13BCS-00025-001

CSIRT del Gobierno de Chile

Equipo de Respuesta ante Incidentes de Seguridad Informática

Publicado el Viernes 11 de Octubre de 2019

Resumen de noticias, reportes, alertas e indicadores de compromisos informados por CSIRT entre el miércoles 03 y el jueves 10 de Octubre.

Falsificación de Registro o Identidad

8FFR-00076-001 CSIRT ADVIERTE DE NUEVA WEB BANCARIA FRAUDULENTA

Alerta de seguridad informática	8FFR-00076-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de Octubre de 2019
Última revisión	02 de Octubre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulento asociado a una IP que suplanta el sitio web oficial de Banco Estado, el que podría servir para robar credenciales de usuarios de esa entidad. Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad bancaria aludida.

Enlace:

https://www.csirt.gob.cl/alertas/8ffr-00076-001/
https://www.csirt.gob.cl/media/2019/10/8FFR-00076-001.pdf

8FFR-00077-001 CSIRT ADVIERTE DE SITIO BANCARIO FRAUDULENTO QUE PODRÍA SERVIR PARA ROBO DE CREDENCIALES

Alerta de seguridad informática	8FFR-00077-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de Octubre de 2019
Última revisión	03 de Octubre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulento asociado a una IP que suplanta el sitio web oficial de Banco Scotiabank, el que podría servir para robar credenciales de usuarios de esa entidad. Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad bancaria aludida.

Enlace:

https://www.csirt.gob.cl/alertas/8ffr-00077-001/
https://www.csirt.gob.cl/media/2019/10/8FFR-00077-001.pdf

8FFR-00078-001 CSIRT COMPARTE INFORMACIÓN SOBRE PORTAL BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR-00068-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de Octubre de 2019
Última revisión	03 de Octubre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulento asociado a una IP que suplanta el sitio web oficial de Banco Estado, el que podría servir para robar credenciales de usuarios de esa entidad. Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad bancaria aludida.

Enlace:

https://www.csirt.gob.cl/alertas/8ffr-00078-001/
https://www.csirt.gob.cl/media/2019/10/8FFR-00078-001.pdf

8FFR-00079-001 CSIRT INFORMA SOBRE LA ACTIVACIÓN DE PORTAL BANCARIO FRAUDULENTO QUE PODRÍA SERVIR PARA EL ROBO DE INFORMACIÓN DE USUARIOS

Alerta de seguridad informática	8FFR-00079-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de Octubre de 2019
Última revisión	05 de Octubre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulento asociado a una IP que suplanta el sitio web oficial de Banco Estado, el que podría servir para robar credenciales de usuarios de esa entidad. Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad bancaria aludida.

Enlace:

https://www.csirt.gob.cl/alertas/8ffr-00079-001/
https://www.csirt.gob.cl/media/2019/10/8FFR-00079-001-1.pdf

8FFR-00080-001 CSIRT ADVIERTE DE LA ACTIVACIÓN DE WEB BANCARIA FRAUDULENTA

Alerta de seguridad informática	8FFR-00080-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de Octubre de 2019
Última revisión	05 de Octubre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulento asociado a una IP que suplanta el sitio web oficial de Banco Security, el que podría servir para robar credenciales de usuarios de esa entidad. Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad bancaria aludida.

Enlace:

https://www.csirt.gob.cl/alertas/8ffr-00080-001/
https://www.csirt.gob.cl/media/2019/10/8FFR-00080-001.pdf

8FFR-00081-001 CSIRT ADVIERTE DE SITIO BANCARIO FRAUDULENTO QUE PODRÍA SERVIR PARA EL ROBO DE CREDENCIALES DE CLIENTES

Alerta de seguridad informática	8FFR-00081-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de Octubre de 2019
Última revisión	07 de Octubre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulento asociado a una IP que suplanta el sitio web oficial de Banco Estado, el que podría servir para robar credenciales de usuarios de esa entidad. Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad bancaria aludida.

