datos que robó al Senado argentino: hay números de DNI, CUIL y trámite, además de fotocopias del DNI de frente y dorso, domicilio, firmas a mano alzada, licencias de conducir y más. Un botín nada despreciable que se suma a la lista de filtraciones que sufrió el Estado en los últimos años. Pueden traerse a la memoria el hack de 2020 por parte del grupo REvil, donde se sustrajeron 50 GB de datos de la Dirección Nacional de Vialidad y el golpe que dio Netwalker contra la Dirección Nacional de Migraciones. A finales de 2021, llegó la estocada del ransomware Everest que ofreció en la dark web varios accesos oficiales por la suma de US$ 200.000. "El incremento fue de 261 por ciento en casos de asistencia de incidentes de seguridad informática y lo explican dos factores. El primero es la creación de un nuevo Equipo de Respuesta a Incidentes Informáticos Nacional (CERT.ar), se optimizó la asistencia. El otro factor es la tendencia a nivel global de mayor uso de TICs durante la pandemia, con más posibilidades de comisión no solo de ciberdelitos sino de incidentes de seguridad informática", explica Gustavo Sain, director nacional de Ciberseguridad de la Nación. Según Sain, lo que diferencia al Estado de las empresas es que el gobierno no negocia: el ransom no se paga y hay menos posibilidad de lucro. Para Horacio Azzolin, titular de la unidad fiscal especializada en ciberdelincuencia del Ministerio Público Fiscal, "es una cuestión natural que está relacionada con el crecimiento de internet y como se potenció con la pandemia". La complejidad y el secretismo que rodea a todos los ataques cibernéticos también se palpa en el Estado, lo que dificulta su entendimiento. Una fuente cercana a áreas técnicas del Estado así lo explica: "Hubo casos complejos, y hubo casos que se sobredimensionaron, como fue Renaper. Se habló de un ataque pero en realidad

existe una puerta trasera que permite ejecutar código remoto o si tu sistema ya aparece en herramientas como Crimepack es solo apuntar y tomar control. Eso es más fácil que un phishing, pero ahí fallaron muchas cosas en seguridad. Además, penetrar un sistema de esa manera puede llevar a una zona estancada y sin lateralidad". En cambio, un phishing con un profiling potenciado por IA y enfocado en un actor particular puede otorgar un acceso mucho más aprovechable a un sistema que está más defendido. "Lograr un phising personalizado a un CEO o un CFO da un acceso más específico y poderoso de lo que puede lograr un exploit tradicional en un sistema muy vulnerable", explica García.

Mientras que el caso del malware se presenta en diferentes sabores: por un lado, se suelen aprovechar malas configuraciones por parte de las organizaciones. Según datos de Kaspersky, hubo un aumento del 78 por ciento en ataques **RDP.** Mientras que por otro lado, también se conocen infecciones por parte de dispositivos maliciosos como pendrives. Finalmente, en otros casos, se trata de inyecciones de código malicioso a partir de vulnerabilidades web en las compañías. "El eslabón más débil es el factor humano, independiente de todo, se puede ser víctima siempre de un ataque de ingeniería social. Es total y completamente cierto que es uno de los principales vectores", reconoce García. Sin embargo, no todo se resume a clickear donde no se debe. "Todos los sistemas tienen vulnerabilidades. Incluso, si es que los fabricantes publican responsablemente los parches y los usuarios los aplican, siempre hay una ventana de explotación de vulnerabilidades de **día cero.** Esto quiere decir que, técnicamente, no es culpa del fabricante ni de la víctima. Nadie puede defenderse contra tal explotación porque la vulnerabilidad en cuestión no es conocida todavía. La Argentina maneja los mismos sistemas que en otras partes del mundo. Hemos visto caer a los grandes. Es por esto que al final de cuentas es todo una cuestión de la necesidad de parte del atacante y del dinero destinado al ataque", reconoce, casi de manera pesimista, Bestuzhev. Aunque más allá de lo técnico, también hay cuestiones legislativas que pueden fortalecer los perímetros de seguridad en las organizaciones. Así lo cree Stranieri, que explica que: "Contamos con un marco regulatorio y un sistema de políticas públicas significativamente consolidados, que en ciertos casos deben actualizarse, como la ley de Protección de Datos que no sufre modificaciones desde hace más de 20 años". Antes de 2008, no había leyes específicas en el país para frenar el delito cibernético. Gracias a la falta de regulaciones y políticas, los ciberdelincuentes prosperaron porque sus actividades no fueron categorizadas como delictivas. Sin embargo, todo cambió en 2008 cuando el gobierno adoptó la ley de Delitos Cibernéticos. "Con la evolución tecno-

RDP: Es un protocolo de Microsoft para que los administradores accedan a las computadoras de escritorio remotamente. Ofrece control total sobre el dispositivo y es un punto de entrada valioso para los ataques. Suele aprovechar puertos 3389 (de conexión remota) que no están bien configurados.

día cero: Se trata de un ataque que aprovecha una vulnerabilidad en una pieza de software desconocida para el usuario y el fabricante. Han pasado "cero días" desde que se conoce el problema. Se suelen vender en el mercado negro de la dark web. El rango de precios va desde US$60.000 (Adobe Reader) hasta US$2.500.000 (Apple iOS).



