



FUNDACIÓN LED
Libertad de Expresión + Democracia



PROTECCIÓN DE **DATOS PERSONALES**

HACKEOS Y VULNERABILIDAD DE LOS
DATOS PERSONALES EN PODER DEL
SECTOR ESTATAL

Protección de **Datos Personales**

Hackeos y vulnerabilidad de los datos personales en poder del sector estatal

1.	Introducción	2
2.	Consideraciones	6
3.	Casos de hackeos y exposición de información pública y datos personales	7
3.1.	Ataque informático al Banco Nación - octubre 2019	7
3.2.	Ataque informático a la Dirección Nacional de Migraciones - septiembre 2020	10
3.3.	Ataque informático al RENAPER - octubre 2021	18
3.4.	Ataque informático al Senado de la Nación - enero 2022	25
3.5.	Ataque informático al Poder Judicial de Chaco - febrero 2022	29
3.6.	Censo Nacional de Población, Hogares y Viviendas - mayo 2022	31
4.	Una mirada sobre ataques cibernéticos dirigidos a otros Estados	37
5.	Conclusión	40

1. Introducción

La información que los ciudadanos brindan durante toda su vida a las distintas jurisdicciones estatales, forma parte de la relación del ciudadano con el Estado, y constituye un eje fundamental para el ejercicio de sus derechos civiles, sociales y políticos. Este intercambio de información privada se produce en base a un acuerdo reglado por Ley que establece la protección y preservación de la misma y la utilización específica para los fines que haya sido requerida.

Desde la incorporación de herramientas digitales para la captación, manejo y administración de las bases de datos personales, se han experimentado enormes avances para la agilización de los trámites y procedimientos administrativos que los ciudadanos pueden requerir. La digitalización del Estado y las herramientas de Gobierno Abierto permiten generar un estado más transparente, cercano al ciudadano y dentro de un entorno participativo, pero, si estas herramientas no se acompañan de protocolos estrictos de seguridad en la preservación de la información y en la manipulación de los datos personales, los derechos ciudadanos pueden verse afectados.

En los últimos meses se han verificado vulnerabilidades informáticas en los sistemas de administración de varias bases de datos que contienen datos personalísimos de los ciudadanos. Por eso desde la Fundación LED Libertad de Expresión + Democracia, proponemos observar con atención cada caso de intrusión, robo o hackeo de los repositorios de datos que alimentan las distintas bases a fin de analizar los niveles de seguridad informática que hubieran fallado a fin de contribuir al debate sobre la necesidad de construir un Estado más transparente, eficaz y respetuoso de los derechos ciudadanos.

Existen elementos que resultan básicos para una efectiva protección de los datos personales y los encontramos en las legislaciones particulares de cada país, variando sus disposiciones respecto al ámbito de aplicación, su contenido y encuadre. Algunos de estos elementos podemos encontrarlos en el orden nacional configurados en la ley de Protección de Datos Personales (Ley 25.326) y en el orden internacional en los “13 Principios Actualizados sobre la Privacidad y la Protección de Datos Personales”, aprobado en el año 2021, por la Asamblea General de la Organización de Estados Americanos¹.

Estos trece principios determinan los elementos que deben ser protegidos por los Estados que recopilan y almacenan información sobre datos personales de sus ciudadanos, teniendo en consideración:

- i) **Finalidades Legítimas**, para los cuales se recopilan los datos bajo valores democráticos y en un estado de derecho, y asimismo, Lealtad basada en legalidad y cumplimiento de la expectativa razonable de quien lo otorga;
- ii) **Transparencia y Consentimiento**, que especifican categorías, finalidad, destinatarios y los derechos del Titular de los Datos;

¹https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf

- iii) **Pertinencia y necesidad**, la primera en relación con la finalidad y la segunda como razonable proporcionalidad donde la medida no sobrepase lo que se necesita para alcanzar un fin legítimo, correspondientemente;
- iv) **Tratamiento y Conservación Limitados**, refiriendo a las expectativas razonables de las personas, con la recopilación de los Datos y el uso responsable y, a subes, por el tiempo limitado para el fin;
- v) **Confidencialidad**, refiriendo en el caso particular al entorno informático controlado y confiablemente seguro;
- vi) **Seguridad de Datos**, conformando y sosteniendo medidas de carácter administrativo y técnico que garanticen la disponibilidad de esos datos, su integridad y confidencialidad, contra toda vulneración.
- vii) **Exactitud de los Datos**, tomando en cuenta su sensibilidad en contrapartida con la posibilidad de que sean expuestos causando perjuicios de gravedad;
- viii) **Acceso, Rectificación, Cancelación, Oposición y Portabilidad**, en relación a sistemas informáticos simples, rápidos y sobre todo eficientes en la manipulación del titular de los datos;
- ix) **Datos Personales Sensibles**, considerándolos con aquellos privados e íntimos que comportan mayor gravedad ante su uso no autorizado;
- x) **Responsabilidad**, definida según el desarrollo y cumplimiento de metas y su vigilancia, que demuestren el cumplimiento de los principios rectores;
- xi) **Flujo Transfronterizo de Datos y Responsabilidad**, entendido en el marco de la cooperación e intercambio de metodologías que eviten complicaciones;
- xii) **Excepciones**, entendidas como aquellas con el único poder suficiente de limitar los derechos de privacidad de las personas, ante casos particulares de protección de prerrogativas, como por ejemplo, de orden público;
- xiii) **Autoridades de Protección de Datos**, que garanticen la protección, haciendo cumplir las leyes en el orden Nacional, Provincial y Municipal, contando con la pericia técnica necesaria para la consecución de dicho fin, obteniendo o creando lazos de cooperación con países extranjeros.

Asimismo, ante la manipulación de datos personales los Estados deben tener en consideración distintos instrumentos internacionales rectores como “Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (No 108, 28 de enero de 1981) y su Protocolo de enmiendas (8 de noviembre de 2001)”, “Protocolo de enmiendas al Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (“Convenio 108 plus”, abierto a firma el 10 de octubre de 2018, aún no en vigor)” y la “Decisión del Secretario-General de la Organización para la Cooperación y Desarrollo Económico (OCDE) sobre la Protección de Individuos en relación con el Tratamiento de sus Datos Personales, en vigor desde el 3 de mayo de 2019” -entre otros-.

El acceso a los datos, garantizado por nuestra Constitución Nacional al amparo de la protección del marco jurídico de los Derechos Humanos, debe permitir verificar la legalidad utilizada por parte de quien interviene en la recopilación de esos datos, impidiendo el uso abusivo o discriminatorio de los mismos.

La irrupción de la Pandemia de Covid 19, puso en evidencia la importancia del correcto manejo de datos personales y la utilización de los mismos por parte de quienes son, a su vez, encargados de resguardar su privacidad y seguridad. Los primeros desarrollos de aplicaciones de trackeos de contagios en el mundo generó la preocupación de la Fundación LED, la colisión de algunos sistemas implementados en el continente asiático con los derechos humanos fue el disparador para el análisis realizado en el *"Informe Especial sobre Aplicaciones de Seguimiento de Contagios COVID-19"*², en el que LED planteó lo que sucede cuando los Estados monitorean los movimientos y circulación de las personas a través de Apps que geolocalizan su ubicación o recaban información médica sin resguardar anonimato.

La privacidad y protección de los datos requiere que cualquier acción desarrollada en torno a los mismos tenga una finalidad legítima, que no comporte la utilización de esos datos para fines distintos de aquellos que fueron comunicados a sus titulares, cumpliendo con el principio de transparencia y confidencialidad, mediante medidas técnicas responsables y bajo altos estándares de seguridad.

Dichas medidas precisan de decisiones pertinentes y concretas que acompañen el avance tecnológico y el compromiso de los gobernantes. Argentina, en 2016 ya había propuesto un camino de gestión y compromiso en este sentido, incluso en el plano internacional, conformando los Grupos Mundiales de Trabajo (GMT) realizados por GOPAC, entidad formada como resultado de una Conferencia mundial realizada en Ottawa dedicados a combatir la Corrupción y mejorar la buena gobernabilidad³. Asimismo, participó de la Cumbre Regional de Gobierno Abierto en 2017 y la Conferencia Internacional de Datos Abiertos en 2018, impulsando desde la Organización de los Estados Americanos (OEA), la creación del Programa Interamericano de Datos Abiertos contra la Corrupción (PIDA), aprobado en Medellín por la Asamblea General. Es así que, en el marco del ingreso de la República Argentina a la Organización para la Cooperación y el Desarrollo Económicos (OCDE), Argentina fue el primer país del mundo en ser evaluado ante la recomendación en materia de Gobierno Abierto, incorporándose luego al Comité Directivo de la Alianza para el Gobierno Abierto (OGP, por sus siglas en inglés)⁴.

Mientras los procesos de digitalización para la atención ciudadana se aceleraron y las herramientas informáticas en materia de telemedicina, teletrabajo, e-commerce y trámites a distancia tuvieron un impulso enorme. Argentina, desaceleró los procedimientos de modernización y digitalización en los primeros meses del 2020 y dictó algunas medidas retrotrayendo los plazos. El Decreto 338/2020, por ejemplo autorizó la utilización de soporte papel y la firma ológrafa en lugar del uso de documentos digitales oficiales. La evaluación consiguiente de los organismos internacionales que forman indicadores de transparencia y

² <http://fundacionled.org/informes-y-publicaciones/informes-especiales/informe-especial-sobre-aplicaciones-de-seguimiento-de-contagios-covid-19>

³ <http://gopacnetwork.org/es/757-2/>

⁴ https://www.argentina.gob.ar/sites/default/files/cuarto_plan_de_accion_nacional_de_gobierno_abierto_-_argentina_-_v4.pdf

revisan entre otros criterios el acceso a la información y mecanismos de transparencia en los procedimientos administrativos, señalan, que Argentina ha descendido en el ranking por segundo año consecutivo, obteniendo 38 puntos sobre 100, de acuerdo al informe emitido por Transparency International⁵.

El objetivo del presente informe se centra en contribuir a un mayor progreso y concientización sobre la salvaguarda de los derechos de las personas, frente a una protección informática vulnerable o insuficiente por parte del Estado, que compromete la manipulación, recopilación, conservación, tratamiento y responsabilidad, en la interacción de ese Estado con la ciudadanía, en un marco tecnológico extremadamente dinámico, hoy endeble.

⁵ https://transparencia.org.es/wp-content/uploads/2022/01/CPI2021_Report_ES-web.pdf

2. Consideraciones

La informática forense

Dentro del marco de la protección en análisis, utilizando los trece elementos descritos en el punto precedente, nos convoca a investigar distintos incidentes o sucesos acaecidos en nuestro país.

Es por ello, que resulta oportuno indicar que un incidente de seguridad o una caída del sistema, así como el robo o espionaje de información son tareas de suma dificultad que se enmarcan dentro de lo que se denomina informática forense (conjunto de leyes, procedimientos, normas y pruebas que permiten la adquisición de evidencias locales o remotas, así como el análisis de las mismas, preservando su integridad y su cadena de custodia), que no es la técnica utilizada en el presente trabajo de investigación, sino que, dada la disponibilidad de la evidencia y el grado de acceso a la información sobre los hechos, se procedió al análisis de los casos particulares desde un grado de profundidad técnica que no se introduce o asimila a la práctica de la informática forense propiamente dicha.

Riesgos y vulnerabilidades frente a la protección de la privacidad y la custodia de datos personales

Los Estados deben adoptar los criterios internacionales que definen aquello que constituye la vulneración en la seguridad de los Datos Personales, como lo han manifestado en distintos acuerdos, convenciones, pactos y tratados a los que han adherido en distintas materias.

La existencia de vulnerabilidades dentro del sistema permite y facilita a los actores de amenazas cibernéticas, la incorporación de nuevas herramientas con varios propósitos durante sus ataques. Los responsables de ciberseguridad deben advertir las diversas TTPs que se utilizan a lo largo del ciclo de vida de un ataque, estando preparados para prevenir, detectar y responder a actividades abusivas que pueden ser indicativas de un compromiso en el sistema que puede provocar una interrupción operativa generalizada, daños a la reputación y la pérdida de confidencialidad de la información, sobre todo en aquellos datos que requieren un grado mayor de protección y que traen aparejada una mayor responsabilidad en su divulgación.

En este sentido, deben existir sanciones efectivas para los responsables de la filtración de la información, que no hayan mantenido la debida diligencia en el deber de cuidado de dicha información, puesto que su inobservancia genera consecuencias o perjuicios de distinta gravedad, conforme se advierte de los casos en estudio.

Los ataques informáticos han ido en aumento contra plataformas y servicios digitales del Estado Argentino, donde existen vulnerabilidades en la seguridad sobre datos personales sensibles. Gran parte de estos ataques son debidos a la técnica de "Ransomware" (secuestro de datos), que se desarrollan a través de una metodología de doble extorsión en la mayoría de los casos que tomaron dominio público, filtrando grandes cantidades de información confidencial con el fin de lucrar o de extorsionar a las víctimas.

Las filtraciones se llevan a cabo utilizando tácticas, técnicas y procedimientos (TTPs), que aprovechan herramientas de doble uso para varios propósitos, intentando minimizar su huella y evadiendo la detección de los controles de seguridad actuales, perfeccionando el ciclo de vida de diferentes tipos de ataques (ej. en el Ransomware), pretendiendo operar de manera evasiva. En algunos casos, una vez lograda la intromisión en el sistema estatal vulnerable, son extraídos los datos, resultando pasibles de publicación en sitios web controlados por atacantes conocidos como "sitios de fuga de datos", afectando el principio de confidencialidad de los mismos.

3. Casos de hackeos y exposición de información pública y datos personales

Análisis de los hackeos, intrusiones, y robo de información sensible sufridos por distintas áreas gubernamentales en Argentina desde 2019 a la fecha.

Descripción de Organismos afectados

Organismo afectado	Fecha	Consecuencias inmediatas / Información expuesta
Banco Nación	octubre 2019	Perjuicio económico aproximado: \$667.243,80
Dirección Nacional de Migraciones	septiembre 2020	Rescate exigido: hasta USD76 millones 22 carpetas, 2.200 documentos relativos a consulados embajadas, la Agencia Federal de Inteligencia y datos personales de al menos 25.723 ciudadanos argentinos e información sobre 161.707 radicaciones entre otros
RENAPER	octubre 2021	Rescate exigido: USD17.000 (0,29 BTC) Más de 45 millones de registros a la venta en la Dark Web: foto e información sensible de cada argentino
Senado de la Nación	enero 2022	Información relevante de la Cámara Alta, fotocopias completas de DNIs, firmas a mano alzada, licencias de conducir, números de CUIL, datos biométricos parciales
Poder Judicial de Chaco	febrero 2022	Todas las bases de datos y documentos críticos en los servidores y equipos afectados
INDEC - CENSO 2022	mayo 2022	Denuncias de filtración de información personal de los censados

3.1. Ataque informático al Banco Nación - octubre 2019

Descripción

En 2019, una persona ingresó a la plataforma de home banking del Banco de la Nación⁶ "desarrollada y operada por la firma Red Link S.A.", "se autenticó y mediante técnicas específicas para detectar vulnerabilidades en sistemas informáticos modificó a su favor la cotización del dólar dentro de su navegador". Luego, adquirió en las operaciones dólares a una cotización de \$5,695 (cuando la real era de \$56,95), y después los vendió a \$530,50 (cuando la real era de \$53,05), todo ello por un monto total de U\$S 11.800, lo que implicaría un perjuicio económico aproximado de \$667.243,80.- con solo mover la "coma" del valor.

