Provincia de Santa Fe
Ministerio de Gobierno, Justicia
y Derechos Humanos
Subsecretaría de Asuntos Legislativos
Dir. Pcial. de Asuntos Legislativos

NOTA Nº 44254
SANTA FE "Cuna de la Constitución Nacional" 14/07/2022
REF.:Comunic 28481/22

Señor:

MINISTRO DE GESTION PUBLICA

Tengo el agrado de dirigirme a usted a los fines de hacerle llegar fotocopia autenticada de la Comunicación de referencia, aprobada por la H. Cámara de DIPUTADOS

.....

Su respuesta a la presente, será remitida por intermedio de esta Dirección a la H. Cámara de origen.

Salúdole muy atentamente.

Abog. María Soledad Senn
Subsecretaria de Asuntos Legislativos
Ministerio de Gobierno
Justicia y Derechos Humanos
Provincia de Santa Fe

NOTA Nº 28481 22

FOLIO Nº 2

CÁMARA DE DIPUTADOS
DE LA PROVINCIA DE SANTA FE

SANTA FE, 23 de junio de 2022.

Al señor
Gobernador de la Provincia
C.P.N. Omar PEROTTI
SU DESPACHO

Tengo el agrado de dirigirme al señor Gobernador llevando a su conocimiento que esta Cámara de Diputados, en sesión de la fecha, ha aprobado la Comunicación **Nº 46853 CD,** cuyo texto a continuación se transcribe:

"La Cámara de Diputados de la Provincia vería con agrado que el Poder Ejecutivo, por intermedio del organismo que corresponda, informe en relación con la filtración de datos informáticos sensibles del portal web santafe.gob.ar informada por la empresa DarkTracer, lo siguiente:

a) si el gobierno tenía conocimiento de la filtración previo al informe de la mencionada empresa;

b) si se han implementado y actualizado las medidas de seguridad; y,

c) si se dio aviso a las personas que sufrieron el robo de sus datos informáticos sensibles del portal web de la provincia."

Salúdole muy atentamente.

ES COPIA

Victor Manuel Reynoso
Subdirector General de Técnica Legislativa
Ministerio de Gobierno, Justicia
y Derechos Humanos

RECIBIDO
04 JUL 2022
Registro Gral.
de Leyes

CÁMARA DE DIPUTADOS DE LA PROVINCIA DE SANTA FE

Lic. GUSTAVO PUCCINI
SECRETARIO PARLAMENTARIO
CÁMARA DE DIPUTADOS

Provincia de Santa Fe
Ministerio de Gestión Pública

MINISTERIO DE GESTIÓN PÚBLICA
FOLIO Nº
3

REF. EXPTE. Nº 02001-0061778-0

/ / /TA FE, "***Cuna de la Constitución Nacional***", 26 de julio de 2022

Visto. A los efectos correspondientes, gírense las presentes actuaciones al Sr. **Secretario de Tecnologías para la Gestión.-**

Oficie la presente de atenta nota.-

CPN MARCELO VAZQUEZ
SECRETARIO PRIVADO
MINISTERIO DE GESTIÓN PÚBLICA

Son 03 fs.
mgb

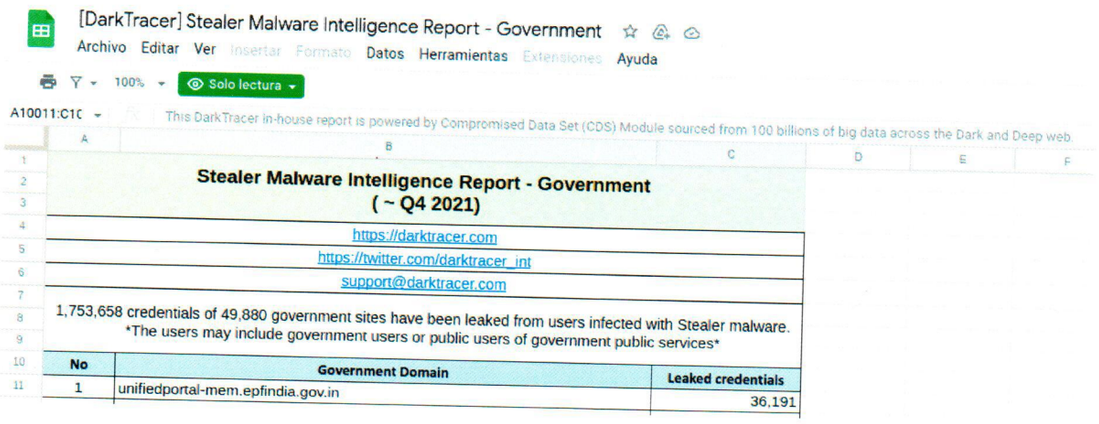
Mas allá de la infraestructura de protección que posteriormente detallaremos, se realizan consultas programadas basadas en herramientas OSINT para buscar publicaciones relacionadas con brechas de seguridad donde se nombre a los sitios de gobierno de Santa Fe.

