SOLUZIONI

REPORTE MENSUAL - ANTISPAM

“Servicio de Seguridad Perimetral en Alta Disponibilidad para el INSN”

Instituto Nacional de Salud del Niño

INSN

JULIO 2024

Project Manager Office Soluzioni

SOLUZIONI

CONTENIDO

ILUSTRACIONES

Telf.: (+511) 4018460

www.soluzioni.pe | contacto@soluzioni.pe

Calle Los Petirrojos 495 – San Isidro

INTRODUCCION

Barracuda Email Security Gateway es una solución integrada de hardware y software diseñada para proteger su servidor de correo electrónico contra ataques de spam, virus, suplantación de identidad, phishing y spyware. Las opciones de filtrado y cifrado de salida también impiden que la información confidencial o confidencial se filtre deliberadamente o sin intención fuera de la organización. La capa de protección en la nube (CPL) protege a los servidores de correo electrónico del malware entrante y de los ataques DoS mientras filtra el correo spam antes de que toque el perímetro de la red.

En el presente informe se detalla a través de análisis estadísticos el flujo de correo entrante y saliente identificado por la solución ESG Barracuda perteneciente al mes de JULIO.

Telf.: (+511) 4018460
www.soluzioni.pe | contacto@soluzioni.pe
Calle Los Petirrojos 495 – San Isidro

1. Tráfico entrante

El objetivo de Barracuda ESG y CPL es identificar el tráfico spam entrante sin bloquear mensajes válidos.

1.1 CPL Barracuda Estadísticas de correo electrónico entrante

La función opcional Barracuda Cloud Protection Layer (CPL) de Barracuda Email Security Gateway es una capa adicional de protección basada en la nube que bloquea las amenazas antes de que lleguen a su red, evita el phishing y los ataques de día cero, y proporciona continuidad al correo electrónico.

A continuación, se muestra un resumen estadístico perteneciente al mes de JULIO.

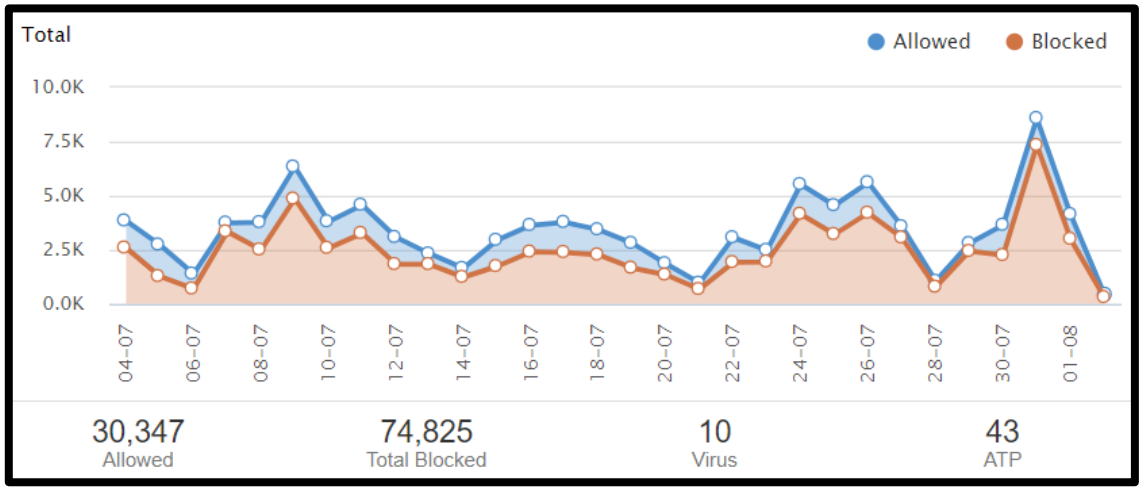

Ilustración 1: Estadística General CPL

Interpretación:

Se puede observar en la ilustración N°1 que en el periodo de análisis del tráfico entrante:

- Se permitieron 30347 correos.
- Se bloquearon 74825 correos.
- Se detectaron 10 Virus.
- Se detectaron 43 Amenazas avanzadas.