Enlace:

https://www.csirt.gob.cl/alertas/8ffr-00081-001/
https://www.csirt.gob.cl/media/2019/10/8FFR-00081-001.pdf

8FFR-00082-001 CSIRT ADVIERTE DE SITIO WEB QUE REDIRIGE A PÁGINAS BANCARIAS FRAUDULENTAS

Alerta de seguridad informática	8FFR-00082-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de Octubre de 2019
Última revisión	07 de Octubre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulento asociado a una IP que redirige a sitios que suplantan el sitio web oficial de Banco Chile, lo que podría servir para robar credenciales de usuarios de esa entidad. Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad bancaria aludida.

Enlace:

https://www.csirt.gob.cl/alertas/8ffr-00082-001/
https://www.csirt.gob.cl/media/2019/10/8FFR-00082-001.pdf

8FFR-00083-001 CSIRT ADVIERTE SOBRE LA ACTIVACIÓN DE SITIOS BANCARIOS CLONADOS PARA COMETER FRAUDES

Alerta de seguridad informática	8FFR-00083-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de Octubre de 2019
Última revisión	07 de Octubre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulento asociado a una IP que redirige a sitios que suplantan el sitio web oficial de Banco Estado, lo que podría servir para robar credenciales de usuarios de esa entidad. Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad bancaria aludida.

Enlace:

https://www.csirt.gob.cl/alertas/8ffr-00083-001/
https://www.csirt.gob.cl/media/2019/10/8FFR-00083-001.pdf

8FFR-00084-001 CSIRT ADVIERTE LA ACTIVACIÓN DE PORTAL BANCARIO FRAUDULENTO QUE PODRÍA SERVIR PARA EL ROBO DE CREDENCIALES

Alerta de seguridad informática	8FFR-00084-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de Octubre de 2019
Última revisión	07 de Octubre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulento asociado a una IP que suplanta el sitio web oficial de Banco Chile, el que podría servir para robar credenciales de usuarios de esa entidad. Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad bancaria aludida.

Enlace:

https://www.csirt.gob.cl/alertas/8ffr-00084-001/
https://www.csirt.gob.cl/media/2019/10/8FFR-00084-001.pdf

8FFR-00085-001 CSIRT ADVIERTE SOBRE SITIO WEB BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR-00085-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de Octubre de 2019
Última revisión	10 de Octubre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulento asociado a una IP que redirige a sitios que suplantan el sitio web oficial de Banco Scotiabank, lo que podría servir para robar credenciales de usuarios de esa entidad. Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad bancaria aludida.

Enlace:

https://www.csirt.gob.cl/alertas/8ffr-00085-001/
https://www.csirt.gob.cl/media/2019/10/8FFR-00085-001.pdf

Alertas de Phishing

8FPH-00065-001 CSIRT ADVIERTE DE PHISHING POR BLOQUEO TEMPORAL DE CUENTA

Alerta de seguridad informática	8FPH-00065-001
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de Octubre de 2019
Última revisión	06 de Octubre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de phishing a través de un correo electrónico cuyo mensaje intenta engañar a los usuarios del Banco Estado para cometer un fraude. El correo indica que, producto de una actualización de los servidores la cuenta del usuario no estaría registrada correctamente y, por lo tanto, el banco se habría visto obligado a bloquearla temporalmente. El mensaje insta a la víctima a registrar nuevamente la cuenta, acción que solo puede ser realizada a través de este correo electrónico a través del enlace adjunto. El enlace para, supuestamente, restaurar la cuenta, redirige a la víctima a un sitio fraudulento donde las víctimas se exponen al robo de sus credenciales bancarias.