Fuente: Kaspersky, 2021.

lógica de los últimos años, es necesaria una actualización constante tanto de las leyes, normativas, como de los planes educativos. Teniendo en cuenta que la digitalización incorporó personas que están teniendo sus primeras experiencias online, existe una gran parte de la sociedad que no cuenta con la información básica para proteger sus datos y su identidad digital", contextualiza Stranieri.

Aunque con menor preponderancia en lo que respecta a daños, existe otro tipo de ataque del que se habla poco y destaca por su espectacularidad. Se trata de los ataques dirigidos a infraestructuras críticas y de los ataques hacktivistas. Desde que el FBI, la NSA y la Unidad 8200 de las Fuerzas de Defensa de Israel lanzaron en 2010 la operación **"Juegos Olímpicos"** con el fin de desestabilizar las plantas de purificación de uranio de Natanz; en Iran, la ciberguerra no paró de crecer. Una realidad que hoy se ve a todas luces en el conflicto de Rusia y Ucrania. En el caso argentino, según apuntan los expertos, no se han detectado ataques provenientes de actores maliciosos sponsoreados por gobiernos. "Los ataques de destrucción son muy bajos, los de ransom tomaron mucha más presencia porque para los atacantes es una inversión armar el malware y que sea redituable el ataque. Cuando se hace el análisis de un ataque o malware se busca quién está detrás y que intenciones había. Pero cuando uno ve los **wipers** y otros malware de destrucción, tiene que ser un ataque que quiera minar la competencia entre empresas. Solo busca cortar la disponibilidad. Mientras que los ransom y los de criptominería tienen una estructura de negocio detrás", explica Botter. En la misma línea, Camilo Gutierrez Amaya, jefe de Concientización e Investigación en Eset para América latina, diferencia que "para hablar de ciberguerra tiene que haber una nación atacando a otra para tratar de afectar su infraestructura crítica, pero en la región eso es algo lejano, no sucede. Aunque ciberataques a sistemas críticos si se conocen". "En el caso de las infraestructuras críticas, los actores buscan ventajas estratégicas u objetivos de alto valor, donde el beneficio de la

El ataque utilizó un malware llamado Stuxnet que se infiltraba en los PLC de los rotores de las plantas, alterando su normal funcionamiento. Cuando se conoció, fue el virus informático más complejo y peligroso de la historia.

Malware diseñado para corromper y "limpiar" el almacenamiento de una máquina, haciendo inutilizables los archivos y la información.

Más información en
InfoTechnology.com

hubo exceso de uso de credenciales. Si alguien que tiene una credencial hace algo mal es un tema de legales porque sería un actor malicioso de adentro y no una vulnerabilidad. Lo sabemos por el tipo de consultas que se realizaron" y a esto Sain agrega, en sintonía: "Cuando un usuario autorizado y legítimo filtra datos en forma indebida e ilícita, no existen medidas técnicas que sirvan, y esto pasa tanto en el sector público como en el privado". La fuente en off the record agrega que: "el tema pandemia complicó todo porque abriste redes, hay más accesos, más puntos de brecha. Muchos de los ataques son internos y eso pasa en todos lados. En el Estado pasan cosas por volumen de usuarios no porque sea el Estado específicamente". Un gobierno es un target de alta prioridad para cualquier atacante.

Pero, por su propia esencia, el Estado no puede pensarse en los mismos términos que una empresa: el impacto es distinto, los riesgos son distintos y la manera de abordarlo también. Aunque el eje común es la bidireccionalidad de los ataques, o bien se gana dinero o bien se daña la reputación. Azzolin rememora algunos casos testigo de ataques especialmente motivados por la política cuyo hábitat natural son los sistemas gubernamentales: "hubo casos de hacktivismo pero no fueron gran cosa. Hubo ataques de DDoS a algunos medios, como pasó con Página 12 cuando ganó Macri, algo muy grave para la democracia porque silencia voces. Tuvimos casos en momentos puntuales, como las reuniones del G20 o épocas de elecciones, que son como un piquete tecnológico", expresa. Respecto a esto, Azzolin afirma que en la Argentina no operan bandas de ciberdelincuentes organizadas, aunque sí reconoce que hay algunos casos de APT que operan en territorio nacional pero "que no son de alta sofisticación".