La seguridad en los datos, comprende la confidencialidad, su tratamiento y conservación limitada. Lo contrario comporta una fuga indebida. En el caso particular, se advierte que hubo una falla en el ciclo de vida de desarrollo de software, responsabilidad de la entidad.

⁶ <https://www.telam.com.ar/notas/202012/537135-sobreseen-a-un-joven-que-manipulo-el-valor-del-dolar-para-denunciar-fallas-de-seguridad-informatica.html>

Se debe tener en consideración que, una vez detectado un ataque, al intentar solucionar las vulnerabilidades, cuanto más tarde se detecten las vulnerabilidades, mayor será su perjuicio. Situación que necesariamente debe ser advertida por quienes desarrollan y operan el home banking del Banco Nación. Sin embargo, lo sucedido indica en principio que hubo al menos una falla durante el ciclo de vida del sistema.

Análisis sobre los ciclos de desarrollo de software

El ciclo de desarrollo de los sistemas o ciclo de vida de los sistemas (SDLC: Systems Development Life Cycle) es un enfoque por etapas de análisis y de diseño que postula que el desarrollo de los sistemas mejora cuando existe un ciclo específico de actividades del analista y de los usuarios.

A su vez, el modelado de amenazas es una técnica formal, estructurada y repetible que permite determinar y ponderar los riesgos y amenazas a los que estará expuesta una aplicación y que puede aplicarse al ciclo de vida del desarrollo de software

Desde el punto de vista de la seguridad, y para el caso bajo análisis, las etapas más relevantes son:

- Análisis de requerimientos: Arquitectura, plataforma, marcos normativos, perfiles, niveles de acceso, acciones, modos de autenticación
- Diseño: Aunque por norma general se sigue una lista de “buenas practicas” también se deben aplicar técnicas de análisis de riesgos como Threat Modelling o el método **STRIDE**, que ayuda a identificar amenazas en los componentes de un sistema.
- Codificación (o programación): También hay una lista de buenas prácticas. Entre los tipos de vulnerabilidades más habituales y que directamente son producto de una codificación de mediano y bajo perfil podemos encontrar términos cada vez más familiares como SQL injection, Code injection, Cross Site Scripting (XSS) y buffer overflows
- Pruebas: En esta etapa deberían aplicarse varias técnicas tendientes a comprobar la seguridad de una aplicación, como ser: el test de seguridad funcional clásico, pruebas de mutación de datos, un test de seguridad basado en el Threat Modelling y otras.
- Implementación: Se suelen aplicar técnicas como hardening de software de base que comprende ir reduciendo vulnerabilidades.

El análisis de riesgos consiste, de forma muy resumida, en las siguientes actividades:

- Recopilación de los recursos que deben ser protegidos.
- Clasificación de los actores del proyecto. Cuáles son sus casos de uso y qué roles representan.
- Recopilación de requisitos legales y de negocio. Certificaciones que hay que cumplir, restricciones de encriptación o bien reglas de negocio más específicas.

Se destaca la técnica STRIDE dado que, como el acrónimo que su nombre es así lo indica, incluye específicamente el análisis de riesgos sobre “Tampering with Data”, que implica la modificación maliciosa de datos, e “Information Disclosure”, que es cuando se divulga información a usuarios no autorizados. Cuestiones que abarcan el caso bajo análisis.

Análisis sobre la vulnerabilidad

En el caso en estudio, diversas fuentes señalaron que el usuario modificó a su favor la cotización del dólar dentro de su navegador. En primera instancia, evaluamos que se trata de una explotación de vulnerabilidad como una Inyección de algún tipo (SQL, OS, LDAP, etc.), exposición de información sensible, Web Parameter Tampering o un Cross-site Scripting (XSS).

El Proyecto OWASP nos brinda el marco para evaluar objetivamente la gravedad de este y otro conjunto de vulnerabilidades web <https://owasp.org/www-project-top-ten/>

Ante esta situación, las posibilidades mencionadas se encuentran enmarcadas en el OWASP TOP 10 2021, principalmente dentro de las categorías referidas a inyección y fallas de diseño. Muchas aplicaciones web y APIs no protegen adecuadamente datos sensibles, tales como información financiera, de salud o Información Personal Identificable (PII) y, ante tales vulnerabilidades, los Actores de amenazas pueden robar o modificar estos datos para llevar a cabo fraudes con tarjetas de crédito, robos de identidad u otros delitos. Los datos sensibles requieren métodos de protección adicionales, como el cifrado en almacenamiento y tránsito, que reduzca la capacidad de daño a sus titulares.

El Web Parameter Tampering (ataque de manipulación de parámetros web) se basa en la manipulación de parámetros intercambiados entre cliente y servidor para modificar datos de la aplicación, como credenciales y permisos de usuario, precio y cantidad de productos, etc. Por lo general, esta información se guarda en cookies, de forma oculta, campos o cadenas de consulta de URL, y se utiliza para aumentar la funcionalidad y el control de la aplicación.

Para esta clase de ataques se utilizan principalmente herramientas como WebScarab y Paros proxy. Otras veces, basta con un add-on o extensión, según el navegador y el caso, que permita modificar la información a enviar al servidor. Su éxito depende de los errores del mecanismo de validación de integridad y lógica, y su explotación puede tener otras consecuencias, como XSS, inyección SQL, inclusión de archivos y ataques de divulgación de ruta.

En el siguiente ejemplo, provisto por la comunidad OWASP⁷, vemos en forma genérica una de las posibles formas en la que se pudo haber explotado la vulnerabilidad.

Un atacante puede alterar los parámetros de URL directamente. Considere una aplicación web que permite a un usuario seleccionar perfil y opciones de un cuadro combinado o formulario y debitar la cuenta:	http://www.atackbank.com/default.asp?profile=741&debit=1000
En este caso, podría manipular la URL utilizando otros valores para el perfil y el débito:	http://www.atackbank.com/default.asp?profile=852&debit=2000
Se pueden cambiar otros parámetros, incluidos los parámetros de atributos. Como ejemplo, es posible manipular la variable de estado y eliminar una página del servidor:	http://www.attackbank.com/savepage.asp?nr=147&status=read
O también, modificar la variable de estado para eliminar la página:	http://www.attackbank.com/savepage.asp?nr=147&status=del

⁷ https://owasp.org/www-community/attacks/Web_Parameter_Tampering

Ahora bien, si un producto web no protege adecuadamente los valores supuestamente inmutables en campos ocultos de formularios, parámetros, cookies o URL, esto puede conducir a la modificación de datos críticos. Las aplicaciones web a menudo suponen erróneamente que los datos pasados al cliente en campos ocultos o cookies no son susceptibles de manipulación. La validación incorrecta de los datos que son controlables por el usuario puede hacer que la aplicación procese entradas incorrectas y, a menudo, maliciosas.

Es por ello que se debe hacer énfasis en la ampliación de los mecanismos de protección que garanticen el respeto al principio de Seguridad de los Datos. Sin los mecanismos de protección adecuados el cliente puede manipular fácilmente las cookies y datos web similares. Confiar en los envíos del cliente sin una validación detallada puede dar lugar a violaciones de las políticas de seguridad en el lado del servidor (como eludir la autenticación, la suplantación de identidad del usuario y la escalada de privilegios), con la posibilidad suplementaria de dar lugar a la divulgación de datos confidenciales del usuario.

Entonces, encontrándose disponible la información sobre la cotización del dólar en múltiples fuentes accesibles desde el lado del servidor que provee el servicio de homebanking del Banco Nación, surgen inquietudes en cuanto a los criterios empleados durante el desarrollo que llevaron a depender del usuario (del navegador) para informar la cotización de la moneda estadounidense.

Finalmente, con la información disponible y lo hasta aquí explicado, se entiende que la implementación inadecuada del ciclo de vida de desarrollo seguro posibilitó al usuario/atacante a efectuar con éxito un Web Parameter Tampering

3.2. Ataque informático a la Dirección Nacional de Migraciones - septiembre 2020

Descripción

En septiembre de 2020, información de la Dirección Nacional de Migraciones fue robada y luego publicada en Internet por actores de amenazas que vulneraban el sistema, después que el Gobierno no pagara el rescate de entre 4 y 76 millones de dólares para devolver la información y no hacerla pública. El rescate debía abonarse antes del miércoles 9 de septiembre⁸ pero el gobierno se negó a negociar y los denunció penalmente por extorsión, daño informático y acceso ilegítimo.



Vista parcial del blog de Netwalker, en aquella época

⁸ <https://viapais.com.ar/argentina/1988669-hackeo-a-migraciones-el-gobierno-no-pago-y-publicaron-la-informacion-robada/>

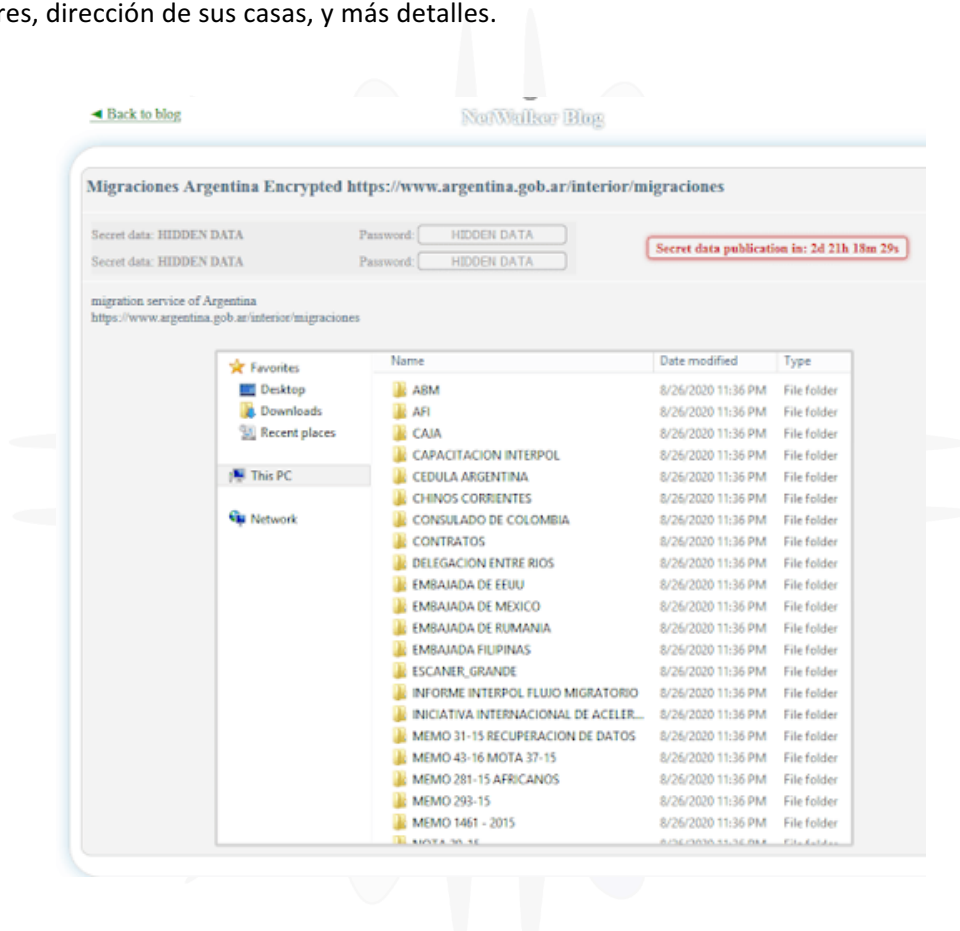
⁹ <https://www.infobae.com/tecno/2020/09/10/vencio-el-plazo-y-los-hackers-publicaron-la-informacion-robada-a-migraciones/>

Los datos fueron publicados en el blog de Netwalker dentro de un archivo comprimido de 1,8 GB, alojados en DropMeFiles.

Según una captura de pantalla^{10 11} del sitio en la Dark Web, los hackers codificaron **22** carpetas, **2.200** documentos¹², con información relativa a la Agencia Federal de Inteligencia (AFI), flujos migratorios, **consulados** y **embajadas**.

El ataque afectó en particular al Sistema Integrado de Captura Migratoria (SICaM), el cual es utilizado en los pasos internacionales para “el control y el registro informático” de las personas, argentinas o extranjeras, que ingresan y egresan del territorio nacional.

Uno de los documentos es una tabla con datos de **25.723** argentinos que regresaron al país durante la cuarentena. Contiene no sólo sus datos personales, sino también correos, teléfonos celulares, dirección de sus casas, y más detalles.



En la misma carpeta constaban distintas planillas de Excel en la que se daban a conocer identidades de ciudadanos de otros países que entraron o salieron del país durante el Aislamiento Social Preventivo y Obligatorio (ASPO)

¹⁰ <https://www.infobae.com/tecno/2020/09/10/vencio-el-plazo-y-los-hackers-publicaron-la-informacion-robada-a-migraciones/>

¹¹ <https://www.infobae.com/sociedad/policiales/2020/09/10/la-identidad-de-cuatro-agentes-de-la-afi-el-ingreso-de-un-violador-a-mendoza-y-una-red-de-trata-proveniente-de-india-que-dicen-los-archivos-que-los-hackers-le-robaron-a-migraciones/>

¹² https://www.clarin.com/tecnologia/ciberataque-migraciones-espas-sicarios-trata-chinos-datos-privados-miles-personas_0_qIAOxPSfV.html

Asimismo, se dejó al descubierto la identidad de cuatro integrantes de la Agencia Federal de Inteligencia (AFI) y el nombre de uno de sus directores.

ESTRICTAMENTE SECRETO Y CONFIDENCIAL

MEMORANDO

PARA INFORMACIÓN DE:

*Dirección Operacional de Inteligencia
sobre Terrorismo y Delitos contra
el Orden Constitucional*

PRODUCIDO POR:

*Dirección de Inteligencia
Antiterrorista*

Buenos Aires, 1 de febrero de 2016

Asunto: Solicitar reseteo claves DNM

Elevo para su conocimiento y efectos la solicitud de reseteo de las claves otorgadas por la Dirección Nacional de Migraciones a los agentes autorizados de esta D.I.A. para realizar las consultas en la base de datos del citado organismo.

Motiva el requerimiento, el hecho que las claves otorgadas en NOV2015 han sido bloqueadas por la D.N.M. por razones de seguridad.

Los agentes autorizados por esta D.I.A. son:

Entre los archivos filtrados se conoció un informe reservado de la dirección de Asuntos Consulares del Ministerio de Relaciones Exteriores y Culto, dirigido a Migraciones, sumado a un documento interno de Migraciones que informaba la cantidad de extranjeros radicados en el país y la procedencia de cada uno de ellos.