La información que motiva esta consulta fue detectada el 2/3/22 6:45AM en el siguiente twitt

https://twitter.com/darktracer_int/status/1498957779813679105

Allí se exponían los 10000 sitios de gobierno mas comprometidos (a nivel mundial), y se publicó un xls en Drive con los dominios y la cantidad de cuentas supuestamente comprometidas

https://docs.google.com/spreadsheets/d/1KC615oNu1GJN4hymAR1Hxe1M46WG_FW4UMmHWbD3y3s/edit#gid=0



[DarkTracer] Stealer Malware Intelligence Report - Government

Archivo Editar Ver Insertar Formato Datos Herramientas Extensiones Ayuda

100% Solo lectura

This DarkTracer in-house report is powered by Compromised Data Set (CDS) Module sourced from 100 billions of big data across the Dark and Deep web.

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

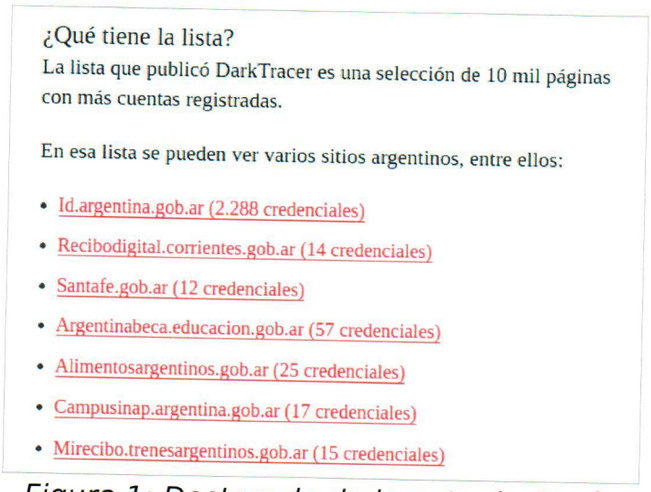
No	Government Domain	Leaked credentials
1	unifiedportal-mem.epfindia.gov.in	36,191

Cabe destacar de este informe que entre los **top 10000** sitios mundiales solo figuraban **256 argentinos**, de ellos **7 de Santa Fe** pertenecientes al poder Judicial, EPE, MPA y algunos ministerios. Nosotros podemos responder solo por los que están alojados en la infraestructura central basada en los 2 centros de procesamiento de datos (principal y secundario) de la ciudad de Santa Fe.

La cantidad de **credenciales indicadas (12)** es un número absolutamente irrelevante respecto a la cantidad de cuentas activas, al menos en la plataforma de correo e Intranet que superan las 160000

Tampoco indican que hayan sido hackeadas, sino que mayormente fueron recolectadas de formularios de phishing, sitios gemelos, etc, donde usuarios inexpertos dejan sus datos.

Diario Clarín lo levanta en una nota el mismo día 2 de marzo a las 15:45 https://www.clarin.com/tecnologia/aseguran-filtraron-1-7-millones-accesos-sitios-gubernamentales-256-dominios-argentinos_0_CS73etXFEc.html



¿Qué tiene la lista?

La lista que publicó DarkTracer es una selección de 10 mil páginas con más cuentas registradas.