Telf.: (+511) 4018460
www.soluzioni.pe | contacto@soluzioni.pe
Calle Los Petirrojos 495 – San Isidro

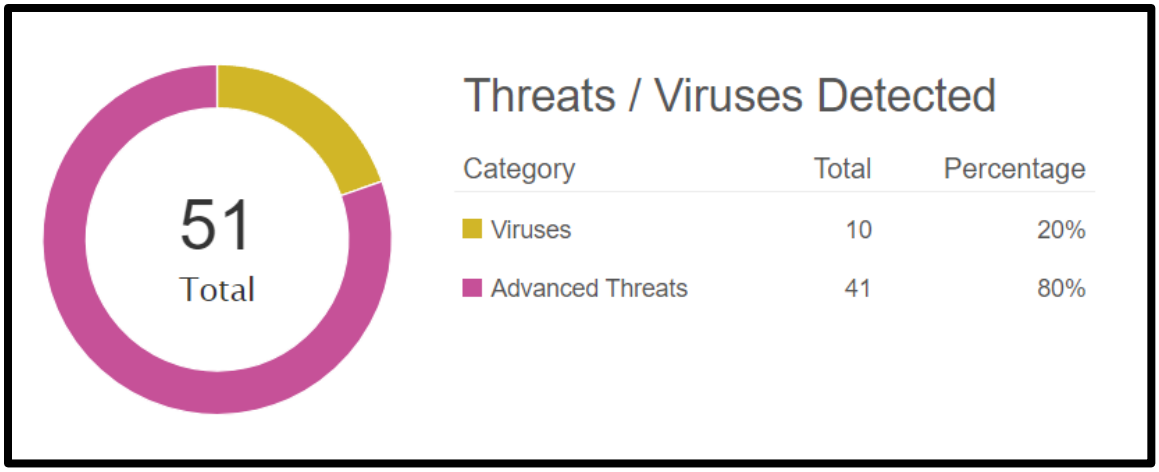

Ilustración 2: Estadística de Amenazas Avanzadas y Virus

Interpretación:

Se puede observar en la ilustración N°2 que en el periodo del análisis del tráfico entrante:

- Se detectaron 10 Virus.
- Se detectaron 41 Amenazas avanzadas.

Telf.: (+511) 4018460
www.soluzioni.pe | contacto@soluzioni.pe
Calle Los Petirrojos 495 – San Isidro

Rank	Sender	Blocked
1	marketing@naochan.org	15,743
2	info@moriaa.com	10,189
3	sender@muratauto.com	8,387
4	-	5,002
5	nsanchez.sma@tlaxcala.gob.mx	2,327
6	correo@insn.gob.pe	2,221
7	jruiz@eaav.gov.co	2,185
8	dsalas@emaseo.gob.ec	1,858
9	info@caffemario.com	1,350
10	mail@insn.gob.pe	1,198

Ilustración 3: Top de cuentas externas que generaron SPAM en CPL

Interpretación:

Se puede observar en la ilustración N°3 que en el periodo del análisis del tráfico entrante:

- Se detectaron diferentes cuentas externas originarias del tráfico spam en el top 3 (marketing@naochan.org, info@moriaa.com, sender@muratauto.com)
- Cabe mencionar que estos correos maliciosos fueron bloqueados en el ambiente CPL.

Telf.: (+511) 4018460
www.soluzioni.pe | contacto@soluzioni.pe
Calle Los Petirrojos 495 – San Isidro

Rank	Recipient	Blocked
1	correo@insn.gob.pe	2,221
2	mail@insn.gob.pe	1,198
3	admin@insn.gob.pe	1,135
4	habarca@insn.gob.pe	550
5	amaurtua@insn.gob.pe	424
6	mvicuna@insn.gob.pe	413
7	lkolevic@insn.gob.pe	373
8	lkaseng@insn.gob.pe	361
9	brojas@insn.gob.pe	361
10	onunez@insn.gob.pe	324

Ilustración 4: Top de cuentas internas a las que enviaron SPAM en CPL

Interpretación:

Se puede observar en la ilustración N°4 que en el periodo del análisis del tráfico entrante:

- Un top 10 de direcciones de correo internas que más tráfico de spam recibieron.
- Cabe mencionar que estos correos maliciosos fueron bloqueados en el ambiente CPL.