Guardia baja

Los puntos flacos del Estado se aparecen como una consecuencia de su propio funcionamiento. Uno de ellos, que es un eco de lo que sucede en el sector privado, es la falta de recursos humanos. Una fuente cercana dentro del Estado que prefiere guardar el anonimato así lo reconoce: "es un sector muy demandado, un perfil medio gana más que un juez y los jueces ganan fortunas. Hay dependencias que tienen sysadmins que cobran $ 100.000 y así es posible que se den fugas", deja entrever. Pero existe también una pata técnica y una economía que hay que considerar. Uno

Foto: Gustavo Fernández

de esos talones de Aquiles es el tema de las licencias de software, que según la misma fuente en off the record, "no están en su mejor momento". Se trata de casos donde el software no se actualiza por los altos costos. "Hay equipos y licencias que pueden costar US$ 200.000, son problemas que exceden los deseos de hacer las cosas bien", desliza. Otro problema adicional, típicamente estatal, es la gestión política. Cuando la coalición Cambiemos dejó el gobierno, hubo actualizaciones tecnológicas que quedaron a mitad de camino y que la nueva administración puede elegir no continuar. "La gestión anterior contrato servicios cuestionables para manejar los datos de AFIP, llevándolos a Amazon Web Services. En la migración hubo una falla y durante meses hubo scripts corriendo hacia los servicios de AFIP que pedían DNI, CUIL y otros datos. De la misma manera que hubo un empujón muy fuerte de poner Oracle en todos lados cuando había soluciones mejores y más baratas", cuenta la misma fuente. Así, la Jefatura de Gabinete estableció que debe haber requisitos mínimos de seguridad de la Información en el Sector Público Nacional. "Se trata de una

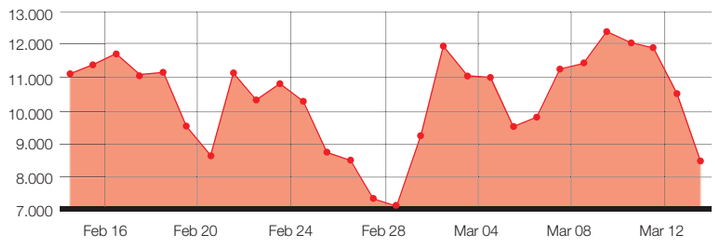
"EL INCREMENTO DE CASOS FUE DEL 261 POR CIENTO."

GUSTAVO SAIN,
Director Nacional de Ciberseguridad.

operación va a ser a largo plazo y puede influir en el funcionamiento de toda una nación. Cuando hablamos de grupos que atacan este tipo de objetivos estamos hablando de grupos relacionados con gobiernos o sistemas de inteligencia, generalmente", según Stranieri. Sobre esto, Gutiérrez Amaya comenta que "se han visto ataques de filtración de información de entidades de gobierno o de entidades financieras pero que no afectan como tal a la operatividad, sino que buscan dañar la reputación". Este vocero también menciona el caso del hacktivismo, otro modus operandi de ataque que está por fuera del esquema del negocio del cibercrimen. Hay ataques hacktivistas que apuntan a objetivos específicos y los hacen grupos que están disconformes con algo y la forma de protesta es publicar información y exponer las vulnerabilidades de los sistemas. Más allá de la protesta, que puede ser válida o no y es un juicio de valor aparte, es un delito", explica. En diciembre de 2021, por caso, el grupo hacker Anonymous se adjudicó un ataque de DDoS contra Pan American Silver por la explotación minera en la provincia de Chubut. Pero no es el único: el Estado sufrió un caso de hacktivismo en 2019 tras la difusión de archivos de mail e información personal de las fuerzas policiales (en el llamado "gorra leaks"), como así también diferentes casos de defacing (alteración) de sitios webs de las fuerzas armadas y prefectura. "Es muy menor el tema de ataques solo para hacer daño en el caso del mundo corporativo. El 25 por ciento de las empresas tiene ataques con botnet, menos del 20 por ciento son ataques con infostealers y por detrás llega todo el mundo de los criptominers", evalúa Coronel.
Otra de las amenazas que los expertos consideran menor en la Argentina son las llamadas amenazas persistentes avanzadas o APT, por sus siglas en inglés. Se trata de grupos que operan contra objetivos específicos y por largos períodos de tiempo, buscando generar el mayor daño posible (y, por consiguiente, la mayor ganancia posible). En la Argentina se conocen algunos casos: Packrat fue una operación APT que trabajó en

Tipos de ataque en la Argentina

Cantidad de ataques cada cuatro días, durante un período de tiempo de un mes



>> Este informe de Kaspersky analiza la actividad de malware durante un período de un mes, de febrero a marzo de 2022. Los mineros de cripto (5%), los troyanos (5%) y ransomware (4%) fueron los más detectados.