En esa lista se pueden ver varios sitios argentinos, entre ellos:

- Id.argentina.gob.ar (2.288 credenciales)
- Recibodigital.corrientes.gob.ar (14 credenciales)
- Santafe.gob.ar (12 credenciales)
- Argentinabeca.educacion.gob.ar (57 credenciales)
- Alimentosargentinos.gob.ar (25 credenciales)
- Campusinap.argentina.gob.ar (17 credenciales)
- Mirecibo.trenesargentinos.gob.ar (15 credenciales)

Figura 1: Destacado de la nota de Clarín

Las fuentes de datos de esta empresa son acumulativas, por lo que la cantidad de cuentas comprometidas no es actual, y muchas de ellas seguramente ya han cambiado sus claves o no están mas activas.

Tal como se ve en el mail adjunto, me puse en contacto con la empresa, la que jamas respondió al correo, ya que en el Drive de muestra indica que la información detallada solo la brindan a sus CLIENTES en el modulo de CDS (Compromised Data Set), siendo este un producto de pago en dolares.

https://darktracer.com/pricing

La infraestructura central vinculada a Internet esta protegida por 2 equipos IDS/IPS que analizan trafico de red, con contrato de soporte vigente y actualizaciones permanentes. Esto permite bloquear y mitigar automáticamente unos **200 mil intentos de acceso diarios** en los 2 enlaces principales de Internet. Se pueden observar detalles en los gráficos del reporte que se adjuntan.

Sumado a estos equipos IPS existen diferentes barreras de seguridad combinadas entre Firewalls de red, WAF y zonas DMZ que hacen que los ataques recibidos hasta el momento no hayan concretado su objetivo.

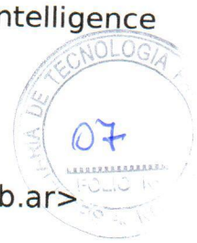
Estas medidas de mitigación son dinámicas y se van implementando a medida que los análisis de riesgo periódicos y vulnerabilidades publicadas lo requieren, ya sea porque se publican nuevos servicios y sistemas o bien se descubren vulnerabilidades sobre los ya publicados.

Por supuesto que no podemos decir que estamos 100% ya que eso no puede decirlo ninguna organización, pero hasta el momento los intentos de intrusión, phishing, etc detectados no han sido positivos.

También se realizan comunicaciones a las sectoriales sobre vulnerabilidades, parches, ciclos de vida de productos de software, etc, a fin de mantener actualizada y seguras las aplicaciones desplegadas, todas estas relacionadas con la información recibida del CERT.AR, LACNIC, NIST, etc sobre alertas de seguridad.

Téc. FERNANDO CORVALAN
Subsecretario de Infraestructura
Tecnológica y Comunicaciones
SECRETARÍA DE TECNOLOGÍAS PARA LA GESTIÓN

Asunto: Request for Information about "[DarkTracer] Stealer Malware Intelligence Report - Government"
De: Fernando Corvalan STG GSF <fernandocorvalan@santafe.gob.ar>
Fecha: 24/3/22 21:58
A: support@darktracer.com
Message-ID: <b6196c7e-3be9-5a6b-b76c-51d29b12940b@santafe.gob.ar>
MIME-Version: 1.0
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Thunderbird/91.7.0
Content-Language: es-AR
Content-Type: text/plain; charset=UTF-8; format=flowed
Content-Transfer-Encoding: 8bit



Contact them for the "Stealer Malware Intelligence - Government" Report, and I have been following the different publications of the same.
I am the official in charge of the technological infrastructure of the Santa Fe government (santafe.gov.ar) and the list of affected credentials would be very useful to be able to act more proactively with these users.
Although we have issued warning bulletins, if we were able to have this data, it would be very important to analyze possible intrusions or breaches that, if they did exist, we have not yet detected.
Thank you very much for your attention.

--
Fernando A. Corvalan
Subsecretario de Infraestructura Tecnológica y Comunicaciones
Secretaría de Tecnologías para la Gestión
Ministerio de Gestión Pública

Gobierno de Santa Fe
Ministerio de Gestión Pública
Secretaría de Tecnologías para la Gestión

Política de Seguridad

IPS

Hardware

Los equipos utilizados para la protección de amenazas y vulnerabilidades son dos IPS marca IBM modelo XGS5100 con bahías de extensión de puertos, ubicados uno en cada Centro de Procesamiento de Datos del Gobierno Provincial.