Enlace

https://www.csirt.gob.cl/alertas/8fph-00065-001/
https://www.csirt.gob.cl/media/2019/10/8FPH-00065-001.pdf

8FPH-00066-001 CSIRT ADVIERTE DE PHISHING QUE SIMULA CRÉDITO DE CONSUMO

Alerta de seguridad informática	8FPH-00066-001
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de Octubre de 2019
Última revisión	06 de Octubre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de phishing a través de un correo electrónico cuyo mensaje intenta engañar a los usuarios del Banco Chile. El correo informa que puede realizar una simulación para un crédito de consumo para sus futuros proyectos, y dicha oferta tiene una vigencia 01 al 31 de octubre del 2019. Los estafadores disponibilizan un enlace, incitando a sus víctimas a ingresar al vínculo, exponiéndolos al robo de sus credenciales desde un sitio semejando al del Banco.

Enlace

https://www.csirt.gob.cl/alertas/8fph-00066-001/
https://www.csirt.gob.cl/media/2019/10/8FPH-00066-001.pdf

Vulnerabilidades

9VSA-00059-001 CSIRT COMPARTE ACTUALIZACIONES DE GOOGLE CHROMEOS

Alerta de seguridad informática	9VSA-00059-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Medio
TLP	Blanco
Fecha de lanzamiento original	03 de octubre de 2019
Última revisión	03 de octubre de 2019

Vulnerabilidad

CVE-2019-16508

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información obtenida del sitio web oficial del sistema operativo de Google, referente a una vulnerabilidad que afecta a ChromeOS y cómo mitigarla.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa-00059-001/
https://www.csirt.gob.cl/media/2019/10/9VSA-00059-001.pdf

9VSA-00060-001 CSIRT COMPARTE ACTUALIZACIONES DE WHATSAPP PARA ANDROID

Alerta de seguridad informática	9VSA-00060-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de octubre de 2019
Última revisión	03 de octubre de 2019

Vulnerabilidad

CVE-2019-11932

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información obtenida de diferentes fuentes, referente a una vulnerabilidad que afecta a Whatsapp y cómo mitigarla.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa-00060-001/
https://www.csirt.gob.cl/media/2019/10/9VSA-00060-001.pdf

9VSA-00061-001 CSIRT COMPARTE ACTUALIZACIONES PARA PRODUCTOS DE CISCO

Alerta de seguridad informática	9VSA-00061-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Medio
TLP	Blanco
Fecha de lanzamiento original	3 de octubre de 2019
Última revisión	3 de octubre de 2019

Vulnerabilidad

CVE-2019-12698	CVE-2019-12631	CVE-2019-12674
CVE-2019-12710	CVE-2019-12712	CVE-2019-12675
CVE-2019-12695	CVE-2019-12713	CVE-2019-12700
CVE-2019-12693	CVE-2019-12630	CVE-2019-12699
CVE-2019-12707	CVE-2019-15259	CVE-2019-12679
CVE-2019-12715	CVE-2019-15272	CVE-2019-12680
CVE-2019-12716	CVE-2019-12673	CVE-2019-12681
CVE-2019-12711	CVE-2019-15256	CVE-2019-12682
CVE-2019-12706	CVE-2019-12678	CVE-2019-12683
CVE-2019-12701	CVE-2019-12676	CVE-2019-12684
CVE-2019-12696	CVE-2019-12677	CVE-2019-12685
CVE-2019-12697	CVE-2019-1915	CVE-2019-12686
CVE-2019-12691	CVE-2019-12690	CVE-2019-12689
CVE-2019-12694	CVE-2019-12687	
CVE-2019-12714	CVE-2019-12688	

Resumen

Una vulnerabilidad en la interfaz de administración basada en web del software Cisco Firepower Management Center (FMC) podría permitir que un atacante remoto autenticado ejecute código arbitrario en el sistema operativo subyacente de un dispositivo afectado.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa-00061-001/
https://www.csirt.gob.cl/media/2019/10/9VSA-00061-001.pdf

9VSA-00062-001 CSIRT COMPARTE ACTUALIZACIONES EN APLICATIVO PUTTY

Alerta de seguridad informática	9VSA-00062-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Medio
TLP	Blanco
Fecha de lanzamiento original	08 de Octubre de 2019
Última revisión	08 de Octubre de 2019