Telf.: (+511) 4018460
www.soluzioni.pe | contacto@soluzioni.pe
Calle Los Petirrojos 495 – San Isidro

1.2 Appliance ESG Barracuda Estadísticas de correo electrónico entrante

Day	Rate Controlled	Blocked: Spam	Blocked: Virus	Quarantined	Allowed: Tagged	Allowed	Total Received
2024-07-01	0	104	0	0	61	1353	1518
2024-07-02	0	143	0	0	58	1359	1560
2024-07-03	0	70	0	0	45	1155	1270
2024-07-04	0	116	0	0	48	1100	1264
2024-07-05	0	131	0	0	79	1212	1422
2024-07-06	0	68	0	0	70	515	653
2024-07-07	0	91	0	0	28	340	459
2024-07-08	0	45	0	0	42	1163	1250
2024-07-09	0	195	0	0	52	1246	1493
2024-07-10	0	144	0	0	43	1054	1241
2024-07-11	0	98	0	0	43	1150	1291
2024-07-12	0	76	0	0	50	1113	1239
2024-07-13	0	22	0	0	13	396	431
2024-07-14	0	71	0	0	18	329	418
2024-07-15	0	63	0	0	61	1113	1237
2024-07-16	0	88	0	0	73	1117	1278
2024-07-17	0	152	0	0	168	1087	1407
2024-07-18	0	147	0	0	35	946	1128
2024-07-19	0	168	0	0	66	957	1191
2024-07-20	0	61	0	0	46	304	411
2024-07-21	0	41	0	0	13	229	283
2024-07-22	0	116	0	0	58	1080	1254
2024-07-23	0	86	0	0	30	368	484
2024-07-24	0	201	0	0	49	1188	1438
2024-07-25	0	102	0	0	52	1180	1334
2024-07-26	0	54	0	0	330	937	1321
2024-07-27	0	13	0	0	60	415	488
2024-07-28	0	20	0	0	25	198	243
2024-07-29	0	21	0	0	8	363	392
2024-07-30	0	64	0	0	204	1244	1512
2024-07-31	0	63	0	0	32	1100	1195
Total	**0**	**2834**	**0**	**0**	**1960**	**27311**	**32105**

Ilustración 5: Tráfico de correo Entrante

Interpretación:

Se puede observar en la ilustración N°5 en el periodo del análisis del tráfico entrante del barracuda local on-premise:

- Se permitieron 27311 correos.
- Se bloquearon 2834 correos.
- Se detectaron 0 virus.

Telf.: (+511) 4018460
www.soluzioni.pe | contacto@soluzioni.pe
Calle Los Petirrojos 495 – San Isidro

#	Top Spam Recipients	Count
1	wzevallos@insn.gob.pe	302
2	lcancino@insn.gob.pe	224
3	cosorio@insn.gob.pe	222
4	cpillaca@insn.gob.pe	186
5	savilah@insn.gob.pe	147
6	csotou@insn.gob.pe	140
7	jagueroa@insn.gob.pe	131
8	jreque.insn@gmail.com	119
9	apenadillo@insn.gob.pe	62
10	iguzmanc@insn.gob.pe	48

Ilustración 6: Top de cuentas internas a las que enviaron SPAM en el ESG

Interpretación:

Se puede observar en la ilustración N°6 en el periodo del análisis del tráfico entrante del barracuda local y on-premise:

- Un top 10 de direcciones de correo internas que más tráfico de spam recibieron.
- Cabe mencionar que estos correos maliciosos fueron bloqueados en el ambiente local.