Se trata de dispositivos exclusivos basados en hardware de características modulares, con procesadores con capacidad de realizar una inspección profunda y detallada a través de sensores de características "inline" aplicados sobre cada segmento de red definido.

Firmware

El firmware de los IPS se actualiza cada vez que el proveedor libera una nueva versión. Al día de la fecha se encuentra instalada la versión IBM QRadar Network Security 5.5.0.11 publicada el 19 de julio de 2022.

Ambos equipos se encuentran gestionados mediante un controlador que permite desplegar políticas en forma centralizada y almacenar los registros de eventos para posterior análisis.

Licencias

Los IPS se encuentran licenciados para habilitar las siguientes funcionalidades:

- Flexible Performance Level 2
- Identity and Application Control
- Reputación IP y Geolocalización
- Inspección SSL
- Actualizaciones de contenido X-Force
- Actualización de Firmware

Políticas

La protección contra vulnerabilidades desde internet esta especificada según recomendación de X-Force y utilizando patrones de "firmas" de ataques que se actualizan diariamente.

Se cuenta con protección de sitios con mala reputación IP y Geolocalización de ubicaciones geográficas donde no se esperan que exista tráfico.

Todos los servidores web cuentan con una política de Inspección SSL online para evitar ataques que puedan venir encriptados.

Actualizaciones

Los dispositivos utilizan las siguientes actualizaciones:

Actualizaciones de firmware

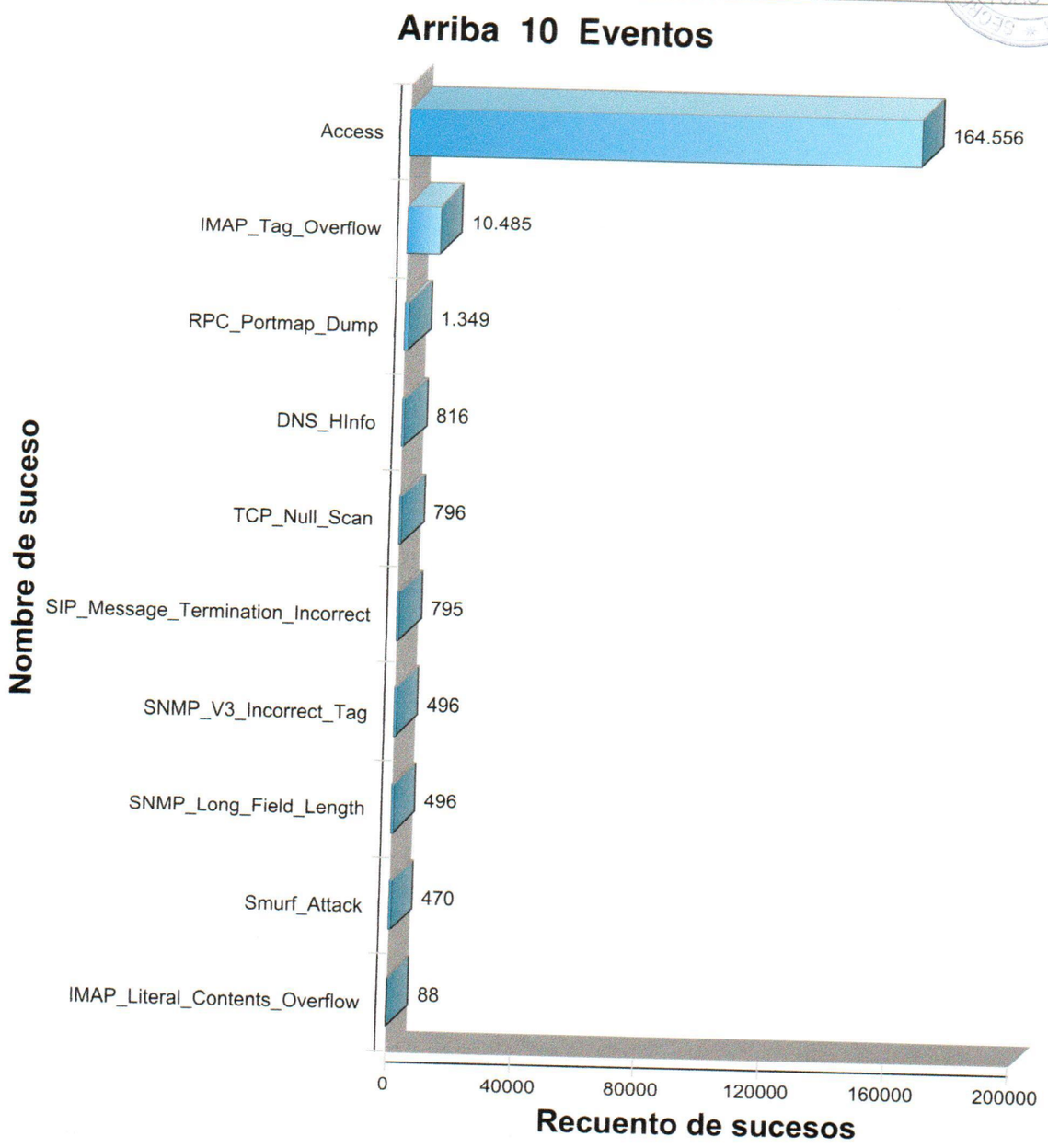
Contienen nuevos archivos de programa, correcciones o parches, mejoras y ayuda en línea. Esta actualización es un proceso que debe realizarse en forma manual.