DNM - RADICACIONES RESUELTAS - AÑO 2019				
NACIONALIDAD	PERMANENTE	TEMPORARIA	TOTAL	%
1 VENEZOLANA	18.180	46.894	65.074	40,24
2 PARAGUAYA	14.324	11.208	25.532	15,79
3 BOLIVIANA	13.619	11.627	25.246	15,61
4 PERUANA	4.923	5.120	10.043	6,21
5 COLOMBIANA	4.178	5.666	9.844	6,09
6 BRASILEÑA	5.687	810	6.497	4,02
7 ECUATORIANA	804	1.886	2.690	1,66
8 CHILENA	888	1.432	2.320	1,43
9 CHINA	1.173	690	1.863	1,15
10 URUGUAYA	812	972	1.784	1,10
11 ESTADOUNIDENSE	370	1.254	1.624	1,00
12 MEXICANA	299	1.062	1.361	0,84
13 ESPAÑOLA	282	1.009	1.291	0,80
14 FRANCESA	138	529	667	0,41
15 ITALIANA	168	408	576	0,36
16 DOMINICANA	368	203	571	0,35
17 HAITIANA	138	320	458	0,28
18 CUBANA	216	235	451	0,28
19 ALEMANA	82	216	298	0,18
20 SALVADOREÑA	40	231	271	0,17
OTRAS NACIONALIDADES	843	2.403	3.246	2,01
Total general	67.532	94.175	161.707	100,00

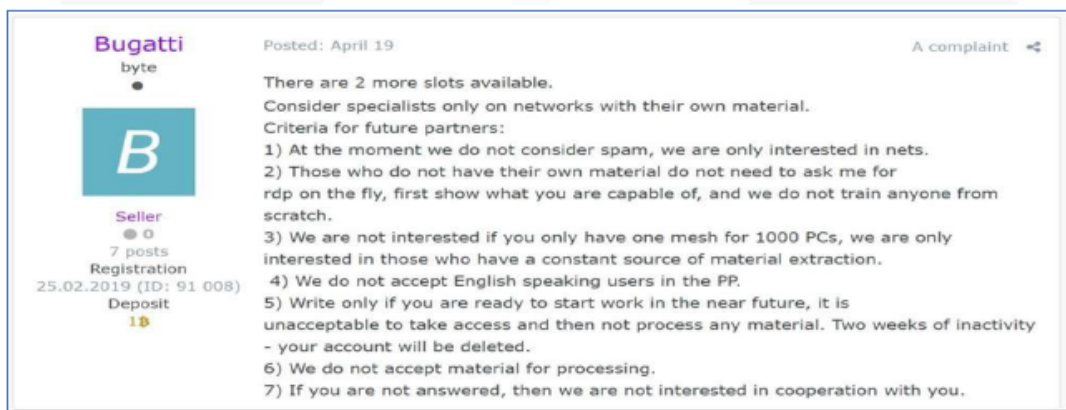
Las acciones descriptas dejaron al descubierto la necesidad de una mayor seguridad en el manejo de datos, que garanticen la confidencialidad, almacenamiento y tratamiento de los mismos, permitiendo generar un “Flujo transfronterizo de Datos y Responsabilidad” controlado, dentro del Estado Nacional, conforme las recomendaciones de la Organización de Estados Americanos (OEA).¹³

Descripción general de NetWalker

Descubierto en agosto de 2019, NetWalker es, inicialmente, un tipo de Ransomware específico para Windows que cifra y extrae todos los datos que viola. Creado por un grupo de ciberdelincuencia llamado Circus Spider¹⁴ ha tenido éxito al distribuirse mediante phishing o VBScript

NetWalker ha evolucionado notablemente desde un concepto de carga útil o payload, o modelo de Recurso, hacia un modelo de Ransomware como Servicio (RaaS) más estable y robusto, investigaciones de empresas como McAfee¹⁵ (informe del **03/08/2020**) sugieren que los operadores de malware apuntaron a convocar criminales técnicamente avanzados y emprendedores a través un programa de afiliado en el que se verifica a los solicitantes antes de que sean aceptados.

Por ello, en su modalidad RaaS, el grupo detrás de NetWalker priorizo la calidad sobre la cantidad y busco personas que hablen ruso y tengan experiencia con grandes redes. También eran especialmente buscadas las personas que ya tenían un punto de apoyo en la red de una víctima potencial y podían filtrar datos con facilidad.



El grupo del malware exhibía un estricto "código de conducta" que prohibía su utilización contra Rusia o la Commonwealth of Independent States (CIS)¹⁶. Como nota de color, el sitio que utilizaron para publicar la información extraída de Migraciones, DropMeFiles¹⁷, está registrada en www.nic.ru

¹³ [https://www.oas.org/es/sla/cji/docs/Publicacion Proteccion Datos Personales Principios Actualizados 2021.pdf](https://www.oas.org/es/sla/cji/docs/Publicacion%20Proteccion%20Datos%20Personales%20Principios%20Actualizados%202021.pdf), pág. 77.

¹⁴ <https://www.logpoint.com/en/blog/in-depth-look-at-the-netwalker-ransomware-operators/>

¹⁵ <https://www.mcafee.com/blogs/other-blogs/mcafee-labs/take-a-netwalk-on-the-wild-side/>

¹⁶ <https://blog.segu-info.com.ar/2020/09/netwalker-como-fue-el-ataque.html?m=0>

¹⁷ <https://www.whois.com/whois/dropmefiles.com>

Los montos exigidos han oscilado entre USD 1.000 y USD 3.000.000 y se practicaban tácticas de doble extorsión mediante las cuales los afiliados exigían dinero por descifrar archivos y por no difundir los datos filtrados.

En febrero de 2021¹⁸, funcionarios búlgaros confiscaron un servidor utilizado para albergar portales de la Dark Web para la banda NetWalker, mientras que los funcionarios en los EE.UU. Acusaron a un ciudadano canadiense, Sebastien Vachon-Desjardins, que supuestamente ganó al menos 27,6 millones de dólares infectando empresas con el Ransomware. La acción policial internacional coordinada incluyó la incautación de casi medio millón de dólares en criptomonedas¹⁹



Página de inicio del sitio de la Dark Web incautado

Programado en PowerShell afín de ser ejecutado en memoria y así evadir la detección, cuando compromete una red apunta a encriptar todos los dispositivos Windows conectados a ella. El Ransomware agrega una extensión aleatoria a los archivos de interés cifrándolos mediante el algoritmo Salsa20^{20 21}.

Para evitar la detección implementa -entre otras-, una técnica de evasión de defensa conocida como carga reflexiva de DLL, que inyecta una DLL directamente en el espacio de memoria del proceso explorer.exe.

¹⁸ <https://blog.ehcgroupp.io/2021/02/03/10/37/12/10567/interrumpen-la-red-del-ransomware-netwalker/seguridad-informatica/ransomware/ehacking/>

¹⁹ <https://blog.chainalysis.com/reports/netwalker-ransomware-disruption-arrest/>

²⁰ <https://openarchive.usn.no/usn-xmlui/bitstream/handle/11250/2730004/Master2020Knutson.pdf?sequence=1&isAllowed=y>

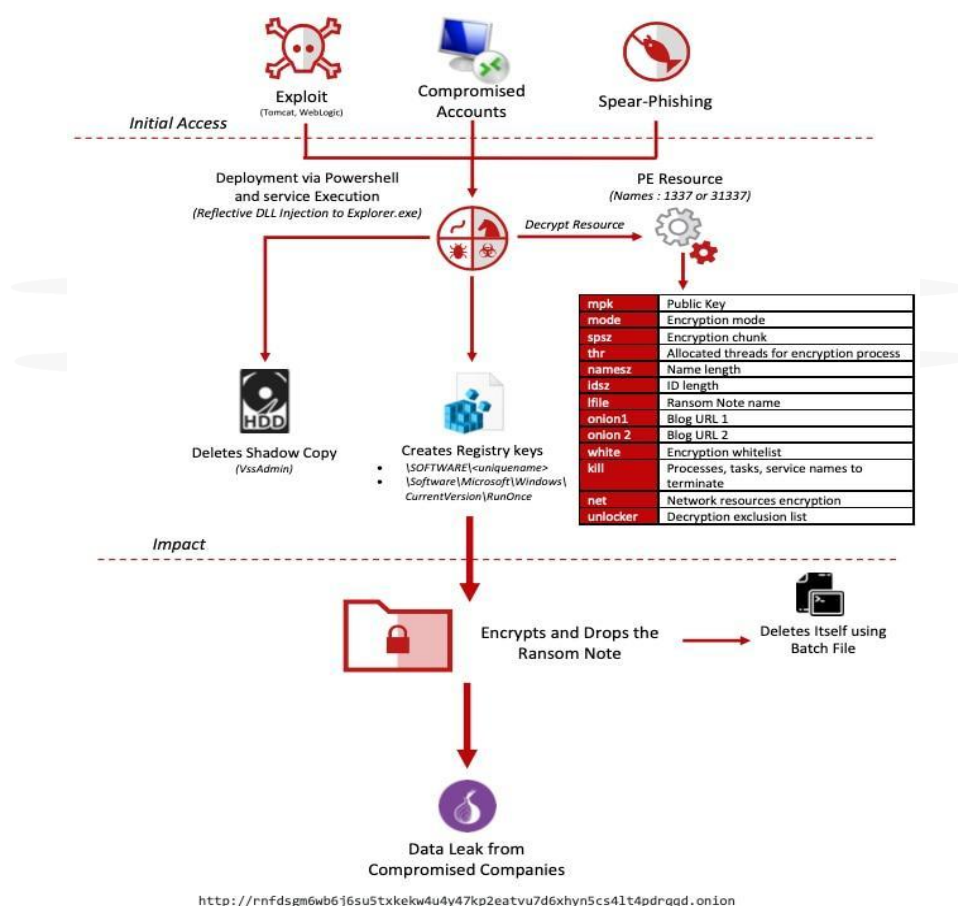
²¹ <https://blog.cryptographyengineering.com/2012/10/09/so-you-want-to-use-alternative-cipher/>

La lista completa de técnicas, tácticas y procedimientos (Tactics, Techniques, and Procedures – TTPs) específicas empleadas para el desarrollo de este Ransomware se pueden ver en el sitio web de MITRE por medio del siguiente link:

<https://attack.mitre.org/software/S0457/>

Mediante diversas fuentes se indicó que NetWalker accedía de dos maneras:

- A través de un dropper²² desarrollado en Visual Basic Script (VBS) que se adjunta a correos electrónicos de phishing (con algún asunto referido a Coronavirus, generalmente) que ejecutan la carga útil del Ransomware una vez que se hace doble clic o abriendo los documentos de Office que contienen el script VBS en su interior; o,
- A través de un archivo ejecutable que se ha difundido en la red y que un usuario descuidado haya ejecutado.



Esquema general de NetWalker (Fuente->McAfee²³)

²² <https://www.incibe.es/protege-tu-empresa/blog/dropper-amenaza-silenciosa>

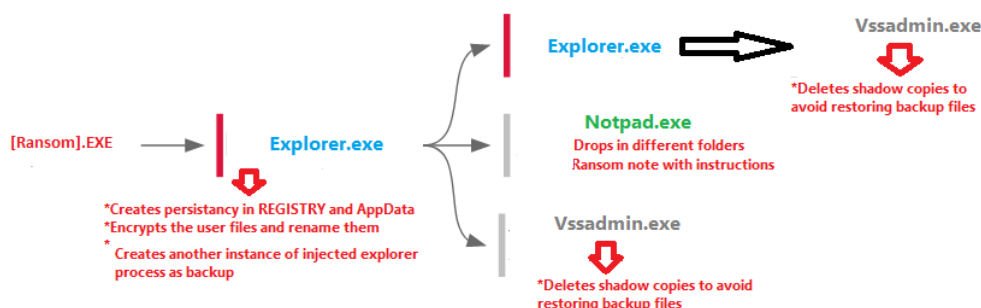
²³ <https://www.mcafee.com/blogs/other-blogs/mcafee-labs/take-a-netwalk-on-the-wild-side/>

La tercera vía de acceso que puede darse, es que un actor de amenazas localice una máquina visible desde internet, utilice con éxito una vulnerabilidad y, una vez penetrada una organización, explore la red, distribuyendo un dropper para el Ransomware en sí.

Obtenido el acceso, los afiliados pueden orquestar ataques utilizando secuencias de comandos por lotes que se ejecutan, con la ayuda de controladores de dominio²⁴, en cualquier máquina a la que pueda llegar tal controlador de dominio (muchas veces, toda la red de la organización objetivo). Los scripts bajan al dispositivo objetivo las cargas útiles de los atacantes mediante psexec o certutil. Alternativamente, ellos mismos distribuyen el ejecutable del Ransomware dentro de la red objetivo, intentando copiarlo en todas las máquinas a las que pueden acceder

Luego, la ejecución del Ransomware NetWalker se lleva a cabo en cuatro fases²⁵:

- El código malicioso importa las funciones de las librerías de Windows que usará durante el resto de la ejecución.
- El fichero de configuración del Ransomware, donde se encuentran diversos parámetros relativos al cifrado y rescate, se extrae de los recursos del ejecutable.
- Inicialización de variables, tales como el identificador del usuario afectado. Se eliminarán las instantáneas de volumen ejecutando vssadmin.exe en una ventana oculta, con el objetivo de impedir que se puedan recuperar los ficheros cifrados desde la copia de seguridad generada por el servicio VSS (Volume Shadow Copy)
- Procedimiento principal donde se llevaría a cabo el proceso de cifrado de archivos. Se genera un identificador único de 6 caracteres (ID del usuario afectado) que utiliza como extensión para los archivos cifrados y como parte del nombre de las notas de rescate



Análisis particular sobre el caso.

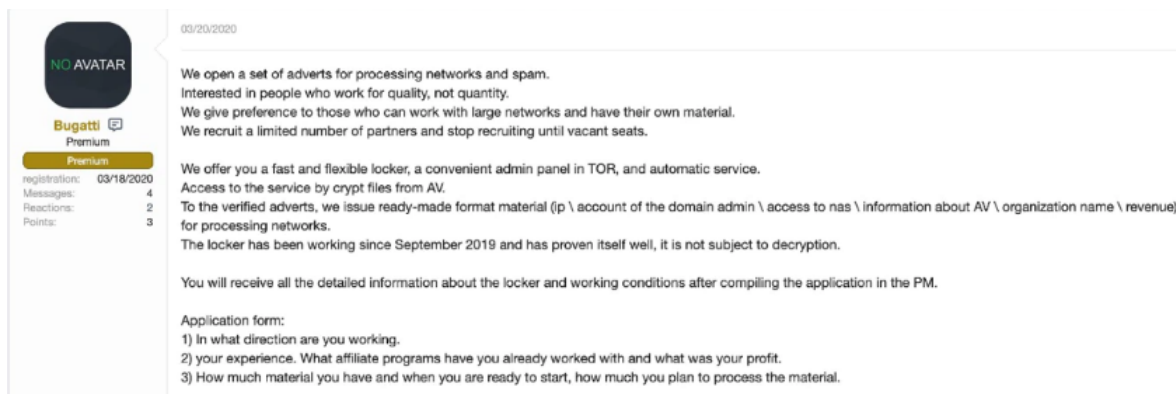
Cabe destacar que, en el modelo "Ransomware as a Service" (RaaS) el actor de amenazas que obtuvo acceso no necesariamente es quien retiene el entorno para pedir rescate. Hay casos de malware diseñados para diseminarse rápidamente a través del entorno, generar y retener un acceso y operar en un contexto de botnet. Luego, el acceso que brinda el malware es vendido en la Dark Web²⁶

²⁴ Un controlador de dominio (DC) es un servidor que responde a las solicitudes de autenticación de seguridad dentro de un dominio de Windows Server, autentica a los usuarios, almacena la información de la cuenta del usuario y aplica la política de seguridad para un dominio de Windows controlando el acceso del host a los recursos del dominio de Windows.

