CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

BOLETÍN DE CIBERSEGURIDAD

Año 5 | N.º 256

semana del 24 al 30 de mayo de 2024

LA SEMANA EN CIFRAS

IP INFORMADAS

3

IP advertidas en múltiples campañas de phishing y de fraude.

URL ADVERTIDAS

4

URL asociadas a sitios fraudulentos y campañas de phishing y malware

PARCHES COMPARTIDOS

1

Las mitigaciones son útiles en productos de Check Point.

HASH REPORTADOS

8

Hashes asociados a múltiples campañas de phishing con archivos que contienen malware.

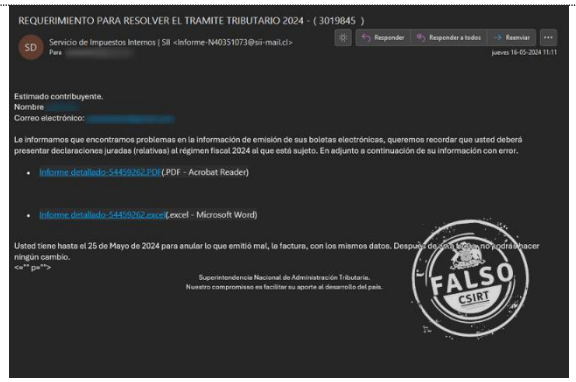
CONTENIDO

1. Malware 3
2. Phishing 5
3. Vulnerabilidades 7
4. Recomendaciones y buenas prácticas 8
5. Muro de la Fama 9

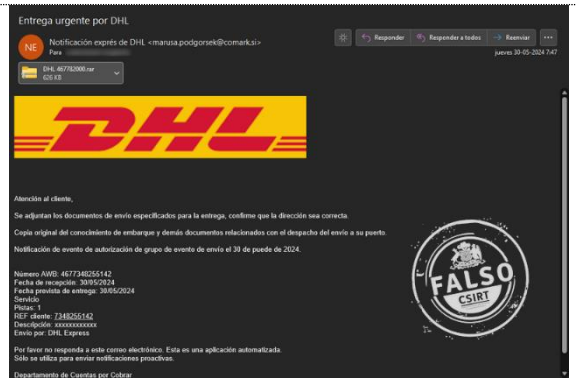
CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

1. Malware

Solicitud fraudulenta de datos bancarios - Suplantación con malware	
Código de alerta	CMV24-00464
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de mayo de 2024
Última revisión	27 de mayo de 2024
Indicadores de compromiso	
Asunto	
Datos bancarios	
Correo de salida	
laracena@synergygroup.com.do	
SHA256	
977131718295bb0d52814d2d30da09646abbbc32ced7a0a215000b59678e3195 9e87201967f5b16c669301ad815198837b8a9e7b50b9e9226e49f72fd2717363	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/cmv24-00464/	



Conaset - Suplantación con malware	
Código de alerta	CMV24-00465
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de mayo de 2024
Última revisión	28 de mayo de 2024
Indicadores de compromiso	
Asunto	
REQUERIMIENTO PARA RESOLVER EL TRAMITE TRIBUTARIO 2024 – (3019845)	
Correo de salida	
Informe-N40351073@sii-mail.cl	
SHA256	
69917b3dc70ffe5c6bfabff6ac0938c3ab2402826d0298bca26c1d72f698c22d 7e643c188a1ee3b0251b7dfcab000b7c48fd840eff35189e8a45901852e3910a 91a3d5c44efe38c16b038480db835d34b7f3151cda18fd066a7ee4c2270bd280 e28e34fbdaff077669586dcdb4e10f0ba2ca6c9973ed4d372a5c3ec3b8ad20e7	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/cmv24-00465/	



DHL - Suplantación con malware	
Código de alerta	CMV24-00466
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de mayo de 2024
Última revisión	30 de mayo de 2024

Indicadores de compromiso

Asunto

Entrega urgente por DHL

Correo de salida

barbara.kosi@colby.si

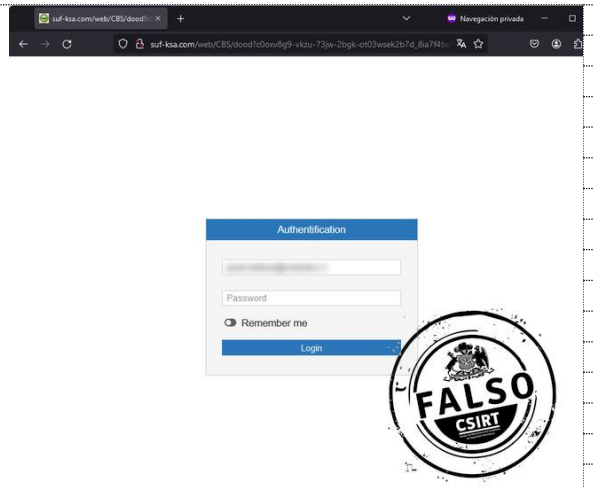
SHA256

739aa9e81a4963bce4521386fed3e464f0573125dc503249ab0d60000346d28f
ea07a13d0955fc66206df074a3beb333201e126389c224a045f9932a2b87d2ce