Actualizaciones de seguridad

Las actualizaciones de seguridad contienen los más recientes contenidos de seguridad de IBM X-Force respecto a firmas de IPS, clasificación URL, y reputación IP, que a su vez se retroalimenta de información de terceros para lograr una mejor clasificación. Estas actualizaciones se realizan regularmente en forma automática.

Informe diario IPS STG

Grupo(s): Internet
Hora de inicio: 02/08/2022 23:10
Hora de finalización: 03/08/2022 23:10



Nombre de suceso	Gravedad	Recuento de sucesos	Porcentaje total
Access	Medio	164.556	90,95%
IMAP_Tag_Overflow	Alto	10.485	5,80%
RPC_Portmap_Dump	Bajo	1.349	0,75%
DNS_HInfo	Bajo	816	0,45%
TCP_Null_Scan	Bajo	796	0,44%
SIP_Message_Termination_Incorrect	Bajo	795	0,44%
SNMP_Long_Field_Length	Bajo	496	0,27%
SNMP_V3_Incorrect_Tag	Bajo	496	0,27%
Smurf_Attack	Medio	470	0,26%
IMAP_Literal_Contents_Overflow	Alto	88	0,05%

Información de seguridad

Access

https://exchange.xforce.ibmcloud.com/signature/Access

Medio

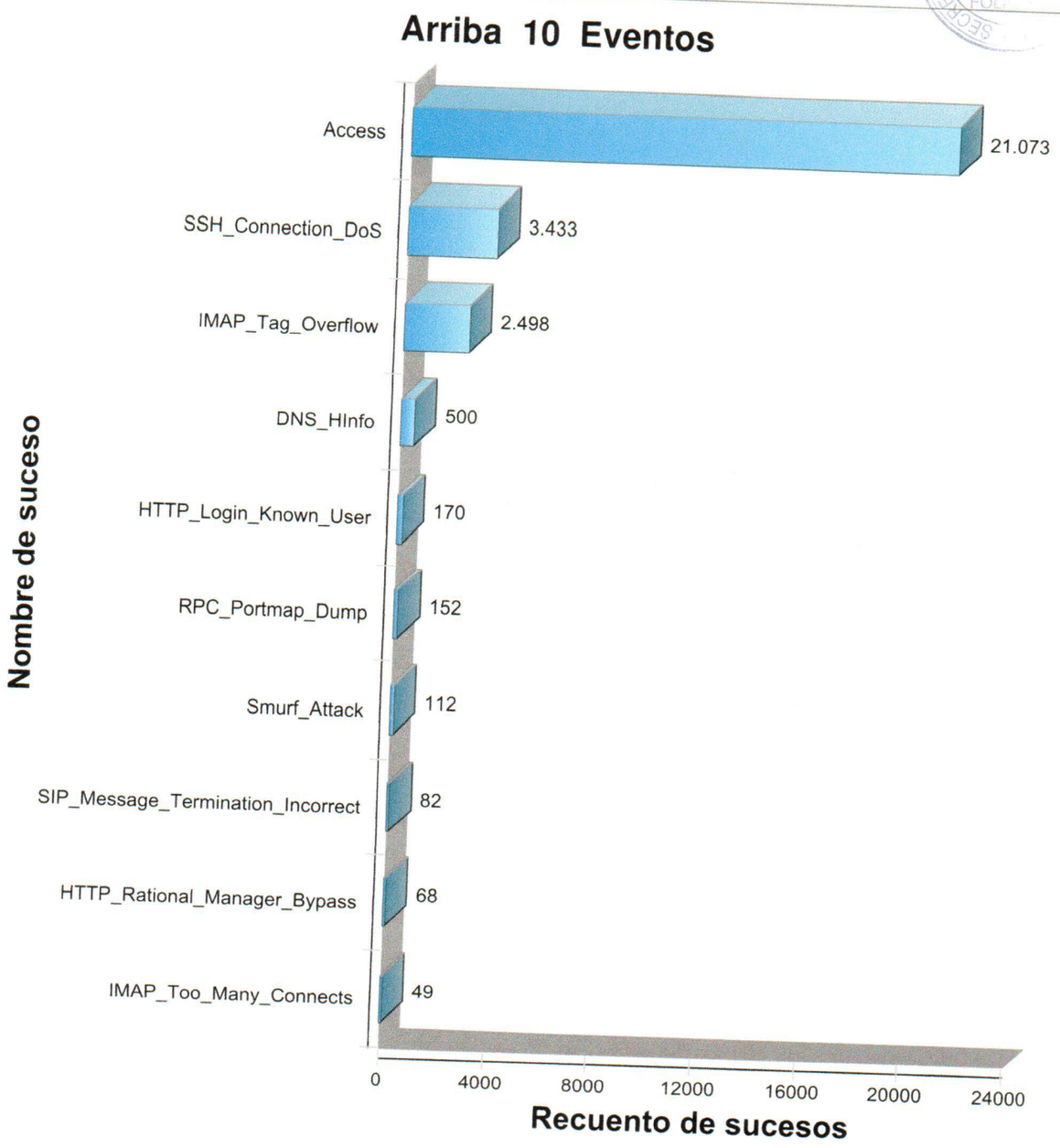
Falta información de seguridad impresa hasta que la XPU de base de datos de SiteProtector apropiada se haya aplicado.

Orígenes de sucesos (5540)

Origen	Primer suceso	Último suceso	Recuento de sucesos