Telf.: (+511) 4018460
www.soluzioni.pe | contacto@soluzioni.pe
Calle Los Petirrojos 495 – San Isidro

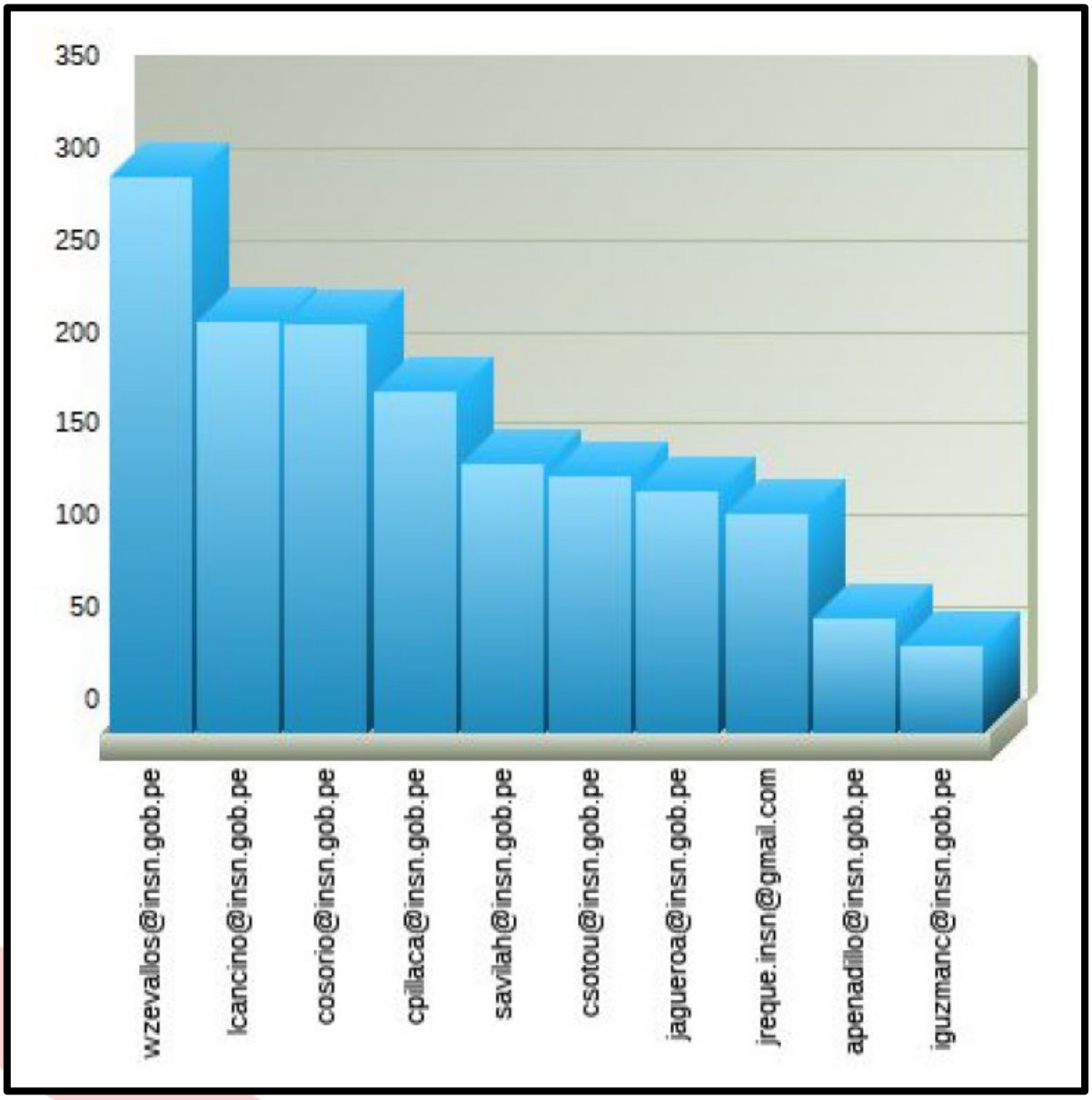

Ilustración 7: Gráfico de las cuentas internas a las que enviaron SPAM en el ESG

Telf.: (+511) 4018460
www.soluzioni.pe | contacto@soluzioni.pe
Calle Los Petirrojos 495 – San Isidro

2. Tráfico Saliente

El objetivo de Barracuda ESG es identificar el tráfico spam saliente sin bloquear mensajes válidos.