Vulnerabilidad

CVE-2019-17067 CVE-2019-17068 CVE-2019-17069

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por diferentes fuentes referente a vulnerabilidades que afectan al aplicativo Putty.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa-00062-001-csirt/
https://www.csirt.gob.cl/media/2019/10/9VSA-00062-001.pdf

9VSA-00063-001 CSIRT COMPARTE ACTUALIZACIONES PARA EL LECTOR PDF FOXIT DE WINDOWS

Alerta de seguridad informática	9VSA-00062-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Medio
TLP	Blanco
Fecha de lanzamiento original	08 de Octubre de 2019
Última revisión	08 de Octubre de 2019

Vulnerabilidad

CVE-2019-5031 CVE-2019-13327 CVE-2019-13331
CVE-2019-13123 CVE-2019-13328 CVE-2019-13332
CVE-2019-13124 CVE-2019-13329 CVE-2019-17183
CVE-2019-13326 CVE-2019-13330

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por diferentes fuentes referente a vulnerabilidades que afectan al aplicativo Putty.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa-00063-001/
https://www.csirt.gob.cl/media/2019/10/9VSA-00063-001.pdf

9VSA-00064-001 CSIRT COMPARTE ACTUALIZACIONES PUBLICADAS POR MICROSOFT EN SU TRADICIONAL MARTES DE PARCHE

Alerta de seguridad informática	9VSA-00064-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de octubre de 2019
Última revisión	09 de octubre de 2019

Vulnerabilidad

CVE-2019-1070	CVE-2019-1060	CVE-2019-1311
CVE-2019-1329	CVE-2019-1322	CVE-2019-1338
CVE-2019-1345	CVE-2019-1356	CVE-2019-1368
CVE-2019-1230	CVE-2019-1166	CVE-2019-1315
CVE-2019-1330	CVE-2019-1323	CVE-2019-1339
CVE-2019-1358	CVE-2019-1357	CVE-2019-1371
CVE-2019-1313	CVE-2019-1238	CVE-2019-1316
CVE-2019-1331	CVE-2019-1325	CVE-2019-1340
CVE-2019-1359	CVE-2019-1362	CVE-2019-1372
CVE-2019-1314	CVE-2019-1239	CVE-2019-1317
CVE-2019-1334	CVE-2019-1326	CVE-2019-1341
CVE-2019-1361	CVE-2019-1364	CVE-2019-1375
CVE-2019-1327	CVE-2019-1255	CVE-2019-1318
CVE-2019-1337	CVE-2019-1333	CVE-2019-1342
CVE-2019-1363	CVE-2019-1365	CVE-2019-1376
CVE-2019-1328	CVE-2019-1307	CVE-2019-1319
CVE-2019-1344	CVE-2019-1335	CVE-2019-1343
CVE-2019-1369	CVE-2019-1366	CVE-2019-1378
CVE-2019-0608	CVE-2019-1308	CVE-2019-1320
CVE-2019-1321	CVE-2019-1336	CVE-2019-1346
CVE-2019-1347	CVE-2019-1367	

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Microsoft en su reporte mensual de actualizaciones correspondiente a octubre del 2019, parchando un total de 62 vulnerabilidades en sus software, de ellos 9 han sido clasificados como críticos, 49 como importante, dos como moderado y dos como bajo.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa-00064-001/
https://www.csirt.gob.cl/media/2019/10/9VSA-00060-001.pdf

9VSA-00065-001 CSIRT COMPARTE INFORMACIÓN SOBRE ACTUALIZACIONES PARA ANDROID

Alerta de seguridad informática	9VSA-00065-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Medio
TLP	Blanco
Fecha de lanzamiento original	10 de octubre de 2019
Última revisión	10 de octubre de 2019

Vulnerabilidad

CVE-2019-2110	CVE-2019-2268	CVE-2019-2336
CVE-2019-2114	CVE-2019-2271	CVE-2019-2339
CVE-2019-2173	CVE-2019-2289	CVE-2019-10490
CVE-2019-2184	CVE-2019-2295	CVE-2019-10513
CVE-2019-2185	CVE-2019-2303	CVE-2019-10535
CVE-2019-2186	CVE-2019-2315	CVE-2019-11902
CVE-2019-2187	CVE-2019-2318	CVE-2019-13916
CVE-2019-2215	CVE-2019-2329	CVE-2019-19824
CVE-2019-2251	CVE-2019-2335	