186.121.182.125	3 ago 2022 0:00	3 ago 2022 23:00	36.587
190.231.23.148	3 ago 2022 3:00	3 ago 2022 18:00	26.140
181.81.128.72	3 ago 2022 0:00	3 ago 2022 22:00	14.296
190.231.22.4	3 ago 2022 3:00	3 ago 2022 9:00	11.704
190.231.22.220	3 ago 2022 0:00	3 ago 2022 1:00	3.846
190.231.22.106	3 ago 2022 20:00	3 ago 2022 22:00	3.402
185.191.171.6	3 ago 2022 0:00	3 ago 2022 23:00	3.350
185.191.171.4	3 ago 2022 0:00	3 ago 2022 23:00	3.132
185.191.171.22	3 ago 2022 0:00	3 ago 2022 23:00	2.840
190.231.20.151	3 ago 2022 2:00	3 ago 2022 3:00	2.781
185.191.171.15	3 ago 2022 0:00	3 ago 2022 23:00	2.771
185.191.171.13	3 ago 2022 0:00	3 ago 2022 23:00	2.421
185.191.171.43	3 ago 2022 0:00	3 ago 2022 23:00	2.305
205.205.150.26	3 ago 2022 18:00	3 ago 2022 23:00	2.207
185.54.230.130	3 ago 2022 1:00	3 ago 2022 22:00	2.055
185.191.171.33	3 ago 2022 0:00	3 ago 2022 23:00	1.988
185.191.171.35	3 ago 2022 0:00	3 ago 2022 23:00	1.768
185.54.230.50	3 ago 2022 0:00	3 ago 2022 21:00	1.366
185.54.230.10	3 ago 2022 0:00	3 ago 2022 19:00	1.264
185.54.230.90	3 ago 2022 2:00	3 ago 2022 20:00	1.263
190.108.95.74	3 ago 2022 0:00	3 ago 2022 22:00	1.243
222.162.139.12	3 ago 2022 0:00	3 ago 2022 23:00	1.162