²⁵ <https://www.incibe-cert.es/blog/ransomware-netwalker- analisis-y-medidas-preventivas>

²⁶ <http://ransomware.org/blog/anatomy-of-a-ransomware-attack/>

A su vez, teniendo en cuenta los objetivos fijados por el actor de amenazas identificado como Bugatti²⁷, teóricamente miembro del grupo desarrollador, quien ha promocionado activamente a NetWalker como RaaS en foros de la Dark Web, el modelo de operación de Netwalker no asegura que haya una lista explícita de objetivos, sino que se delega la elección de los mismos en los afiliados.



03/20/2020

Bugatti Premium

registration: 03/18/2020
Messages: 4
Reactions: 2
Points: 3

We open a set of adverts for processing networks and spam.
Interested in people who work for quality, not quantity.
We give preference to those who can work with large networks and have their own material.
We recruit a limited number of partners and stop recruiting until vacant seats.

We offer you a fast and flexible locker, a convenient admin panel in TOR, and automatic service.
Access to the service by crypt files from AV.
To the verified adverts, we issue ready-made format material (ip \ account of the domain admin \ access to nas \ information about AV \ organization name \ revenue) for processing networks.
The locker has been working since September 2019 and has proven itself well, it is not subject to decryption.

You will receive all the detailed information about the locker and working conditions after compiling the application in the PM.

Application form:
1) In what direction are you working.
2) your experience. What affiliate programs have you already worked with and what was your profit.
3) How much material you have and when you are ready to start, how much you plan to process the material.

Lo anterior se soporta en un trabajo de la firma SophosLabs²⁸. El acceso inicial se efectúa por tres caminos alternativos:

- Phishing por e-mail;
- explotando vulnerabilidades de servidores web Apache Tomcat u Oracle Weblogic; o,
- contraseñas RDP²⁹ débiles.

Los especialistas destacan el aprovechamiento de una vulnerabilidad de ejecución de código remoto que afecta a sistemas Windows Server y Windows 10, entre otros: CVE-2020-0796

Por otro lado, de observaciones sobre la fecha y hora de las carpetas³⁰ de Migraciones contenidas en el archivo difundido por “Netwalker”, se puede estimar el tiempo que tomó la descarga y, a partir de ello, también la velocidad de descarga aproximada³¹, como aquella que se realizó el 27/08/2020 entre las 3:36 AM y 3:55 AM (UTC-3, franja horaria argentina). Los 1,96 GB de información se transfirieron en alrededor de 19 minutos a un promedio aproximado de 13 Mb/s. Dos horas después, aproximadamente, a las 06:11 AM del 27/08/2020 (UTC-3), la información de Migraciones ya estaba alojada en DropMeFiles.

Teniendo en cuenta ello, las herramientas ofrecidas por Bugatti, la información suministrada por las matrices ATT&CK, publicadas por MITRE³² y Sophos³³, y lo mencionado sobre las fases de

²⁷ <https://www.mcafee.com/blogs/other-blogs/mcafee-labs/take-a-netwalk-on-the-wild-side/>

²⁸ <https://news.sophos.com/en-us/2020/05/27/netwalker-ransomware-tools-give-insight-into-threat-actor/>

²⁹ https://en.wikipedia.org/wiki/Remote_Desktop_Protocol

³⁰ https://www.clarin.com/tecnologia/ciberataque-migraciones-espias-sicarios-trata-chinos-datos-privados-miles-personas_0_qIAOxPSfv.html

³¹ <https://blog.segu-info.com.ar/2020/09/netwalker-como-fue-el-ataque.html?m=0>

³² <https://www.mcafee.com/blogs/other-blogs/mcafee-labs/take-a-netwalk-on-the-wild-side/>

³³ <https://news.sophos.com/en-us/2020/05/27/netwalker-ransomware-tools-give-insight-into-threat-actor/>

ejecución de Netwalker, se concluye que el envío de la información se efectuó bajo supervisión del actor de amenazas.

Por todo lo expresado, se evalúan dos escenarios:

- Un actor de amenazas se infiltró en la red con bastante anterioridad, con tiempo suficiente para lateralizar, obtener la información y propagar el Ransomware; o,
- Directamente, un afiliado a Netwalker ejecutó el malware luego de penetrar la red y filtrar la información

Cabe mencionar, además, que los atacantes lograron comprometer SYSVOL de Active Directory y el System Data Center Protection Manager. Surgen entonces dos interrogantes serios: Primero, no hay evidencia que sostenga o refute un número específico de equipos afectados en esa red, pero como mínimo afectaron al controlador de dominio; Segundo, un escenario peor, no sabemos desde cuando estuvo comprometida la red ni si generaron backdoors o se integraron algunos de los elementos de la misma a una botnet.

El razonamiento y las conclusiones previas se sostienen por inteligencia de un caso similar^{34 35}, donde Stealth analizó un ataque en el que los actores de Netwalker instalaron Google Chrome en un servidor de archivos pirateado, aproximadamente 3 horas antes de que desinstalaran la solución de seguridad endpoint y ejecutarán el Ransomware.

Aunque por todo lo expuesto sería razonable asumir que la red fue comprometida el día 26 de agosto 2020, otra fuente señala que los sistemas ya habían sido penetrados por lo menos desde junio de 2020, por cuanto desde un acceso remoto se había generado el usuario “admin.cfeijoo”³⁶. Una hipótesis señalaría que al menos un actor de amenazas retuvo acceso a la red de migraciones desde entonces hasta el incidente Netwalker, y que serían estos los últimos que habrían utilizado ese acceso irregular.

3.3. Ataque informático al RENAPER - octubre 2021

Descripción

El 24 de octubre de 2021, tomó estado público que la base de datos del Registro Nacional de las Personas, RENAPER, fue comprometida y la información de millones de argentinos estaba a la venta en la Dark Web. En la cuenta de Twitter del usuario @aniballeaks (suspendida actualmente) podían verse las fotos y los datos del documento de periodistas, políticos, deportistas y artistas reconocidos, entre otros.

³⁴ <https://twitter.com/falsneg/status/1337148946536226816>

³⁵ <https://drive.google.com/file/d/1enZhQQt4m4dd5nibKyT-LDTmsz6BEI/edit>

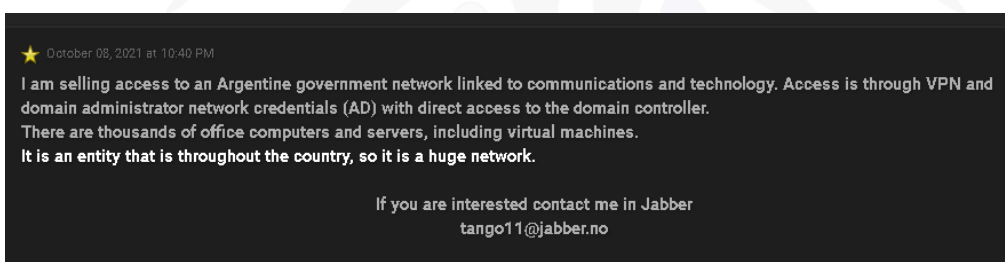
³⁶ <https://www.lanacion.com.ar/politica/hackear-al-estado-asi-operan-las-ciberbandas-que-secuestran-bases-de-datos-y-exigen-rescate-nid24022022/>



En algunos casos³⁷ también aparecía el número de trámite del documento, comportando un dato sensible expuesto ya que, por la pandemia, muchas gestiones comenzaron a hacerse de forma virtual, siendo imprescindible la carga de ese número para acceder a los trámites.

Debe considerarse que a la base de datos del RENAPER tienen acceso decenas de organismos públicos y empresas privadas, que realizan consultas permanentemente para validar datos de distintas operaciones. Y en este caso, el mejor ejemplo es la **App CuidAr** -uno de los principales usuarios de esa base de datos-, quien utiliza el número de trámite de documento como código de validación adicional, de forma similar a cuando se solicita el código de seguridad para las tarjetas de crédito, tal como se explicó en el “Informe Especial Sobre Aplicaciones de Seguimiento Covid-19”³⁸.

Cabe destacar que antes de que tome estado público³⁹, la información se encontraba en venta y no se requería de un navegador Tor (navegador especialmente preparado para navegar por la Dark Web) para hallarla.⁴⁰



³⁷ <https://www.infobae.com/politica/2021/10/31/cuales-son-las-principales-hipotesis-detras-del-hackeo-a-la-base-del-renaper/>

³⁸ <http://fundacionled.org/wp-content/uploads/2020/07/Informe-Aplicaciones-de-Seguimiento-F-LED.pdf>

³⁹ <https://therecord.media/https://therecord.media/wp-content/themes/therecordmedia/1707>

⁴⁰ https://rfmirror.com/Thread-SELLING-Argentina-ID-Card-data-45M?_cf_chl_captcha_tk=_pmd_Pvlhe4mkEKYlGpWqSonkLAuWHgVpE671S5vhqLv9pDQ-1634230526-0-gqNtZGzNAzujcnBsZQjR

El 10 de octubre, se filtró una muestra de 60.000 registros, con secuencia de DNI correlativa. Se trata de un archivo de 2,55 GB con 26 campos por registro, incluida la foto. El análisis de la muestra indicaría que el actor de amenazas tuvo acceso a la base al menos hasta principios de octubre.



Durante la pandemia, el Ministerio de Salud de la Nación y aplicaciones del gobierno como **CuidAR** fueron unos de los principales usuarios de esa base de datos. El organismo habilitó una docena de datos de cada argentino para que la cartera sanitaria pueda consultarlos en la base a través de credenciales informáticas. Salud, a su vez, extendió ese permiso a cientos de actores internos de todo el país, que cargan los resultados de los test de COVID-19 y vacunación en el sistema integrado de salud **SISA**⁴¹, cantidad de consultas que oscilan entre **600.000** y **800.000** por día.

Por otra parte, viene al caso destacar la **vulnerabilidad descubierta en la app Mi Argentina** por el investigador de seguridad cordobés Dan Borgogno⁴², quien demostró en el evento de ciberseguridad EkoParty 2020 cómo dentro de la app **se podía mostrar el DNI de cualquier persona o generar uno totalmente falso**. Esta vulnerabilidad permitía acceder a datos del RENAPER que deberían estar protegidos.⁴³

Además de la entrevista con The Record, otras personas contactaron con el vendedor y terminaron avalando que realmente poseía la información que decía^{44 45}

Servicios de validación de identidad del RENAPER y su seguridad

El número de trámite del DNI argentino, es único e irrepetible para cada habitante y cambia con cada versión del mismo. En base a ese número se tiene acceso a diversos trámites, como negar la salida del país a una persona, controlar gestiones o incluso poner que alguien sufre de COVID-19.⁴⁶

⁴¹ <https://www.infobae.com/politica/2021/10/31/cuales-son-las-principales-hipotesis-detras-del-hackeo-a-la-base-del-renaper/>

⁴² <https://www.infobae.com/tecnologia/2020/09/24/es-posible-hackear-el-dni-digital/>

⁴³ <https://www.rosario3.com/informaciongeneral/Filtracion-de-la-base-del-Renaper-el-verdadero-robo-del-siglo-20211016-0001.html>

⁴⁴ <https://urgente24.com/actualidad/alerta-el-hackeo-al-renaper-como-protejo-mis-datos-n528620>

⁴⁵ <https://www.infobae.com/politica/2021/10/31/cuales-son-las-principales-hipotesis-detras-del-hackeo-a-la-base-del-renaper/>

⁴⁶ <https://www.tecnogeek.com/2021/10/14/argentina-renaper-habria-sufrido-un-hackeo-y-venta-de-datos-personales-de-los-ciudadanos/>

Tal como se refirió en el punto anterior, a la base del RENAPER tienen acceso decenas de organismos públicos y empresas privadas que realizan consultas permanentemente al Sistema de Identidad Digital (SID)⁴⁷, que opera mediante una **cesión de datos**⁴⁸ a través de servicios web, para validar datos para distintas operaciones informáticas, que abarcan desde trámites hasta compras con tarjeta de crédito.

Los Servicios de Validación de Identidad del RENAPER permiten, en tiempo real, a las empresas y organismos otorgar productos o servicios que requieren validar identidad de forma remota. Por supuesto, las entidades que deseen acceder al SID deberán cumplir con la Ley N° 25.326 de Protección de Datos Personales y sus Disposiciones complementarias.

El RENAPER, según el mismo lo informa, provee un SDK con el que se podrán llevar adelante las siguientes alternativas para completar el proceso de validación:

- a) Identificación con documento de identidad, vigencia del mismo y biometría facial
- b) Identificación con biometría facial sin tarjeta DNI
- c) Identificación mediante vigencia del documento con tarjeta DNI
 - a. El ciudadano ingresa de forma manual el número de su documento, género y **número de trámite** que figura en su DNI.
 - b. El SDK recibe esos datos y envía la información al sistema del RENAPER para obtener la vigencia del documento de identidad.

Ante lo expuesto, surge la cuestión sobre qué grado de seguridad informática efectivamente se requiere. En ciberseguridad, actualmente se procede sobre un paradigma de cuatro niveles^{49 50}:

1. Seguridad Básica: Antivirus + Firewall + Backup y actualizaciones
2. Seguridad Avanzada: Cifrado, 2FA, Sistema de prevención de pérdida de datos (DLP)⁵¹, Sistemas de detección/prevenición de intrusiones (IPS/IDS)⁵². Análisis de riesgo, Políticas de seguridad
3. Seguridad Integral: Logs, Endpoint Detection and Response⁵³, Pentest, Evaluación de vulnerabilidades, Gestión Integral y Auditorías
4. Ciberinteligencia: Registros + IoC⁵⁴ + Analisis, Ejercicios de Red Team/Blue Team

De acuerdo a esta clasificación, y a lo informado por el mismo RENAPER⁵⁵, la seguridad de la solución **SID es del tipo 2 o simplemente “Seguridad Avanzada”**

⁴⁷ <https://www.argentina.gob.ar/interior/renaper/sid-sistema-de-identidad-digital>

⁴⁸ <https://www.argentina.gob.ar/sid/proceso-de-verificacion>

⁴⁹ https://www.redseguridad.com/actualidad/ciberseguridad/cybersecurity-open-day-la-evolucion-de-la-digitalizacion-y-la-ciberseguridad-open-week_20210421.html

⁵⁰ https://www.redseguridad.com/canal-redseguridad/eventos/asi-fue-cybersecurity-open-day-ciberseguridad_20210507.html

⁵¹ <https://www.incibe.es/protege-tu-empresa/blog/dlp-protege-tus-datos-fugas-informacion>

⁵² <https://www.incibe.es/protege-tu-empresa/blog/son-y-sirven-los-siem-ids-e-ips>

⁵³ <https://www.cisco.com/c/en/us/products/security/endpoint-security/what-is-endpoint-detection-response-edr-medr.html>

⁵⁴ https://es.wikipedia.org/wiki/Indicador_de_compromiso

⁵⁵ <https://www.argentina.gob.ar/sid/seguridad>

Sobre la divulgación de más de 45 millones de registros de los ciudadanos argentinos

De acuerdo a una entrevista realizada con el medio Rosario3, en octubre del 2021, se le consultó al responsable del hecho sobre diferentes cuestiones. Desde lo técnico y en el marco de la exposición de la información de los ciudadanos argentinos que gestiona RENAPER, se destacan las siguientes:

a) ¿Y respecto a las credenciales de acceso al RENAPER? Supongo que habrás entrado con credenciales válidas y descargado la base.

