Alerta de seguridad informática	2CMV21-00147-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de Febrero de 2020
Última revisión	12 de Febrero de 2020

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones, por lo cual se recomienda establecer una cuarentena preventiva respecto de los IoC mencionados, previa evaluación de impacto en servicios productivos; una vez que sus plataformas de monitoreo no detecten actividad maliciosa, se debe evaluar la posibilidad de liberar del bloqueo a los IoC consignados en el reporte respectivo, tales como servicios de hosting, de cloud o similares.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de malware supuestamente proveniente del Ministerio de Salud de Chile.

El atacante busca persuadir a las personas para descargar el archivo adjunto y ser ejecutado.

El mensaje del correo indica que se inició el registro de vacuna Covid-19 y se encuentra disponible para todas las fases mencionadas registrándose.

El atacante adjunta un vínculo para ser seleccionado y de esa forma descargar un archivo malicioso que al ser ejecutado gatilla la infección del equipo.

Observación

Solicitamos tener en consideración las señales de compromiso en su conjunto.

IoC Correo Electrónico

Datos del encabezado del correo

Servidores Smtp

dns3.sgpnet.com.br
hm1480-47.locaweb.com.br
hm1481-177-44.email.locaweb.com.br
hm1481-n-164.locaweb.com.br
hm1831-24.locaweb.com.br
hm1831-4.locaweb.com.br
host.netpix.com.br
host141-226.viabrs.com.br
host141-244.viabrs.com.br
ip4vps1.servhost.com.br
mail49183.hm1315.locaweb.com.br
mail49189.hm1315.locaweb.com.br
mail-alt3.h44.servidorhh.com
mail-vip42-bra.tpa.com.br
mcegress-30-lw-157.correio.biz
mx03out.mailserverpro.com.br
roma.midc.com.br
smtp010.hospedagemweb.com.br
smtp-12g.idc2.mandic.com.br
smtp-14.idc2.mandic.com.br
smtp-sp217-48.kinghost.net
smtp-sp217-52.kinghost.net
smtp-sp217-53.kinghost.net
smtp-sp217-65.kinghost.net
smtp-14g.idc2.mandic.com.br
smtp-14h.idc2.mandic.com.br
smtp-sp203-145.hospedagem.net
smtp-sp203-48.hospedagem.net
smtp-sp217-118.kinghost.net
smtp-sp217-121.kinghost.net
smtp-sp217-132.kinghost.net
smtp-sp217-14.kinghost.net
smtp-sp217-140.kinghost.net
smtp-sp217-142.kinghost.net
smtp-sp217-148.kinghost.net
smtp-sp217-153.kinghost.net
smtp-sp217-154.kinghost.net
smtp-sp217-171.kinghost.net
smtp-sp217-172.kinghost.net
smtp-sp217-180.kinghost.net
smtp-sp217-181.kinghost.net
smtp-sp217-182.kinghost.net
smtp-sp217-200.kinghost.net
smtp-sp217-23.kinghost.net
smtp-sp217-30.kinghost.net
smtp-sp217-47.kinghost.net
smtp-sp217-58.kinghost.net

Correos Electrónicos

3marcos@cmotanet.com.br
atendimento@caean.com.br
carina@enjoyviagens.tur.br
contato@adaf.esp.br
contato@chicone.com.br
contato@mancinidesign.com.br
contato@rgbviagens.com.br
contato@vilaaprendiz.com.br
contec@contecpr.com.br
coordenador@portalrealidade.com.br
cotacao@soberanabr.com.br
daniel.moraes@cheirinbao.com.br
davi@educandus.com.br
diego@xiruagricola.agr.br
suporte@akinternet.com.br
susele@piottomateriais.com.br
taubate.ctr@seesp.org.br
vendas@rabin.com.br
vendas@unitecparker.com.br
vendas5@mercadaochapaferro.com.br
sergio@inovareconsult.com.br
domingos@nordestao.com.br
edson@sady.com.br
estoque@srpneus.com.br
euricofreire@estudioeuricofreire.com.br
expedicao@vrpapeis.com.br
fabio.bastos@emilcardio.com.br
faleconosco@camacariagora.com.br
faturamento@casafaisca.com.br
financeiro@cetoi.com.br
hernan_24_69@hotmail.com
hirado@ahungara.org.br
imprensa@engenhodanoticia.com.br
irene@numeroumseguros.com.br
jose.silva@dautotintas.com.br
kellen@donalcides.com.br
luceni@coopershoes.com.br
magazine@capezio.com.br
marcelo.gomes@mgsistemas.com.br
prapatricia@ministeriopazeamor.com.br
rafael@oxxyracing.com.br

Asunto

Notificación - Registro de vacunación contra covid-19

IoC Archivo Adjunto

Archivos que se encontraban adjunto en el correo

Nombre : Registro_ID9937003405A4B88.zip
SHA256 : 675C846849A0A3B373A3C98FF5C2143F6AB87CEF1A0008C5D30383C5CDC3107E

Nombre : Registro_ID9937003405A4B88.msi
SHA256 : C9598E8F45BBD36F6CD8B24499BD96DF599BF499A77F4195C1FF3D7D3EAE8212

Nombre : C0214V5S7RSA00B8.zip
SHA256 : 0020DB7D3AC1F10CEAC645C12557F0A78472A7DCEE2D7980E911A4AE3350E1C4

Nombre : JCTHPNEBWK.dll
SHA256 : F695B8B7B0AB2FA84DF2903F70F7EFB397F1A03ED09DAF634521A8D5D9D52CE4

JDEDCU4PLA4ISGJB820RFSFO38M64TFEA0GXQ :
727283D668C8FF7E68AF43FC23AC8A20D4DC30917EC61158C6BFF75DE9FAFF5B

MSR11D7ZWJY3ZSJ3HAR9KSGJ7GF0N :
3CF21F31C5281600CA70D4C87F4F829F0011C6740084D26C3665D2729B092DA2

IoC Comunicación de Red

URL

https[:]//selfhelpwomendevelopment[.]com/wp-includes/images/webmail/registro[.]php

http[:]//www.aralimp.com[.]br/wp-includes/assets/download/Registro_ID9937003405A4B88[.]zip

https[:]//eventosespacofenix.com[.]br//wp-includes/Requests/Utility/C0214V5S7RSA00B8[.]zip

Imagen del mensaje

Gobierno de Chile

Ministerio de Salud actualiza lineamientos técnicos de vacunación contra el COVID-19.

Calendario de vacunación contra Covid-19.

Fase 1: personas de 60 a 74 años.

Fase 2: Personas con comorbilidades crónicas, trasplante y obesidad.

Fase 3: Profesionales de la educación, personas con discapacidad grave, socorristas, funcionarios del sistema penitenciario, trabajadores del transporte público, transportistas de carga por carretera, población privada de libertad.

Se inició el registro de la vacuna Covid-19.

EL SERVICIO ESTÁ DISPONIBLE PARA TODAS LAS ETAPAS DEL PLAN DE VACUNACIÓN COVID-19.

El Ministerio de Salud del gobierno está registrando a todas las personas contra el coronavirus.

Regístrese ahora para asegurar su vacunación.

Registro de vacunación

Recomendaciones

- 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 los sitios web que se ingresen sean los oficiales.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.02.12 17:08:07 -03'00'