Informe diario IPS CPDP

Grupo(s):	CPDP
Hora de inicio:	02/08/2022 23:00
Hora de finalización:	03/08/2022 23:00



Nombre de suceso	Gravedad	Recuento de sucesos	Porcentaje total
Access	Medio	21,073	74.36%
SSH_Connection_DoS	Medio	3,433	12.11%
IMAP_Tag_Overflow	Alto	2,498	8.81%
DNS_HInfo	Bajo	500	1.76%
HTTP_Login_Known_User	Bajo	170	0.60%
RPC_Portmap_Dump	Bajo	152	0.54%
Smurf_Attack	Medio	112	0.40%
SIP_Message_Termination_Incorrect	Bajo	82	0.29%
HTTP_Rational_Manager_Bypass	Alto	68	0.24%
IMAP_Too_Many_Connects	Bajo	49	0.17%

Información de seguridad

Access

https://exchange.xforce.ibmcloud.com/signature/Access

Medio

Falta información de seguridad impresa hasta que la XPU de base de datos de SiteProtector apropiada se haya aplicado.

Orígenes de sucesos (1337)

Origen	Primer suceso	Último suceso	Recuento de sucesos
89.248.163.158	3 ago. 2022 08:00	3 ago. 2022 08:00	7,004
204.101.161.19	3 ago. 2022 00:00	3 ago. 2022 22:00	670
62.75.151.88	3 ago. 2022 04:00	3 ago. 2022 21:00	661
190.6.96.211	3 ago. 2022 00:00	3 ago. 2022 22:00	568
200.12.208.62	3 ago. 2022 00:00	3 ago. 2022 22:00	475
89.248.165.178	3 ago. 2022 00:00	3 ago. 2022 22:00	272
45.143.203.15	3 ago. 2022 00:00	3 ago. 2022 22:00	213
77.234.46.217	3 ago. 2022 19:00	3 ago. 2022 21:00	210
45.143.203.95	3 ago. 2022 01:00	3 ago. 2022 22:00	196
92.63.197.111	3 ago. 2022 00:00	3 ago. 2022 21:00	187
185.156.73.122	3 ago. 2022 00:00	3 ago. 2022 22:00	179
89.248.163.247	3 ago. 2022 00:00	3 ago. 2022 22:00	178
92.63.197.83	3 ago. 2022 00:00	3 ago. 2022 22:00	175
89.248.165.199	3 ago. 2022 00:00	3 ago. 2022 22:00	169
92.63.197.70	3 ago. 2022 00:00	3 ago. 2022 21:00	164
89.248.163.240	3 ago. 2022 00:00	3 ago. 2022 22:00	161
93.174.93.227	3 ago. 2022 00:00	3 ago. 2022 22:00	161
185.156.74.58	3 ago. 2022 00:00	3 ago. 2022 22:00	160
185.156.74.34	3 ago. 2022 00:00	3 ago. 2022 22:00	160
89.248.163.239	3 ago. 2022 00:00	3 ago. 2022 22:00	158
89.248.163.241	3 ago. 2022 00:00	3 ago. 2022 22:00	154
89.248.165.104	3 ago. 2022 00:00	3 ago. 2022 22:00	131

SECRETARÍA DE TECNOLOGÍA PARA LA GESTIÓN
16
FOLIO Nº

Santa Fe, 09 de Agosto de 2022

Señor

Director Provincial de Infraestructura Tecnológica

Secretaría de Tecnologías para la Gestión

Enrique Segalerba

S / D

En vista de la Nota N 28481 22, informamos que desde las áreas informáticas diariamente se reciben reportes e informes de distintos organismos de seguridad que suelen incluir este tipo de cuestiones. Además se llevan a cabo mitigaciones y mejoras en los procesos de seguridad, actualizando sistemas y procedimientos, muchos de ellos automáticos que detectan online algunas cuestiones de este tipo, toman acción y nos informan, por ejemplo de cuentas de correo con actividad fuera de lo normal.