“Si, tengo varias de diferentes entidades, se venden desde hace años. Uno puede dumper las bases de datos con diferentes credenciales, ir rotando para no hacer tanto ruido. Como esto no es nuevo, me dio el tiempo suficiente para dumper todos los registros. Creen que revocando los accesos al Ministerio de Salud solucionaron todo...”

b) ¿Cuál sería el peor escenario de lo que se puede hacer con los datos del RENAPER?

“Los carders⁵⁶ compran y venden esos datos todo el tiempo, los usan para sacar préstamos, abrir cuentas bancarias para mover plata sucia. Con la base de datos de IOSFA que publiqué hace unos días ya tenes mas de un millón de personas para hacerles spam al mail o celular, ingeniería social de todo tipo para sacarles plata.”

c) ¿Crees viable la confección de DNIs falsos?

“Descartando el dato biométrico de la huella, se pueden falsificar perfectamente.”

```
[26.10.2021 16:17:40] che, no tenes miedo que te atrapen?  
[26.10.2021 16:18:35] <tango11> No, eso no es posible y te explico por que  
[26.10.2021 16:19:26] <tango11> Hay recursos como Tor Project o Criptos, servidores en  
países donde jamás le darían pelota a la justicia argentina  
[26.10.2021 16:19:42] <tango11> Uno puede crear una cadena de servidores de tal  
forma que el anonimato este asegurado  
[26.10.2021 16:20:05] si tal cual, y respecto a las credenciales de acceso al  
renaper?  
[26.10.2021 16:20:25] supongo que habrás entrado con credenciales válidas  
(de las cientos que debe haber circulando)  
[26.10.2021 16:20:34] y descargado la base  
[26.10.2021 16:21:22] <tango11> Si tengo varias de diferentes entidades, se venden  
desde hace años  
[26.10.2021 16:21:45] <tango11> Uno puede dumper las bases de datos con diferentes  
credenciales, ir rotando para no hacer tanto ruido
```

```
[26.10.2021 17:06:20] qué medidas de seguridad tomas para que no te  
atrapen?  
[26.10.2021 17:06:52] y que SO usas?  
[26.10.2021 17:07:09] <tango11> Pensar como la policía, eso es lo primero para decidir  
bien que medidas, herramientas usar  
[26.10.2021 17:07:25] <tango11> En este momento Ubuntu  
[26.10.2021 17:07:36] <tango11> Cada conexión que entra y sale pasa por Tor  
[26.10.2021 17:07:55] <tango11> Estoy conectado a esta cuenta en un servidor Windows  
al que me conecto por escritorio remoto  
[26.10.2021 17:08:13] ah claro  
[26.10.2021 17:08:15] <tango11> Ese servidor Windows fue comprado con XMR.  
[26.10.2021 17:08:55] <tango11> Pobre al que le haya tocado buscarme  
[26.10.2021 17:09:37] debes tener varios que te siguen el rastro... no te pone  
un poco nervioso? no tenés miedo que algún día te tumben la puerta?  
[26.10.2021 17:10:03] <tango11> También es otra buena medida no tener prácticamente  
nada en la pc, usar servidores comprados con cripto
```

La primera cuestión requiere definir si se trató de un robo hormiga o si la información fue descargada de una vez. Cabe mencionar que, a un mes del incidente, los investigadores no tenían certezas sobre la extensión de la filtración ni tampoco cómo accedió quien robó los datos, o si fueron una o más personas.⁵⁷ Oficialmente se indicó que no se detectó un aumento

⁵⁶ quienes hacen uso no autorizado de tarjetas de crédito y/o cuentas bancarias de terceros

⁵⁷ <https://www.infobae.com/politica/2021/10/31/cuales-son-las-principales-hipotesis-detras-del-hackeo-a-la-base-del-renaper/>

significativo en la cantidad de consultas en los días previos a que se hiciera público el robo de datos Sin embargo, ante la pregunta de si es factible que hubiera tenido acceso a credenciales de múltiples entidades con potencial acceso a la información en poder del RENAPER. La respuesta corta es: SI.

A modo de ejemplo, la siguiente imagen es parte del “Intelligence Report” de la organización DarkTracer correspondiente al cuarto trimestre de 2021, muestra parte de un listado de **137 sitios “.gob.ar”**, atacados por algún malware tipo Stealer⁵⁸ (como Redline, por ejemplo), de donde se han obtenido un total de **30.409 credenciales**.

Stealer Malware Intelligence Report - Government(~ Q4 2021)		
https://darktracer.com		
https://twitter.com/darktracer_int		
support@darktracer.com		
1,753,658 credentials of 49,880 government sites have been leaked from users infected with Stealer malware.		
The users may include government users or public users of government public services		
No	Government Domain	Leaked credentials
12	auth.afip.gob.ar	12,011
31	servicioscorp.anses.gob.ar	6,105
102	id.argentina.gob.ar	2,288
266	becasprogresar.educacion.gob.ar	968
406	clusterapw.agip.gob.ar	617
454	www.sube.gob.ar	548
502	progresar.educacion.gob.ar	497
603	login.abc.gob.ar	416
626	autenticar.gob.ar	404
640	lbapw.agip.gob.ar	394
724	miba.buenosaires.gob.ar	347
796	curso.seguridadvial.gob.ar	313
918	www.santafe.gob.ar	261
1016	tarjetasube.sube.gob.ar	232
1294	rentasneuquenweb.gob.ar	176
1316	inscripciones.buenosaires.gob.ar	172
1326	gobiernodigital.chaco.gob.ar	170
1463	cas.gde.gob.ar	151
1472	infraccionesba.gba.gob.ar	150
1599	resolucion482020cuhc.descargas.gob.ar	137
1682	becasmanuelbelgrano.educacion.gob.ar	130
1865	licenciasmedicas.abc.gob.ar	115

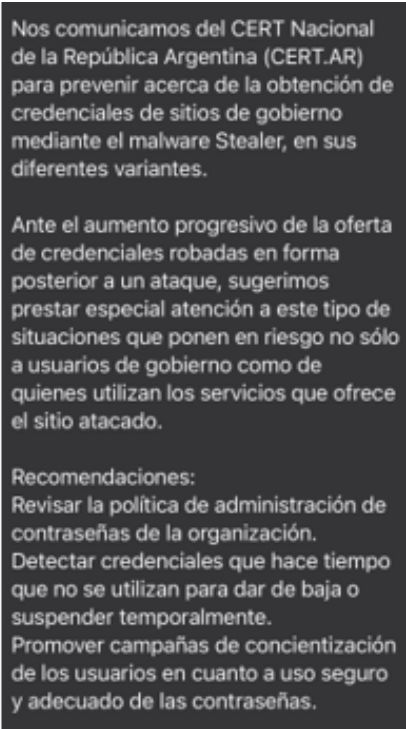
Por otra parte, responsables del Ransomware Everest publicaron a fines del 2021 en un sitio de la Dark Web, que ofrecían para la venta accesos a sistemas gubernamentales de Argentina^{59 60}.

⁵⁸ <https://tn.com.ar/tecno/novedades/2022/01/03/alerta-por-redline-stealer-un-malware-que-ataca-a-gestores-de-contrasenas/>

⁵⁹ <https://www.diariopopular.com.ar/tecnologia/hackeo-al-senado-publican-datos-robados-la-dark-web-n623176>

⁶⁰ <https://www.welivesecurity.com/la-es/2021/11/23/ransomware-everest-asegura-tener-accesos-a-sistemas-gubernamentales-argentina/>

La disponibilidad de credenciales no se limita a los periodos de tiempo mencionados. Es tal el flujo continuo de credenciales robadas que el 03/03/2022 publican el comunicado oficial del CERT Nacional de Argentina (CERT.ar⁶¹):



Nos comunicamos del CERT Nacional de la República Argentina (CERT.AR) para prevenir acerca de la obtención de credenciales de sitios de gobierno mediante el malware Stealer, en sus diferentes variantes.

Ante el aumento progresivo de la oferta de credenciales robadas en forma posterior a un ataque, sugerimos prestar especial atención a este tipo de situaciones que ponen en riesgo no sólo a usuarios de gobierno como de quienes utilizan los servicios que ofrece el sitio atacado.

Recomendaciones:
Revisar la política de administración de contraseñas de la organización.
Detectar credenciales que hace tiempo que no se utilizan para dar de baja o suspender temporalmente.
Promover campañas de concientización de los usuarios en cuanto a uso seguro y adecuado de las contraseñas.

Sobre la cuestión b), con solo tener en cuenta la muestra de **60.000 registros** que difundió, vemos que el actor de amenazas logró tener acceso a información personal y confidencial, demostrando la vulnerabilidad del sistema.

Ciertamente, otros actores de amenazas pueden causar estragos con esta información. A raíz de la difusión de la base de datos de identificación del gobierno, los ciudadanos argentinos aún hoy correrían el riesgo de sufrir sofisticados intentos de phishing, fraude financiero y estafas de suplantación de identidad.

Por ejemplo, la *“Identificación con **documento de identidad**, vigencia del mismo y **biometría facial**”* es muy utilizada por empresas financieras y, aunque se tome el recaudo de pedir al usuario que efectúe una cantidad de gestos de forma aleatoria, aun así podría ser burlada mediante Deepfake.^{62 63}

Con respecto a la cuestión c), de si es posible falsificar el DNI. Recordemos que hay dos versiones: digital y físico.

Un año antes, durante el evento de ciberseguridad Eko Party, un investigador demostró una seria falla de seguridad en la versión digital del DNI que se encuentra dentro de la app oficial **Mi**

⁶¹ <https://www.argentina.gob.ar/jefatura/innovacion-publica/ssetic/direccion-nacional-ciberseguridad/cert-ar>

⁶² <https://deepfakesweb.com/>

⁶³ <https://beebom.com/best-deepfake-apps-websites/>

Argentina⁶⁴ que permitía mostrar datos de otras personas y generar el DNI (digital) de cualquier persona.

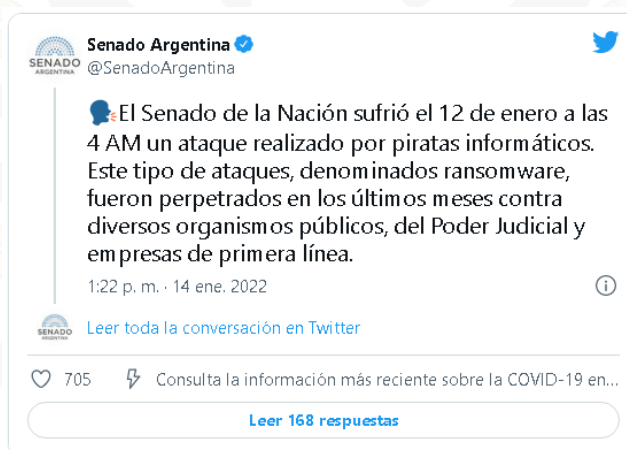
Esta falla se la conoce como Referencia de Objeto Directo Inseguro (Insecure direct object references – IDOR). Esta vulnerabilidad ocurre cuando una aplicación le permite a un usuario acceder directamente a objetos (como recursos, funciones o archivos) en función de la consulta que éste realice, sin realizar el debido control de acceso.

Es una vulnerabilidad muy común en los sitios o aplicaciones web ya que tiene que ver con errores de implementación de control de acceso. Catalogada como CWE-639, esta vulnerabilidad pertenece al OWASP TOP 10 – 2017

3.4. Ataque informático al Senado de la Nación - enero 2022

Descripción

En horas de la madrugada del 12 de enero de 2022, desde el usuario de Twitter de “Senado Argentina”, se informó el acontecimiento de un incidente de piratas informáticos de los denominados Ransomware.



En otros titulares se difundió concomitantemente información indicando “*Hackearon el Senado: piden rescate en Bitcoins para devolver datos de los que no hay << ni un backup>>*”⁶⁵. Posteriormente fue confirmado por las autoridades.

Esta clase de vulnerabilidades en las Instituciones continuó afectando directamente la seguridad, confidencialidad y tratamiento de datos resguardados por parte de los órganos de supervisión, dotados de recursos, organización administrativa y monitoreo.

El problema no se redujo a un solo episodio, sino que el ataque aparejó problemas con la conexión a internet y los teléfonos, indicando desde el soporte técnico del Congreso que habían pedido no encender las computadoras hasta que concluya el proceso de “verificación”. En ese

⁶⁴ <https://www.cronista.com/infotechnology/online/Este-cordobes-explico-como-duplicar-un-DNI-para-hacer-compras-y-sacar-prestamos-que-paso-y-como-cuidarse-20201001-0005.html>

⁶⁵ <https://www.iproup.com/innovacion/28934-hackean-senado-argentino-piden-bitcoins-para-devolver-datos>

punto, 600 de las 2000 computadoras que tenía el Senado habían atravesado ese proceso, permitiendo que se puedan llevar adelante aspectos esenciales como presentar proyectos de ley y pagar sueldos⁶⁶.

Fuentes parlamentarias⁶⁷ confirmaron que habrían alcanzado a datos personales sensibles de cada uno de los funcionarios, incluyendo datos biométricos, del domicilio, sueldos, familiares a cargo declarados, etc. que no se encuentran incluidos en el área de transparencia ni son de acceso público.

El incidente fue un Ransomware similar a lo explicado para Netwalker que, ante la negativa del pago del rescate, terminó en la publicación de la información sustraída por parte del grupo Vice Society en un sitio de la Dark Web, que luego se reprodujo en las redes sociales a partir del 12 de marzo.⁶⁸

De la información publicada, **más de 30.000⁶⁹ archivos**, surgió la filtración de números de DNI, CUIL y trámite, además de fotocopias del DNI de frente y dorso, domicilio, firmas a mano alzada, licencias de conducir y huellas digitales⁷⁰ entre otros datos que pueden ser utilizados para realizar ataques de ingeniería social o incluso robo de identidad.⁷¹



12/03/2022 Fuente: Darktracer⁷²

⁶⁶ <https://www.lapoliticaonline.com/congreso/despues-del-hackeo-en-el-senado-de-la-nacion-no-hay-conexion-a-internet-ni-funcionan-los-telefonos/>

⁶⁷ <https://www.perfil.com/noticias/actualidad/ciberataque-senado-extrajeron-datos-personales-funcionarios-siguen-sin-sistema.phtml>

⁶⁸ <https://www.diariopopular.com.ar/tecnologia/hackeo-al-senado-publican-datos-robados-la-dark-web-n623176>

⁶⁹ <https://www.noticiasdebariloche.com.ar/exclusivo-una-entrevista-con-vice-society-la-banda-de-ciberdelincuentes-que-hackeo-al-senado-de-la-nacion/>

⁷⁰ <https://www.cronista.com/infotechnology/actualidad/hackeo-al-senado-se-filtraron-dni-domicilios-y-hasta-huellas-dactilares/>

⁷¹ <https://www.diariopopular.com.ar/tecnologia/hackeo-al-senado-publican-datos-robados-la-dark-web-n623176>

⁷² https://twitter.com/darktracer_int/status/1502796882027765769/photo/1

Vice Society y consecuencias

El grupo “Vice Society” surgió a mediados de 2021, enfocándose en ataques de doble extorsión, dirigidos principalmente a víctimas pequeñas o medianas. También se ha centrado en los distritos escolares públicos y otras instituciones educativas⁷³. Conforme observaciones de respuesta a incidentes, Vice Society aprovechaba rápidamente las nuevas vulnerabilidades para el movimiento lateral y la persistencia en la red de una víctima. Incluso muestran empeño en innovar al momento de esquivar los endpoint.