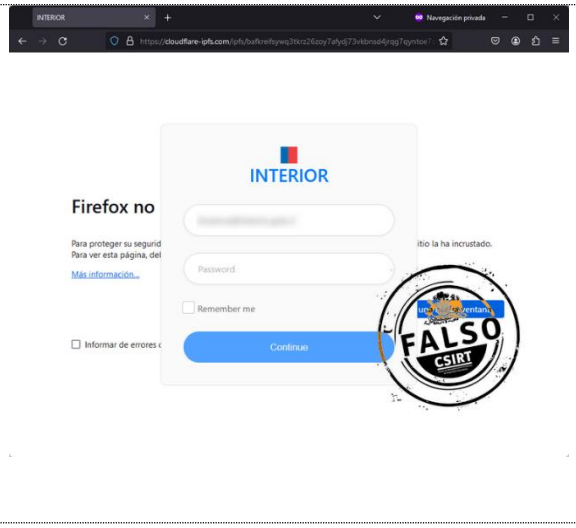
Enlace para revisar IoC:

https://csirt.gob.cl/alertas/cmv24-00466/

2. Phishing



Falso email llamando a cambiar contraseña - Phishing	
Alerta de seguridad cibernética	FPH24-00960
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de mayo de 2024
Última revisión	27 de mayo de 2024
Indicadores de compromiso	
URL redirección	
http://suf-ksa.com/web/CBS/index.php?email={Correoelectronico}	
URL del sitio falso	
http://suf-ksa.com/web/CBS/dood?	
Dirección IP sitio falso	
[162.215.249.101]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/fph24-00960/	



Ministerio del Interior y Seguridad Pública - Phishing	
Alerta de seguridad cibernética	FPH24-00961
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de mayo de 2024
Última revisión	28 de mayo de 2024
Indicadores de compromiso	
URL del sitio falso	
https://cloudflare-ipfs.com/ipfs/bafkreifsywq3tkrz26zoy7afydj73vkbnsd4jrqg7qyntoe7m4xibpdvyq?filename=Login-INBOX%2520%25281%2529last.html#{Correoelectronico}	
Dirección IP sitio falso	
[45.137.22.144]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/fph24-00961/	

Ministerio del Interior y Seguridad Pública - Phishing	
Alerta de seguridad cibernética	FPH24-00962
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de mayo de 2024
Última revisión	28 de mayo de 2024
Indicadores de compromiso	
URL del sitio falso	
https://msellagolan001.wixsite.com/validar	
Dirección IP sitio falso	
[34.117.60.144]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/fph24-00962/	

3. Vulnerabilidades

Check Point Remote Access VPN y otros - Vulnerabilidades	
Código de alerta	VSA24-01022
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de mayo de 2024
Última revisión	30 de mayo de 2024
CVE y puntaje CVSS y EPSS al momento de la publicación	
CVE-2024-24919 7.5 1.85%	
Fabricante	
Check Point	
Productos afectados	
Check Point Remote Access VPN R80.20.x, R80.20SP (EOL), R80.40 (EOL), R81, R81.10, R81.10.x y R81.20 Quantum Security Gateway R80.20.x, R80.20SP (EOL), R80.40 (EOL), R81, R81.10, R81.10.x y R81.20 CloudGuard Network Security R80.20.x, R80.20SP (EOL), R80.40 (EOL), R81, R81.10, R81.10.x y R81.20 Quantum Maestro R80.20.x, R80.20SP (EOL), R80.40 (EOL), R81, R81.10, R81.10.x y R81.20 Quantum Scalable Chassis R80.20.x, R80.20SP (EOL), R80.40 (EOL), R81, R81.10, R81.10.x y R81.20 Quantum Spark Gateways R80.20.x, R80.20SP (EOL), R80.40 (EOL), R81, R81.10, R81.10.x y R81.20	
Enlaces para revisar el informe:	
https://csirt.gob.cl/alertas/vsa24-01022/	

4. Recomendaciones y buenas prácticas

- No abrir correos ni mensajes de dudosa procedencia.
- Desconfiar de los enlaces y archivos en los mensajes o correo.
- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen por internet.
- Prestar atención en los detalles de los mensajes o redes sociales.
- Evaluar el bloqueo preventivo de los indicadores de compromisos.
- Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas.
- Revisar los controles de seguridad de los antispam y sandboxing.
- Realizar concientización permanente para los usuarios sobre este tipo de amenazas.
- Visualizar que los sitios web a los que se ingrese sean los oficiales.

5. Muro de la Fama

El siguiente es el listado de personas y organizaciones que han colaborado explícitamente con el CSIRT de Gobierno para mejorar la seguridad informática en instituciones y organismos del Estado, al informar campañas de phishing, malware y/o sitios fraudulentos.

El CSIRT de Gobierno destaca en este segmento a quienes reportaron incidentes utilizando canales formales (https://www.csirt.gob.cl o al teléfono 1510), siempre que hayan aportado información relevante, manteniendo la reserva del incidente durante el análisis y hasta la certificación de la solución de este.

- Jimmy Ávila
- María José Fuentes Urrutia
- Alejandro Cuzmar
- Natalia Valeska Hace Hernández
- Miguel Becerra
- Kevin Andrés Douglas Riquelme
- Monitoreo Universidad de Chile

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2024.05.31 17:02:26 -04'00'