1. DangerousObject.Multi.Generic
Amenazas sin definir, es decir, son varios malware en uno.
20,41%

2. Trojan.BAT.Miner.gen
Troyano de minería que se ejecuta en servidores de empresas para minar criptomonedas.
5,30%

3. Trojan.WinLNK.Agent.qk
Es un troyano que se esconde en archivos ejecutables y bloquea, destruye y copia datos.
5,17%

4. VHO:Trojan.Win32.Convagent.gen
Es un troyano que dice que el usuario está usando su computadora para mirar pornografía infantil y pide un rescate de la computadora.
4,50%

5. Trojan.WinLNK.Agent.gen
Se trata de un troyano similar a Trojan.WinLNK.Agent.qk.
2,72%

6. Trojan.Win32.Agent.aapao
Este troyano se ejecuta en una computadora y elimina archivos claves del sistema operativo Windows.
2,55%

7. Trojan.Script.Generic
Es un troyano que ejecuta scripts maliciosos, es decir, inyecta código infectado en un sistema.
2,38%

8. Worm.Win32.Autoit.aky
Este malware ejecuta varias tareas destructivas y se propaga rápidamente.
1,58%

9. HackTool.MSIL.Convagent.gen
Los programas HackTool pueden crear nuevos usuarios en una computadora y utilizar un equipo sin permiso para llevar a cabo acciones maliciosas específicas.
1,41%

10. HackTool.Win32.KRT.gen
Es una herramienta fraudulenta que es capaz de generar claves y licencias falsas de activación.
1,28%

Fuente: Kaspersky. 2021.

el país desde al menos 2008 y hasta 2013. Su insignia fue la utilización de RAT (troyanos de acceso remoto) dirigidos sistemáticamente hacia figuras políticas de alto perfil (entre los que se contó al **fiscal Alberto Nisman y a Máximo Kirchner**), periodistas (como víctima más popular tuvieron a Jorge Lanata) y otras personas en varios países con malware y phishing. Un informe de CitizenLab encontró 12 dominios de comando y control de malware diferentes, y más de 30 muestras de malware que se extendieron durante un período de siete años. Packrat también trabajó creando y manteniendo grupos de oposición y organizaciones de noticias falsas que luego utilizaba para distribuir malware y realizar ataques de phishing. Por caso, en 2015 lanzaron una campaña falsa contra el ex presidente ecuatoriano Rafael Correa, donde se instaba a los destinatarios a bajar una supuesta lista de tuiteros espiados por el Estado; que era en realidad un archivo malicioso de spyware. El análisis forense de Citizenlab trabajó la hipótesis de que el actor malicioso podría ser o bien apoyado por un gobierno o bien rentado por un gobierno para esta campaña específica, aunque no se llegó a una conclusión final sobre su naturaleza. Recientemente, Eset encontró un malware que apunta específicamente a usuarios corporativos de la Argentina, el cual bautizó LuxPlague. Según el análisis telemétrico de la compañía, este actor es responsable de la mayoría de RATs NjRAT que hoy operan en el país. Se cree que actúa desde 2018 y al día de hoy está en actividad. Se cree que la propagación de la campaña comenzó con el compromiso de un equipo de una organización gubernamental del país.

El ataque se basó en un correo de phishing con el adjunto "estrictamente secreto y confidencial.pdf.jar," es decir, un archivo java haciéndose pasar por un pdf. El archivo malicioso era un RAT llamado AlienSpy.