El Ransomware Vice Society (probablemente un spin-off de HelloKitty) encripta los sistemas Windows y Linux usando OpenSSL (AES256 + secp256k1 + ECDSA)⁷⁴, como descubrió el experto en Ransomware Michael Gillespie⁷⁵ cuando aparecieron las primeras muestras

Asimismo, Vice Society opera un sitio de fuga de información que utiliza para publicar datos extraídos de víctimas que eligen no pagar sus demandas de extorsión.

Este malware se propaga a través de fuentes de descarga dudosas, como ser, redes de intercambio punto a punto, sitios de alojamiento de archivos gratuitos y no oficiales, etc. aprovechando la utilización por parte de los usuarios de herramientas de activación ilegal ("craqueo") y actualizaciones falsas. Los "cracks" pueden causar infecciones en lugar de activar productos con licencia. Los actualizadores fraudulentos infectan los sistemas abusando de fallas de software obsoletas e instalando programas maliciosos.

Metodología de ataque

De acuerdo al informe de Talos Intelligence (CISCO)⁷⁶, en un caso de estudio, se han observado varias TTPs utilizados en cada etapa del ciclo de vida del ataque. Algunas de las características más interesantes fueron:

- El uso de utilidades como proxychains⁷⁷ e impacket⁷⁸ durante las fases posteriores al compromiso del ciclo de vida del ataque.
- El ataque a copias de seguridad para evitar la recuperación después de la implementación del Ransomware.
- La degradación de los servidores ESX⁷⁹ utilizados para la virtualización en entornos víctimas.

⁷³ <https://www.bleepingcomputer.com/news/security/vice-society-ransomware-joins-ongoing-printnightmare-attacks/>

⁷⁴ <https://www.bleepingcomputer.com/news/security/vice-society-ransomware-joins-ongoing-printnightmare-attacks/>

⁷⁵ <https://twitter.com/demonslay335/status/1403109032014061568>

⁷⁶ <https://blog.talosintelligence.com/2021/08/vice-society-ransomware-printnightmare.html>

⁷⁷ Una herramienta que actúa como un servidor proxy soportando protocolos como HTTP, HTTPS, SOCKS4 y SOCKS5, el cual funciona en sistemas operativos basados en Linux, en BSD y también en macOS. Esta herramienta permite que cualquier conexión TCP realizada por un programa local salga a Internet a través de una serie de proxies configurados hasta su destino. De esta forma, nuestro tráfico podría pasar por uno o varios proxies para anonimizar nuestra identidad en Internet, ocultando la dirección IP pública que nos proporciona nuestro operador, y saliendo a Internet con la IP pública del último proxy al que nos hayamos conectado.

⁷⁸ Es una herramienta común de manipulación de protocolos de red para enumerar el entorno y obtener información adicional. Esto generalmente se hace para identificar objetivos de alto valor que pueden ser atractivos, ya que los ataques intentan maximizar su esfera de influencia sobre la mayor parte del entorno posible antes de, eventualmente, implementar un ransomware y dar a conocer su presencia.

⁷⁹ <https://blog.segu-info.com.ar/2021/04/ransomware-apunta-vulnerabilidades-de.html>

- El uso de una DLL que aprovecha la vulnerabilidad PrintNightmare para la cual Microsoft había lanzado previamente una actualización de seguridad.
- Intentos de eludir las protecciones nativas de Windows para el robo de credenciales y la escalada de privilegios.

A continuación, se indican algunos ejemplos clave de los TTPs utilizados en relación con el marco Mitre ATT&CK.

- Uso de Impacket para ejecutar Windows Management Instrumentation (WMI), para lograr la ejecución de comandos en otros sistemas presentes en el entorno, y la utilidad "proxchains", que se emplea para redirigir el tráfico de la red durante las pruebas de penetración, red teams y otras operaciones ofensivas.
- Uso de un servicio de Windows para ejecutar PowerShell y para mantenerse persistente en el entorno.

Las instrucciones de PowerShell estaban codificadas en Base64 y apuntaban a realizar las siguientes tareas:

- Deshabilitar el registro de PowerShell.
- Omitir la protección AMSI para PowerShell.
- Descargar, descifrar y ejecutar una carga útil de puerta trasera (backdoor) desde un servidor controlado por un atacante.

Al implementar esta persistencia, el atacante puede recuperar el acceso al entorno si la organización atacada destruye su medio de acceso inicial

Una vez operativos dentro del entorno de destino, los actores de amenazas generalmente realizan un reconocimiento, identifican sistemas de destino adicionales, se mueven de un sistema a otro mientras intentan elevar privilegios y luego, en última instancia, implementan un Ransomware en los sistemas que pueden. Normalmente se aprovechan las conexiones de escritorio remoto de Windows para pasar a sistemas adicionales en el entorno.

Cabe mencionar que un actor de amenazas intentará extraer las credenciales de la víctima de dos maneras: accediendo al archivo de catálogo global del directorio activo ntds.dit o utilizando comsvcs.dll.

Comsvcs.dll es un método conocido para extraer datos LSASS (Servicio de subsistema de autoridad de seguridad local). Al invocar comsvcs.dll con rundll32.exe, un actor de amenazas puede crear un volcado de cualquier proceso. Esta es una táctica de Living-of-the-land (LoLBin)⁸⁰ clásica e inteligente que esquivando el uso de herramientas populares de extracción de credenciales como Mimikatz, que pueden alertar al equipo de IT. También puede intentar volcar NTDS.dit, que es una base de datos de información de Active Directory.

Se suele utilizar también PrintNightmare, una serie de vulnerabilidades que permitiría la ejecución remota de código cuando una cola de impresión incorrecta realiza operaciones de archivo privilegiadas. Este vector de ataque es notable en la naturaleza omnipresente de los servicios de impresión en todas las empresas corporativas modernas.

Finalmente, un actor de amenazas típicamente intenta filtrar la información a través de **SMB (TCP/445)** directamente desde un controlador de dominio comprometido.

Conclusiones

Atento al análisis efectuado, surge como consecuencia que el vector de ataque más probable sería un software de craqueo (descargado por algún usuario con permisos suficiente para la ejecución del malware dentro de la red).

Sin perjuicio de ello, en una entrevista con noticiasbariloche,⁸¹ un sujeto se presentó como representante de Vice Society y afirmó que:

- Entraron en la red del Senado a través de “phishing”;
- Que fue fácil. Les tomó seis horas para acceder a todos los sistemas informáticos y seis horas para atacar;
- Que copiaron la información en aproximadamente 5 horas; y,
- Que el Ransomware lo compraron en la Dark Web

De ser cierto, tomando una tasa de 13,5Mbits/s, por similitud con lo acontecido con la red de Migraciones, en cinco horas los actores de amenazas habrían descargado alrededor de 30 GB de información.

3.5. Ataque informático al Poder Judicial de Chaco - febrero 2022

Descripción

El 11 de enero de 2022, el Superior Tribunal de Justicia de Chaco informó que los servicios digitales del Poder Judicial quedaban suspendidos a causa de “*un ataque de un malware del tipo Ransomware que han sufrido algunos servidores del Poder Judicial de la Provincia del Chaco*”⁸²

El ataque afectó la plataforma de gestión de expedientes y otros sistemas de todo el Poder Judicial chaqueño y llevó al Superior Tribunal de la provincia a declarar la suspensión de términos y audiencias, al menos hasta el lunes 17. Tras obtener las conclusiones de informes privados, el Superior Tribunal de Justicia dictó un protocolo de contingencia y lineamientos de trabajo para el restablecimiento gradual y progresivo de los servicios y sistemas a partir del 1 de febrero de 2022.

El Superior Tribunal admitió que el ataque provocó la pérdida de información, comunicándose con la Dirección Nacional de Ciberseguridad, que depende de la Jefatura de Gabinete y radicaron una denuncia penal que investiga una Fiscalía chaqueña.

El ataque ocurrió entre el viernes 7 y el sábado 8 de enero⁸³, cuando las autoridades del Poder Judicial detectaron una serie de errores en la página. A consecuencia de ello, se perdieron algunos servicios y se resolvió desconectar todo. Dada la imposibilidad en determinar la magnitud de las consecuencias del ataque, se dispuso la suspensión de todos los servicios de

⁸¹ <https://www.noticiasdebariloche.com.ar/exclusivo-una-entrevista-con-vice-society-la-banda-de-ciberdelincuentes-que-hackeo-al-senado-de-la-nacion/>

⁸² <https://www.iproup.com/innovacion/28934-hackean-senado-argentino-piden-bitcoins-para-devolver-datos>

⁸³ <https://www.lanacion.com.ar/politica/hackearon-al-poder-judicial-de-chaco-y-piden-un-rescate-por-la-informacion-nid08022022/?R=8c0b31>

índole digital⁸⁴. Se dieron cuenta entonces que el incidente se produjo a raíz de un Ransomware, “Hive Ransomware”, dado que apareció un mensaje diciendo cómo recuperar los archivos, las indicaciones para acceder a la Dark Web, el pedido de rescate, el monto exigido y la forma de concretar el pago

Desde la Superintendencia del Superior Tribunal de Justicia, expresaron que “*un Ransomware se concentró primero en barrer con todos los cortafuegos y antivirus, para luego acceder a la información almacenada y encriptarla*”⁸⁵, sostuvieron que “*los había salvado el servicio de backup*” y que recuperarían “*el 100 por ciento*” de la información de casi todos los fueros (entre ellos, el Penal y el de Familia), aunque restaba determinar cuánto podrían recuperar de dos bases de datos del sistema de gestión de expedientes civiles y comerciales. Transcurrido un mes, todavía se encontraban en proceso de recuperación.

Hive y consecuencias

Al igual que Netwalker RaaS el grupo HIVE RaaS está altamente organizado. Sin embargo, a diferencia del primero, este último centra fuertemente su estrategia en explotar las múltiples vulnerabilidades de seguridad de Microsoft Exchange.⁸⁶

Hive aprovecha una variedad de métodos de compromiso inicial, incluidos servidores RDP vulnerables, credenciales de VPN comprometidas, así como correos electrónicos de phishing con archivos adjuntos maliciosos. Es decir, usa múltiples tácticas, técnicas y procedimientos (TTPs) para comprometer redes específicas.

Se sabe que el grupo explota varias trampas de phishing con archivos maliciosos adjuntos para acceder a sistemas críticos y usar el Protocolo de Escritorio Remoto (RDP) para moverse horizontalmente por la red. Mientras realiza acciones en vivo, el operador de Hive desactiva los servicios de antivirus, antispyware y restauración de la computadora, entre otros. Extrae datos confidenciales y cifra los archivos comerciales guardándolos con una extensión “.hive”. Luego crea los archivos por lotes hive.bat y shadow.bat, que contienen comandos para que la computadora elimine el ejecutable de Hive, las copias de seguridad del disco o las instantáneas y los archivos por lotes. Esta es una técnica común utilizada por el malware para reducir la evidencia forense disponible

Finalmente, Hive deja una nota de rescate, HOW_TO_DECRYPT.txt, en cada directorio afectado. El aviso explica que los archivos cifrados no se pueden descifrar sin la clave maestra, que está en posesión de los actores. Además, la nota contiene los detalles de inicio de sesión del sitio web TOR que la víctima puede usar para pagar el rescate y amenaza con filtrar la información de la víctima en el sitio HiveLeaks.⁸⁷

Estos ataques son particularmente preocupantes, ya que los servidores de intercambio sin parches se pueden descubrir públicamente a través de rastreadores web (web crawlers).

⁸⁴ <https://www.infobae.com/politica/2022/02/09/un-grupo-de-hackers-que-preocupa-al-fbi-estaria-detras-del-hackeo-al-sistema-judicial-de-chaco/>

⁸⁵ <https://www.pressreader.com/argentina/la-nacion/20220209/281496459697356>

⁸⁶ <https://jackofalltechs.com/2022/04/25/experts-warn-that-hive-ransomware-gang-can-detect-unpatched-servers-with-a-web-crawler/>

⁸⁷ <https://socradar.io/dark-web-profile-hive-ransomware-group/>

También cabe aclarar que estas vulnerabilidades no afectan a los servidores de Exchange en la nube ni Office 365.

Para tener una mejor idea: El equipo forense de Varonis⁸⁸ investigó un incidente de Ransomware Hive donde se observó que el actor logró sus objetivos maliciosos y encriptar el entorno en menos de 72 horas desde el compromiso inicial

Por otra parte, Microsoft⁸⁹ publicó el **13 de julio de 2020** una actualización para corregir esta vulnerabilidad. Por lo que al menos desde esa fecha la **vulnerabilidad dejaba oficialmente de ser un Zero Day**.⁹⁰

Los aparentes retrasos en parchear estas vulnerabilidades convierten, a las organizaciones que utilizan Microsoft Exchange para funciones comerciales críticas, en un objetivo ideal para los actores de amenazas, porque permiten a los atacantes reducir la cantidad de reconocimiento y los pasos inmediatos que deben tomar para infiltrarse en los sistemas de destino.

Corolario de lo expuesto, sin acceso a la evidencia ni a mayor información oficial, se concluye que:

- El ataque de Hive RaaS a la plataforma de gestión de expedientes y otros sistemas de todo el Poder Judicial chaqueño no podría haberse realizado con éxito si los servidores Exchange hubieran sido correctamente parcheados o si se hubiera utilizado otro software en su lugar; y,
- Dada la incertidumbre del órgano afectado sobre el alcance de los daños, el tiempo demorado en los procesos de recuperación de información y la indisponibilidad de sistemas durante semanas⁹¹, cabe la hipótesis de que el ataque alcanzo a todas las bases de datos y documentos críticos. Lo cual es consistente con el modus operandi de HIVE.

En estos términos, observamos la imperiosa necesidad de adoptar diferentes niveles de salvaguarda de esta clase de datos sensibles, que debe darse a través de equipos tecnológicos que den inmediata respuesta a incidentes informáticos. La sola existencia de una ley (con más de 20 años) que enmarque el concepto y alcance de la protección no comporta una política clara de atención del problema concreto que, hoy en Argentina, se encuentra en crecimiento.

3.6. Censo Nacional de Población, Hogares y Viviendas - mayo 2022

Descripción

Previo a la fecha de realización del Censo 2022 en Argentina, se observaron ciertas falencias que devinieron en críticas, expresadas por usuarios de redes sociales.