Cabe aclarar que en este caso en particular la filtración no se dio porque vulneraron algún sistema nuestro, sino por Phishing o SPYs a los dispositivos de los clientes. En las bases de autenticación de la Provincia hay en la actualidad mas de 350.000 cuentas acceso a sistemas y mas de 16.000 cuentas de correo y la cantidad "informada por la empresa" es mínima frente a esas cantidades.

Constantemente se piensa en cómo mejorar la seguridad de la información ya que día tras día aparecen nuevas amenazas, esto requiere de gente exclusiva, especializada y con mucha capacitación. Tengamos en cuenta que la seguridad 100% no existe, pero si todos respetamos ciertas normas podemos minimizar las amenazas, en virtud de esto desde el área de Infraestructura para Aplicaciones se envían recomendaciones de seguridad y estándares a las Sectoriales de Informática de cada Ministerio para que las difundan entres sus usuarios.

El los últimos tiempos se a visto que incluso las entidades financieras están teniendo problemas similares en cuanto al Fishing y la Suplantación de páginas Web, no estaría demás que el área de capacitación implemente un plan a corto y mediano plazo para difundir de forma orgánica las recomendaciones de seguridad, las buenas prácticas y las normativas vigentes, ya que la responsabilidad de la utilización de las cuentas es del usuario y debe protegerlas con contraseñas robustas y prestar atención de no entregarlas a terceros.

Para concluir, la información publicada no implica que necesariamente hubo

una vulneración de los sistemas para obtener credenciales, sino que las mismas pudieron ser obtenidas desde los propios usuarios. Lo que es bastante probable teniendo en cuenta que el nro de cuentas informadas es bastante bajo respecto a la cantidad de cuentas que se gestionan en los sistemas.

Asimismo contamos con elementos de seguridad activos que detectan el uso indebido de las cuentas como intentos de accesos reiterados y envíos de correos masivos, que toman acción, informan y bloquean las cuentas.

Sin mas, lo saludo atentamente.

Juan Moragues
Coordinador Área
Infraestructura para Aplicaciones y Servicios
Dirección Provincial de Infraestructura Tecnológica

Ref. Expte. Nro. 02001-0061778-0
Iniciador: Cámara de Diputados
Solicita informe en relación a filtración de datos

//TA FE, 22 de Agosto de 2022.-

Vuelvan las presentes actuaciones administrativas, a la Secretaría Privada del Ministerio de Gestión Pública, para la prosecución del trámite administrativo correspondiente.-

Sirva la presente de atenta nota de remisión.-

Téc. FERNANDO CORVALAN
Subsecretario de Infraestructura
Tecnológica y Comunicaciones
SECRETARÍA DE TECNOLOGÍAS PARA LA GESTIÓN

Provincia de Santa Fe
Ministerio de Gestión Pública

MINISTERIO DE GESTIÓN PÚBLICA
FOLIO N° 19

Santa Fe, Cuna de la Constitución, 1 de setiembre de 2022.-

Ref. Expte. N.º : 02001-0061778-0

Con la intervención correspondiente, gírense las presentes actuaciones a la ***SUBSECRETARÍA DE ASUNTOS LEGISLATIVOS***, a los efectos se sirva dar continuidad al trámite.

Sirva la presente de atte. Nota:

MARCOS CORACH
MINISTRO DE GESTIÓN PÚBLICA

g.g.
Son fs. 19

PROVINCIA DE SANTA FE
Ministerio de Gobierno, Justicia y
Derechos Humanos

NOTA Nº: 520130 SANTA FE - 8 SEP. 2022

HONORABLE CÁMARA
DE DIPUTADOS Y DIPUTADAS
DE LA PROVINCIA DE SANTA FE

En respuesta a la **Comunicación N° 28481/22** de esa Honorable Cámara remitida por el Poder Ejecutivo, en relación a informe sobre aspectos vinculados con la filtración de datos informáticos del portal web santafe.gob.ar.

Se remite **Expediente N° 02001-0061778-0** con las tramitaciones administrativas de las áreas y autoridades competentes, en la cual obra la respuesta a fs. 04 a 17 avalado por el Ministro del área a fs. 19.

Sirva la presente de atenta nota de envío.

Abog. María Soledad Seiin
Subsecretaria de Asuntos Legislativos
Ministerio de Gobierno
Justicia y Derechos Humanos
Provincia de Santa Fe