Entero o a pedazos

Por los daños que ocasiona y por la ganancia que deja, es difícil creer que los ciberataques bajarán de intensidad. Lo que es más, a medida que se acelera la transformación digital, los puntos de ataque se multiplican en todas las organizaciones. Más allá del daño tecnológico o reputacional, ya se están empezando a ver las primeras grietas profundas que dejan estos ataques. El 14 de agosto de 2020 un cliente del banco BBVA fue víctima de un ataque exitoso de phishing que le dio acceso a las cuentas y el homebanking del damnificado. Una vez dentro, se realizó una sustracción de

serie de estándares obligatorios que deben cumplir los organismos públicos nacionales basados en normas ISO. La Dirección Nacional de Ciberseguridad y la Sindicatura General de la Nación (SIGEN) auditará su cumplimiento y serán aplicables también a las empresas proveedoras y contratistas que trabajen para los organismos alcanzados por la norma", contextualiza Sain. Otro problema que hoy es relativamente acuciante en el Estado es la tecnología antigua que no se puede cambiar. "Hay tech vieja que se hereda y se sigue usando, pero no es tanto el legacy, sino organismos que tiene el problema de tener software que corre sí o sí en un Windows viejo, pero en casi todos los lugares se está virtualizado con seguridad más alta, no es lo mismo un XP suelto que en una virtual machine", explica la fuente anónima.

El tema de la seguridad informática estatal es tanto relativamente nuevo como acuciante, ya que como todos los entrevistados coinciden, la virtualidad llegó para quedarse. Pero tanto su novedad como su complejidad técnica generan rispideces en las respuestas del gobierno. "Tenemos gente que se entrena permanentemente. Hoy, por ejemplo, trabajamos mucho el tema delitos con criptomonedas y esto ejemplifica porque los cibercrimines son diferentes a los tradicionales. Las unidades de homicidio no tienen técnicas que les cambian radicalmente todos los años, a lo sumo cambió mucho el ADN cómo se trabaja, pero se investigan igual. En los últimos años aparecieron las criptomonedas, los ransomware, familias nuevas de malware, todo lo cual hace tan solo cinco años directamente no existían", explica Azzolin. "Pese a los prejuicios existentes acerca de lo público, existe un gran talento humano en las áreas de informática y sistemas de los organismos del Estado", concluye Sain, y si bien reconoce el fuerte déficit también expresa que se está trabajando sobre ello. "El año pasado creamos un registro de puntos focales de ciberseguridad, representantes de los organismos centralizados y descentralizados. En este sentido se ha constituido una verdadera comunidad de ciberseguridad dentro del Estado que antes no existía. La Dirección a mi cargo triplicó la oferta académica de capacitación en el Instituto Nacional de la Administración Pública donde se ofrecen capacitaciones a los empleados del Estado en materia de ciberseguridad", cierra. **M.C** IT

1 TBPS

Esa fue la potencia del ataque DDoS más fuerte registrado hasta ahora y sucedió el año pasado.

dinero y un pedido de préstamos ilegítimo. El mail era idéntico al que envió la entidad ya que la concurrencia a sucursales era limitada. El banco solo permitía a sus usuarios hacer operaciones, consultas o reclamos por los canales on line. Dos años después, consta en autos "Urquía, Nicolás Martín c/ Banco BBVA Argentina S.A. - Abreviado - Otros - Trámite oral", que el Juzgado en lo Civil, Comercial y Familia de 3° Nominación de San Francisco, Córdoba, que el banco demandado debe pagar una indemnización por daño moral ($ 200.000) y otra por daño punitivo ($ 400.000). La Dirección Nacional de Protección de Datos Personales investigó de oficio el ya mencionado hackeo a Cencosud, enfocándose en el hecho de que la filtración de la información ponía en riesgo los principios de seguridad y confidencialidad de datos de los que la firma tenía que ser garante. Si bien la empresa afirmó que el daño fue "leve", recibió una multa de $ 290.000 por las infracciones a la Ley 25.236 de Protección de Datos Personales. El daño ya no solo afecta a las operaciones de negocio y la reputación sino que está calando en el sistema legal. La guerra ya está declarada y ante el agresor las organizaciones tienen que comenzar a levantar sus armas. "Interés en inversiones hay un poco más y se habla más de seguridad en las empresas, es algo más establecido en las firmas grandes y medianas. El 44 por ciento de los líderes planea mantener o aumentar el presupuesto de seguridad. Es un comienzo", reconoce Gutiérrez Amaya. "Los atacantes van a continuar y esto no tiene forma de resolverse porque quienes desarrollan malware no tienen las restricciones que tienen las empresas. Están constantemente buscando por dónde dañar. El mantra debe ser prevención antes que deteccion", opina Coronel. "Estamos experimentando la adquisición de sistemas de seguridad informática robustos por parte de las empresas pymes y no solo de corporaciones, lo cual confirma el trabajo de concientización", dice Stranieri y reconoce que "el contexto actual lo exige y es transversal". El experto, sin embargo, reconoce algunos stoppers: "En muchos casos, consideran que no son target hasta que lo viven en primera persona. En otros, creen que es una inversión que se puede hacer más adelante sin tener un peligro actual". La pregunta ya no es si sucederá, sino cuándo. IT