⁸⁸ <https://www.varonis.com/blog/hive-ransomware-analysis>

⁸⁹ <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34473>

⁹⁰ Un Zero day es una vulnerabilidad de software de computadora desconocida para aquellos que deberían estar interesados en su mitigación o conocida y sin un parche para corregirla.

⁹¹ <https://www.lanacion.com.ar/politica/hackearon-al-poder-judicial-de-chaco-y-piden-un-rescate-por-la-informacion-nid08022022/>

Ahora bien, ante este tipo de eventos la información que se recaba debe ser pertinente y no exceder del fin legítimo que busca el Censo conforme Ley 17.622 y Decreto 3110/70. En caso de requerir mayor información que la necesaria para el fin (Censo de ciudadanos), su tratamiento y la conservación de los datos debe ser limitada.

En un marco ideal, las personas censadas deberían poder tener acceso a sus Datos resguardados en el resultado final de dicho Censo, a efectos de tener la posibilidad de petitionar al Responsable para corregir, revisar o eliminar los Datos que se reflejen, todo ello de acuerdo a lo garantizado por el artículo 43 de la Constitución Nacional.

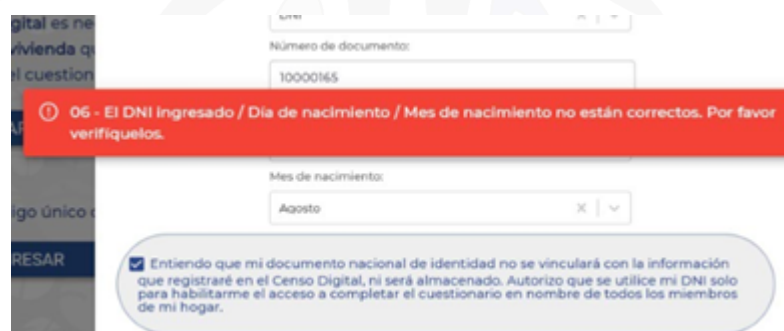
Análisis de falencias/críticas

Ubicación de los servidores, hacia donde van los datos

La ubicación de los mismos, que se desprende del siguiente cuadro, se realizó utilizando herramientas gratuitas disponibles en internet, como Website Reputation Checker⁹², revisamos el sitio <https://www.censo.gob.ar/>

Website Address	Censo.gob.ar	Censo.gob.ar
Last Analysis	23/02/2022	23/03/2022
Domain Registration	2021-05-06	2021-05-06
IP Address	186.33.219.235	18.214.59.219
Reverse DNS	235.219.33.186.in-addr.arpa	ec2-18-214-59-219.compute-1.amazonaws.com
ASN	AS52361 Empresa Argentina de Soluciones Satelitales S.A.	AS14618 AMAZON-AES
Server Location	(AR) Argentina	(US) United States
Latitude\Longitude	-34.6022 / -58.3845 Google Map	39.0469 / -77.4903 Google Map
City	Buenos Aires	Ashburn
Region	Buenos Aires F.D.	Virginia

Consultas a RENAPER



De la imagen entendemos que la validación se realiza contra las bases de datos del RENAPER, dado que este organismo es el responsable del SID

⁹² <https://www.urlvoid.com/scan/censo.gob.ar/>

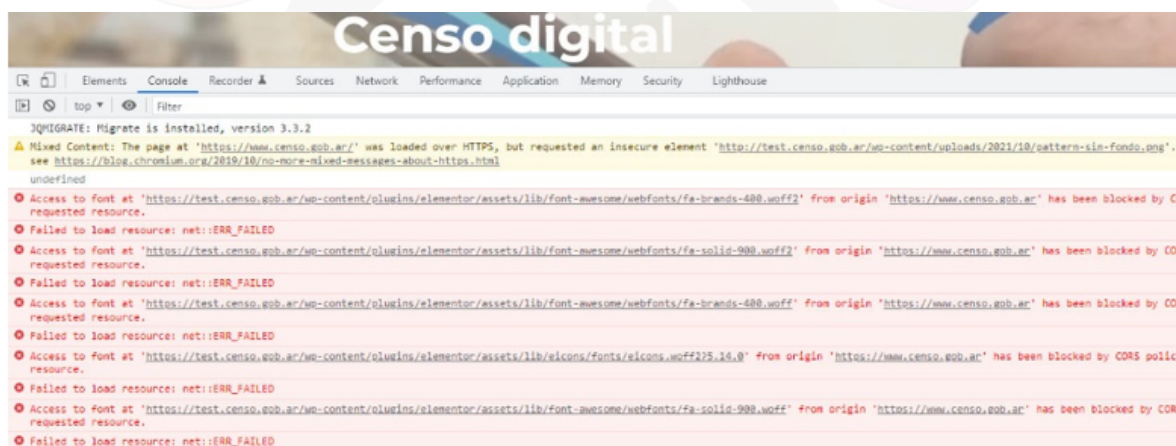
Por otra parte, con alguna antelación, diferentes usuarios de redes sociales (mayormente Twitter, [#Censo2022](#) o [@Censo2022](#)), incluyendo especialistas en ciberseguridad, criticaron especialmente vulnerabilidades de la plataforma que potencialmente ponían en peligro la confidencialidad de los datos cargados en el sistema. Algunas de esas cuestiones fueron solucionándose previo a la realización del Censo (desacreditándolas oficialmente), vale la pena comentar algunas⁹³ a modo de ejemplo.

Las “primeras” críticas

Los usuarios comenzaron a demostrar falencias básicas en cuanto a código y desarrollo⁹⁴. Las imágenes muestran que, al 16 de marzo, el sitio que había sido lanzado a producción todavía buscaba recursos desde test.censo.gob.ar (sitio de pruebas, que por cuestiones de ciberseguridad este tipo de sitios nunca deben ser visibles desde internet) y que algunas funciones que claramente debían conectarse al servidor apuntaban a localhost (al dispositivo del usuario) y ejecutaban llamadas a APIs sin contar con la autorización.

Entre las distintas críticas analizadas, el Dr. Rodrigo Iglesias, abogado y miembro del Observatorio de Derecho Informático Argentino, señaló: *“Los censos son anónimos y tratan datos sensibles, el ciudadano tiene la obligación de decir la verdad, pero a su vez la ley de protección de datos personales explicita que los datos deben ser tratados de una manera responsable e idónea”. “Hay distintas falencias en torno a la regulación, en el censo digital utilizan el DNI como factor de validación. Con el DNI y la fecha de nacimiento que te solicita la página, se genera un código de verificación que está sujeto a 5 dígitos que permiten 60 millones de combinaciones posibles para una base mayor de 45 millones de habitantes”*.⁹⁵

Estos descuidos, por decirlo, y la falta de aplicación o atención sobre los ciclos de desarrollo de software (incluidas principalmente las consideraciones sobre seguridad informática) son las primeras cosas que buscan los actores de amenazas cuando analizan un objetivo.



⁹³ <https://www.iproup.com/innovacion/31510-censo-digital-2022-denuncian-graves-fallas-de-seguridad>

⁹⁴ <https://twitter.com/fabiomb/status/1504183498424397832?lang=en>

⁹⁵ <https://www.mdzol.com/sociedad/2022/3/29/el-riesgo-en-la-filtracion-de-datos-que-atenta-contr-el-censo-digital-230984.html>

Incluso el mismo navegador reconoce que debieron usar el protocolo https en vez de http

```
insecure element "http://test.censo.gob.ar/wp-content/uploads/2021/10/pattern-sin-fondo.png".
```

Tracker (rastreador) en el email de confirmación



1:16 PM · Mar 16, 2022 · Twitter Web App

De las imágenes, publicadas en twitter⁹⁶, surgen de los primeros emails de confirmación. El tracker apunta a mdrctr.com, que según <https://domainwat.ch/> y <https://urlscan.io/> se corresponde con la siguiente información:

IP Address	62.97.140.11
Reverse DNS	www.antevenio.com
Location	 Spain
Hosting Company	Prosodie Iberica SI

Se trataría de una organización dedicada a “Email, móvil y social media marketing” cuyos servicios incluyen:

- Campañas de envío masivo de emails: “crea una cuenta gratuita y realiza hasta 5000 envíos al mes de hasta 5000 contactos”
- Gestión de contactos: “Categorizamos tus usuarios en función de su respuesta a las campañas para ayudarte en la toma de decisiones y para que puedas definir la presión de marketing que creas mejor para cuidar a tus usuarios”

⁹⁶ <https://twitter.com/mis2centavos/status/1504159562617741313>

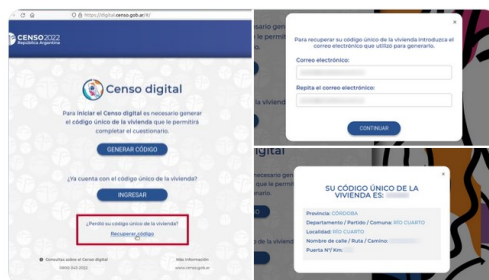
- Informes y análisis: “Potente herramienta de reporting. Heat Map de las campañas. Posibilidad de consultar las métricas filtradas por los campos de la base de datos.”

Recuperar el código de vivienda e información sobre el propietario de email

El riesgo sobre la información privada surge en la forma en que el sitio del INDEC recuperaba el denominado código de vivienda. Al introducir el mail (de alguien que haya completado el censo digital) para obtener el código, este no se enviaba a dicho email, sino que se mostraba directamente en el sitio junto con los datos del domicilio. Es decir, cualquier persona que supiera el mail de otra podía conocer con facilidad sus datos personales.⁹⁷

- 1) Clic en "recuperar código".
- 2) Ingresar el email de una persona que haya hecho el "censo digital".
- 3) El sistema, en vez de reenviar el código a la dirección de email, lo muestra... incluyendo el domicilio de la persona.

¿Nada van a hacer bien, @MarcoLavagna?
#Censo2022



SU CÓDIGO ÚNICO DE LA VIVIENDA ES: SE

SU COMPROBANTE ES: SE

Provincia: MISIONES
Departamento / Partido / Comuna: CAPITAL
Localidad: POSADAS
Nombre de calle / Ruta / Camino: PEDRO CORREA
Puerta N°/ Km:

SU CÓDIGO ÚNICO DE LA VIVIENDA ES: 7Z

SU COMPROBANTE ES: 7Z

Provincia: SANTA FE
Departamento / Partido / Comuna: VERA
Localidad: GARABATO
Nombre de calle / Ruta / Camino: 25 DE MAYO
Puerta N°/ Km:

Para los que piensan "igual mis datos están en todos lados, los tiene Google", etc.

Esto nos decía @SeguInfo el 16 de marzo cuando le consultamos cuál era el problema de que el censo vinculara el DNI a los datos personales.

Migraciones, Renaper, ahora el Censo. Es grave 🙄

“Para los ciudadanos implica un problema grave porque significa que cualquiera podría acceder a los datos y, con los mismos, **un delincuente puede dirigir y perfeccionar cualquier tipo de robo, fraude, estafa** o suplantación de identidad. Supuestamente estos datos serán protegidos pero el Estado ya ha demostrado que no es capaz de hacerlo y, suponiendo que lo hagan, ¿por qué se debería confiar en los proveedores y en quienes acceden (con permiso) a los datos?”, se pregunta el especialista.

⁹⁷ <https://elintransigente.com/2022/05/censo-2022-senalan-al-indec-por-una-grave-falla-de-seguridad-en-el-censo-digital/>

Funcionamiento anormal del servicio

Durante el fin de semana previo a la realización del censo en la página web del mismo, los usuarios denunciaban, a través de las redes sociales, que la página no operaba con normalidad o directamente no podían entrar. A raíz de esas denuncias se abordó el problema y se solucionó minutos antes de las 22 hs del domingo 15 de mayo.⁹⁸

Este evento coincidió con la queja de una persona, que quería volver a ingresar a fin de recuperar el código para mostrarle al censista, indicando que el sitio mostraba todos sus datos personales, entre ellos, el domicilio.

La App para censistas y la inseguridad de su clave

El usuario @maxifirtman, programador, alertó⁹⁹ sobre las cuestiones de **privacidad, seguridad informática y libertades individuales** (prohibición al usuario de disponer libremente de su propiedad) relativas a la App para los censistas.

Y no me piden hilar más fino que la contraseña sea única y fácil para todos, ¿para qué necesita la app para los censistas leer y/o modificar archivos por fuera de la app, ver las conexiones Wi-Fi que hay alrededor y ejecutarse al inicio?



¿Qué pasa si me quedo sin batería?

CensAR está diseñada para tener bajo consumo de batería. Para mejorar el rendimiento de la misma, te sugerimos bajar un poco el brillo. **Está prohibido** utilizar otras aplicaciones (Facebook, TikTok, YouTube, Instagram, Twitter, etc.) que perjudiquen el desarrollo de tu tarea durante el operativo.



Y salieron 650.000 censistas con una App donde se identifican con su número y la misma contraseña para todos, super segura: censo2022 y la cual NO puede ser cambiada.

El nivel de delirio del #Censo2022: una búsqueda en Google te lleva a un sitio para censistas con un video de YouTube que te dice cual es la clave que 600 mil censistas usarán desde hoy. Y mirá la clave... ?

Espero que la difusión obligue a cambiar esta locura. 😬



⁹⁸ <https://www.elsol.com.ar/el-pais/censo-digital-se-cayo-la-pagina-y-detectaron-un-problema-de-seguridad>, <https://twitter.com/maxifirtman/status/1526546884336275457>

4. Una mirada sobre ataques cibernéticos dirigidos a otros Estados.

La vulnerabilidad de la información y sistemas que resguardan los Estados sigue creciendo en todos el mundo. Los hackeos, intrusiones o robo de información suceden de modo anónimo pero puede sospecharse, detrás de muchos casos un interés geopolítico que registra cruces de ataques y episodios dirigido de un determinado país hacia otro. Las herramientas de “guerra cibernética” incluyen virus, phishing, y otros tipos de malware, que incluso suelen ser diseñados para dañar infraestructuras críticas específicas, Ransomware para secuestrar datos, campañas de propaganda o desinformación y robo de datos privados de sitios gubernamentales, entre otros. Uno de los más renombrados es Pegasus, un spyware que se propaga aprovechando vulnerabilidades en las Apps de los celulares, utilizado para acceder a los dispositivos de autoridades, políticos, periodistas, activistas y ciudadanos.