Day	Rate Controlled	Blocked: Spam	Blocked: Virus	Quarantined	Sent	Authentication Failure	Total Received
2024-07-01	1111	181	0	0	3137	0	4431
2024-07-02	783	11	0	0	3700	0	4495
2024-07-03	1029	3	0	0	3766	0	4798
2024-07-04	1015	5	0	0	3506	0	4526
2024-07-05	1172	316	0	0	2896	0	4384
2024-07-06	315	0	0	0	1164	0	1479
2024-07-07	0	0	0	0	202	0	202
2024-07-08	137	1	0	0	2018	0	2156
2024-07-09	1033	9	0	0	6217	0	7259
2024-07-10	336	24	0	0	3591	0	3951
2024-07-11	949	11	0	0	3263	0	4223
2024-07-12	373	3	0	0	2245	0	2621
2024-07-13	0	0	0	0	501	0	501
2024-07-14	0	0	0	0	166	0	166
2024-07-15	494	149	0	0	2419	0	3062
2024-07-16	458	11	0	0	2602	0	3071
2024-07-17	665	2	0	0	3949	0	4616
2024-07-18	621	3	0	0	2853	0	3477
2024-07-19	1726	3	0	0	4427	0	6156
2024-07-20	1193	4	0	0	2802	0	3999
2024-07-21	994	1	0	0	3320	0	4315
2024-07-22	975	1327	0	0	3878	0	6180
2024-07-23	556	679	0	0	1244	0	2479
2024-07-24	1025	3	0	0	5879	0	6907
2024-07-25	2027	16	0	0	5164	0	7207
2024-07-26	865	7	0	0	3660	0	4532
2024-07-27	0	3	0	0	692	0	695
2024-07-28	0	5	0	0	154	0	159
2024-07-29	0	3	0	0	129	0	132
2024-07-30	0	3	0	0	2244	0	2247
2024-07-31	594	2	0	0	2906	0	3502
Total	**20446**	**2785**	**0**	**0**	**84694**	**0**	**107928**

Ilustración 8: Tráfico de correo Saliente

Interpretación:

Se puede observar en la ilustración N°8 en el periodo del análisis del tráfico saliente del barracuda local y on-premise:

- Se permitieron 84694 correos.
- Se bloquearon 2785 correos.
- Se detectaron 20446 intentos de salida de gran cantidad de correos.

Telf.: (+511) 4018460
www.soluzioni.pe | contacto@soluzioni.pe
Calle Los Petirrojos 495 – San Isidro

3. Conclusiones

- Se detectó una alta cantidad de bloqueos spam en el periodo de análisis.
- En el ambiente Cloud para el tráfico entrante se bloquearon 74825 y se permitieron 30347 correos.
- En el ambiente local para el tráfico entrante se bloquearon 2834 y se permitieron 27311.
- En el ambiente local para el tráfico saliente se bloquearon 2785 y se permitieron 84694.

4. Recomendaciones

- Se recomienda realizar un monitoreo diario de los correos bloqueados y permitidos en el CPL y ESG Barracuda para identificar algún falso positivo en el tráfico de correo.
- Se recomienda que el personal que administra la plataforma realice una investigación y depuración periódica de las reglas creadas para bloquear mensajes SPAM esto ayudará a obtener una mayor precisión en el bloqueo de mensajes spam y evitar los falsos positivos.
- Se recomienda que el personal que administra la plataforma realice una revisión periódica de las actualizaciones disponibles para aplicarlas al equipo ESG. Esto ayudará al que el ESG tenga las ultimas actualizaciones en base al sistema operativo, funcionalidad y parches de seguridad.
- Se recomienda utilizar el módulo de Message Log para solucionar y descartar problemas en el tráfico de correo entrante y saliente.
- En el módulo Attachment Filters se recomienda agregar las extensiones que siempre son utilizadas para el envío de Malware (*.js - *.vbs - *.jar - *.cab).

Telf.: (+511) 4018460
www.soluzioni.pe | contacto@soluzioni.pe
Calle Los Petirrojos 495 – San Isidro

SOLUZIONI

SOLUZIONI GROUP

Gestión de Servicios y Atención al Cliente

Telf.: (+511) 080 080 294

E-mail: soporte@soluzioni.pe

www.soluzioni.pe | contacto@soluzioni.pe

Calle Los Petirrojos 495 Urb. Palomar– San Isidro