En este contexto juega también un papel importante la regulación y la política internacional. En dicho sentido, son varios los países que impulsan cambios en relación a la seguridad informática, Por ejemplo:

- Japón abrió su Agencia Digital e incorporó, recientemente, a Ciaran Martin, fundador y ex director del Centro Nacional de Ciberseguridad de Gran Bretaña¹⁰⁰.
- Hong Kong¹⁰¹, a raíz de la nueva Ley de Seguridad Nacional de China, intentó introducir enmiendas¹⁰² en la Ordenanza sobre Privacidad de Datos Personales (PDPO) que le permitieran frenar el doxing¹⁰³. Sin perjuicio de que la mayor parte de los contenidos están fuera de Hong Kong y que el regulador carece de jurisdicción allí, la Coalición de Internet de Asia y la ONU expresaron que ello podría impactar en la libertad de expresión, el derecho a la información y la denuncia de irregularidades
- China, a su vez, aprobaría¹⁰⁴ nuevas normas de seguridad que obligaría a las empresas que cotizan en Hong Kong a someterse a una revisión de ciberseguridad, si manejan “datos relevantes a la seguridad nacional”¹⁰⁵
- Corea del Sur¹⁰⁶ se convierte en el primer país asiático en unirse al Centro de Excelencia de Ciberdefensa Cooperativa (CCDOE), el grupo de defensa cibernética de la OTAN.
- Estados Unidos creó en 2009 el United States Cyber Command (USCYBERCOM), cuenta con una estrategia nacional de ciberseguridad que revisa periódicamente y recientemente invirtió USD 1000 millones en ciberseguridad¹⁰⁷

La gran mayoría de los ataques informáticos no toma estado público debido a la naturaleza misma de la guerra y el espionaje cibernético, por lo que poco frecuente la publicidad sobre

¹⁰⁰ <https://www.intelligenceonline.com/surveillance--interception/2022/01/20/former-uk-cyber-security-chief-ciaran-martin-to-help-britain-break-into-japanese-market,109717985-art>

¹⁰¹ <https://thediplomat.com/2021/09/the-downfall-of-hong-kongs-privacy-law/>

¹⁰² https://www.legco.gov.hk/yr20-21/english/brief/cmabcr72245_20210714-e.pdf

¹⁰³ <https://cnnespanol.cnn.com/2021/07/06/doxing-hong-kong-facebook-twitter-google-trax/>

¹⁰⁴ http://www.cac.gov.cn/2021-11/14/c_1638501991577898.htm

¹⁰⁵ <https://www.reuters.com/technology/china-regulator-proposes-cyber-security-review-some-firms-planning-hong-kong-2021-11-14/>

¹⁰⁶ <https://www.dw.com/es/corea-del-sur-se-une-al-centro-de-ciber-defensa-de-la-onu/a-61689217>

¹⁰⁷ https://www.axios.com/biden-signs-infrastructure-bill-law-8c5a984c-8222-4f68-9b9c-f3a025ceb0a0.html?stream=politics&utm_source=alert&utm_medium=email&utm_campaign=alerts_politics

ellos. Sin embargo, solo en **2018**, según reportes privados, hubo más de **30 millones** de ataques informáticos en general (80.000 ciberataques por día)¹⁰⁸

De acuerdo con [privacyaffairs.com](https://www.privacyaffairs.com)¹⁰⁹, desde 2009, entre aquellos ataques informáticos que han sido informados sólo alrededor de 500 se clasifican como ataques informáticos geopolíticos. A su vez, entre 2009 y 2018 hubo un aumento del 440% en los ataques de “guerra cibernética” a nivel mundial y el aumento más significativo en la cantidad de ataques ocurrió en los últimos cuatro años.

En 2021, el Instituto Internacional de Estudios Estratégicos (IISS)¹¹⁰, luego de analizar las capacidades de ciberdelincuencia, defensa e inteligencia de 15 países, colocó a los Estados Unidos como la superpotencia cibernética más importante del mundo.

La metodología empleada¹¹¹ para el análisis arroja que Estados Unidos fue la única nación que se clasificó en un nivel por encima del resto. El segundo nivel lo ocupan Australia, Canadá, China, Francia, Israel, Rusia y el Reino Unido. A su vez, el tercer nivel incluye a India, Indonesia, Irán, Japón, Malasia, Corea del Norte y Vietnam.

A su vez, China ve a EE.UU. como el *líder* de los ataques cibernéticos¹¹². No obstante, desde 2009 ha habido 79 ataques confirmados y documentados llevados a cabo por atacantes supuestamente patrocinados por el Estado chino, dirigidos a 20 países contra gobiernos nacionales. El 32% de los ataques de China se dirigieron a EE. UU., lo que convierte a EE. UU. en el principal objetivo de los delincuentes cibernéticos chinos. Hong Kong también es un objetivo frecuente de esos mismos atacantes.

Fueron reportados ataques a 19 países en 75 incidentes entre 2009 y 2019. El objetivo sería EE. UU., pero también atacaron a 8 países de la Unión Europea, incluida una serie de ataques contra el parlamento alemán¹¹³. Ucrania también fue objetivo frecuente de Rusia, de acuerdo al Microsoft Digital Defense Report 2021¹¹⁴ fue uno de los tres países más afectados. Entre julio de 2020 y junio de 2021, Rusia, según consigna esta fuente, ha sido la fuente de la mayoría de los ciberataques patrocinados por algún Estado¹¹⁵. Más del 50 % de los ataques cibernéticos entre ese período se originaron en Rusia, mientras que Corea del Norte estuvo detrás del 23 % de ellos

Corea del Norte, entre 2009 y 2019 llevó a cabo 32 ataques contra 9 países, más de la mitad entre 2017 y 2018. Doce de esos ataques fueron contra Corea del Sur, incluido el incidente de diciembre de 2018 del centro de refugiados de Hana¹¹⁶, en el que se accedió a los datos personales de más de 1000 desertores norcoreanos.

¹⁰⁸ <https://purplesec.us/resources/cyber-security-statistics/>

¹⁰⁹ <https://www.privacyaffairs.com/geopolitical-attacks/>

¹¹⁰ <https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power>

¹¹¹ <https://www.c4isrnet.com/cyber/2021/06/28/who-can-match-the-us-as-a-cyber-superpower-no-one/>

¹¹² <https://www.bloomberg.com/news/articles/2021-03-18/u-s-china-meeting-will-underscore-biden-s-continuity-with-trump>

¹¹³ <https://www.bbc.com/news/technology-36284447>

¹¹⁴ <http://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFli>

¹¹⁵ <https://www.deccanherald.com/international/world-news-politics/cyberwarfare-and-countries-involved-ukraine-among-3-most-affected-by-russian-cyber-activity-1085308.html>

¹¹⁶ <https://portswigger.net/daily-swig/hack-exposes-identities-of-1-000-north-korean-defectors>

Desde Irán se habrían atacado a 7 países en 31 ataques, con el 42% de sus ataques dirigidos a los EE. UU., Israel varias veces (incluido aquel episodio de marzo de 2019)¹¹⁷, el ataque contra miembros del parlamento británico (junio de 2017)¹¹⁸ y el ataque a los servicios de telecomunicaciones¹¹⁹ en Irak, Pakistán y Tayikistán (junio de 2019).

Se ha reportado que Estados Unidos habría sido fuente de al menos 12 ataques cibernéticos en los últimos diez años, la mitad de los cuales ocurrieron en 2019. Tres de los ataques conocidos se habrían dirigido a Corea del Norte y, a su vez, China e Irán habrían sido atacados dos veces cada uno.

Por otra parte, cabe mencionar las actividades realizadas bajo el avatar de Anonymous, que opera de modo transnacional en una estructura de comando flexible y descentralizada, bajo consignas que se oponen a la censura, el control de Internet y la cibervigilancia.

Con un pico de actividad en 2011-2012 y una marcada actividad en 2022, que incluye una declaración de guerra cibernética a Rusia^{120 121 122}, se les atribuye al menos 124 eventos, dirigidos contra organizaciones públicas y privadas, desde sus inicios.

Finalmente, las tensiones que surgen en el contexto internacional¹²³, agravadas ahora por la invasión de Rusia a Ucrania, instalan con fuerza la discusión sobre Splinternet¹²⁴. Lo que inició como un debate entre Libertad de Expresión y seguridad, en el que a través de legislaciones los gobiernos pretendían obligar a las empresas de Internet a cumplir y a adaptarse a determinados parámetros para poder ofrecer allí sus productos y servicios, deriva ahora en una cierta posibilidad de que el ciberespacio termine fragmentado, controlado y regulado por diferentes países.

Es en este sentido, Estados Unidos y la Unión Europea recientemente han impulsado una declaración no vinculante sobre el futuro de Internet¹²⁵ que, entre sus principios incluye la Protección de los DDHH, las libertades fundamentales y la gobernanza de Internet de múltiples partes interesadas.

¹¹⁷ <https://www.reuters.com/article/us-israel-election-iran/israel-suspects-iran-of-hacking-election-frontrunner-gantz-phone-tv-idUSKCN1QV2RR>

¹¹⁸ <https://www.bbc.com/news/uk-40394074>

¹¹⁹ <https://www.cyberscoop.com/muddywater-tajikstan-clearsky/>

¹²⁰ <https://www.theguardian.com/world/2022/feb/27/anonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia>

¹²¹ <https://twitter.com/YourAnonNews/status/1496954238290653184>

¹²² <https://www.cnn.com/2022/03/25/what-is-anonymous-the-group-went-from-4chan-to-cyberattacks-on-russia.html>

¹²³ <https://techcrunch.com/2019/03/13/the-splinternet-is-already-here/>

¹²⁴ https://www.uv.mx/infosegura/general/conocimientos_splinternet/

¹²⁵ <https://www.infobae.com/america/agencias/2022/04/28/eeuu-se-suma-a-55-paises-para-promover-una-internet-libre/>

5. Conclusión

Argentina fue uno de los primeros países de América en contar con un marco regulatorio para la protección de datos personales, participando asimismo en el “Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal” del Consejo de Europa (CdE).

Entre 2016 y 2019 se dio un fuerte impulso en la Administración Pública Argentina con respecto a cambios en políticas y regulación TIC. El Decreto Nº 87/2017 que, sobre gobierno electrónico, significó la creación de una plataforma digital orientada a facilitar la interacción entre las personas y el Estado y consolidó el camino para la creación de la Agenda Digital Argentina a través del Decreto Nº 996/2018, que tiene entre sus objetivos “desarrollar capacidades en ciberseguridad para generar confianza en los entornos digitales”. Continuando con esas políticas de impulso en el año 2017, a través del Decreto 577/17 se creó el Comité de Ciberseguridad, con el objetivo de desarrollar una estrategia nacional de seguridad cibernética, que se consolidó mediante la Resolución 829/2019, que dio lugar a la Resolución 1523/2019 definiendo las “Infraestructuras Críticas e Infraestructuras Críticas de información”.

Estos avances en el marco de gobierno abierto y gobierno digital, facilitaron el apoyo del BID¹²⁶ en 2019 y convenios con Estados Unidos, España y Chile en relación a la implementación de políticas relacionadas con infraestructura crítica, seguridad de los datos personales, buenas prácticas en el uso de las TIC, y el fortalecimiento de las capacidades nacionales en ciberseguridad.

Luego a través del Decreto 338/2020, hubo un retroceso en los avances consolidados, con medidas como el denominado “procedimiento de contingencia”¹²⁷ con el fin de garantizar el soporte papel de los actos administrativos. En un contexto de Industria 4.0 y Transformación Digital que distintos países llevan adelante, la decisión reduce drásticamente la trazabilidad de la documentación, afecta la transparencia, atenta contra la integridad de la información y facilita la exposición de datos personales sensibles. Cabe destacar que conforme expresó la OCDE en el Estudio de Integridad de Argentina “La publicación activa de datos y la búsqueda de la comunicación con los ciudadanos enviaría una fuerte señal del compromiso con la integridad del sector público y facilitaría la rendición de cuentas, lo que también puede fomentar la confianza (OCDE, 2019)”¹²⁸

Por otra parte, recién en el año 2021, a raíz del ataque informático a la Dirección Nacional de Migraciones, se comenzó a avanzar en la toma de medidas en relación a ciberseguridad y protección de datos, creando un Comité Asesor para el Desarrollo e Implementación de aplicaciones seguras (Disposición 6/2021) y el Centro Nacional de Respuestas a Incidentes Informáticos -CERT.ar- (Disposición 1/2021), estableciendo mínimos requisitos de seguridad de la información para organismos públicos (Decisión Administrativa 641/2021). Sin embargo, como pudo ser advertido del presente informe, tales Decisiones Administrativas no fueron

¹²⁶ Proyecto AR-L1304 - <https://www.iadb.org/es/project/AR-L1304>

¹²⁷ <https://www.lanacion.com.ar/economia/polemica-un-decreto-vuelve-permitir-tramites-papel-nid2351043/>

¹²⁸ OCDE (2019), Estudio de la OCDE sobre Integridad en Argentina: Lograr un cambio sistémico y sostenido, Estudios de la OCDE sobre Gobernanza Pública, OECD Publishing, París, <https://dx.doi.org/10.1787/g2g98f15-es>.

suficientes para prevenir ni responder inmediatamente de forma adecuada ante los incidentes del RENAPER, del Poder Judicial de Chaco y del Senado de la Nación.

En una reciente publicación, 28 de enero 2022 (en conmemoración a la firma del Convenio 108 para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal por parte del Consejo de Europa, en el año 1981) se informó que “Access Now en conjunto con la Asociación por los Derechos Civiles, Fundación Vía Libre y el Observatorio de Derecho Informático Argentino, presentaron en el Día Internacional de la Protección de Datos Personales, una carta abierta dirigida al Poder Ejecutivo y Legislativo Nacional. En la misma solicitaron la suspensión del desarrollo e implementación de tecnologías que impliquen el procesamiento masivo de datos personales hasta tanto se brinde mayor información para esclarecer los hechos sucedidos, se implementen mejoras en materia de seguridad informática y se establezcan mecanismos democráticos para la toma de decisiones sobre la utilización de estas herramientas tecnológicas¹²⁹”.

Para junio de 2022, se proyecta realizar una capacitación en nuestro país para revisar las prácticas de ciberseguridad de las dependencias estatales, gracias a un aporte de la Organización de Estados Americanos (OEA), conforme informó Kerry-Ann Barrett, gerente del programa de ciberseguridad de la OEA, en una mesa redonda de la cumbre AWS Summit 2022. Quien explicó a su vez que “Ese reporte es para delinear las recomendaciones para llevar la ciberseguridad a un siguiente nivel”.¹³⁰

Hasta este momento, la protección en el tratamiento, manipulación y almacenamiento de los datos personales y sensibles no formó parte activa de la agenda política actual, tanto en los niveles y/o velocidad que algunos de los países vecinos le están imprimiendo. Puesto que, como indicó Gaspar Pisanu, Líder de Políticas Públicas para América Latina “Los países vecinos ya cuentan con una normativa actualizada o se encuentran debatiendo un proyecto en la materia”.¹³¹

En este contexto resulta imprescindible que, desde las organizaciones de la sociedad civil continuemos bregando por una mayor protección de los datos de las personas y la implementación de políticas que posibiliten un adecuado marco de protección que garantice su tratamiento dentro de las garantías de los Derechos Humanos

¹²⁹ <https://www.accessnow.org/proteccion-datos-personales-argentina-medidas-urgentes/>

¹³⁰ https://www.clarin.com/tecnologia/aws-summit-2022-oea-ayudara-argentina-proteger-ciberataques_0_wufokn8L14.html

¹³¹ ídem 126



FUNDACIÓN LED
Libertad de Expresión + Democracia

WWW.FUNDACIONLED.ORG

  /FUNDACIONLED

El presente informe fue elaborado por
Eduardo Tallarico, Agustín Alonso, Juan Cañada, Silvana Giudici

Argentina 2022

Publicación Buenos Aires, Argentina - Junio 2022

Tel.: +54 (011) 112-384-7731

www.fundacionled.org - fundacionled@fundacionled.org