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Android en su boletín mensual de Octubre, parchando un total de 26 vulnerabilidades, 8 de las cuales han sido catalogadas como críticas y 16 de ellas como altas. Estas son de tipo ejecución de código remoto, escalación de privilegios, exposición de información, denegación de servicios, entre otras.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa-00065-001/
https://www.csirt.gob.cl/media/2019/10/9VSA-00065-001.pdf

Reportes

10CND-00019-001 INFORME SOBRE MENSAJES QUE SUPLANTAN AL ISL

Resumen Ejecutivo

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), fue alertado el día 25 de Septiembre del presente año sobre un una campaña de phishing a través de la aplicación de mensajería instantánea WhatsApp. El mensaje afirmaba, a la persona que lo recibía, sobre la existencia de un fondo (monto de dinero) disponible en el Instituto de Seguridad Laboral de Chile (ISL), invitándolo a seleccionar el enlace para verificar su nombre en la lista de los posibles beneficiados. Este informe proporciona detalle del método de infección y el comportamiento de la campaña. Además se comparten indicadores de compromisos y formas de prevenir ataques de ingeniería social que son utilizados por los atacantes. Si bien las técnicas descubiertas por CSIRT ya han sido documentadas anteriormente, el objetivo de este documento es llamar a los usuarios a tener precaución.

Enlace

https://www.csirt.gob.cl/reportes/10cnd-00019-001/
https://www.csirt.gob.cl/media/2019/10/10CND-00019-001.pdf

10CND-00022-001 INFORME SOBRE PHISHING QUE SIMULA ENVIAR CORREO DESDE LA PROPIA CUENTA DEL USUARIO

Resumen Ejecutivo

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, detectó una campaña de phishing cuyo objetivo era extorsionar a las personas que lo recibían. En este caso, el atacante hacía creer al usuario que tenía control del correo electrónico. Los usuarios podían leer que ellos eran los remitentes de la información, por lo que un usuario podía presumir que había sido vulnerada su cuenta. Este informe explica que, dependiendo de la configuración del Sender Policy Framework (SPF), un atacante podría suplantar el dominio del correo y, de esa forma, facilitar la recepción del correo de phishing al usuario final.

Enlace

https://www.csirt.gob.cl/reportes/10cnd-00022-001/
https://www.csirt.gob.cl/media/2019/10/10CND-00022-001.pdf

Indicadores de Compromisos

Se comparte a continuación el listado de indicadores de compromisos que fueron detectados durante la pasada semana por el Equipo del CSIRT intentando ejecutar escaneaos puertos, ataques de denegación de servicios o tratando de infectar con códigos maliciosos, entre otros ataques, para el conocimiento de la comunidad:

IoC	Motivo
186[.]148[.]209[.]58	Port scan
37[.]235[.]52[.]42	Port scan
185[.]205[.]210[.]48	Malware
172[.]253[.]2[.]3	Port scan
172[.]253[.]2[.]5	Port scan
172[.]253[.]2[.]4	Port scan
172[.]253[.]0[.]3	Port scan
172[.]253[.]1[.]5	Port scan
172[.]253[.]1[.]1	Port scan
164[.]68[.]117[.]5	Port scan
188[.]165[.]230[.]26	Port scan
185[.]187[.]198[.]10	Malware
118[.]174[.]139[.]50	Malware
159[.]203[.]197[.]27	Port scan
185[.]200[.]118[.]56	Port scan
120[.]52[.]152[.]17	Port scan
159[.]203[.]197[.]27	Port scan
67[.]198[.]196[.]34	Port scan
163[.]172[.]127[.]64	Port scan
158[.]69[.]58[.]44	Port scan

80[.]82[.]77[.]86	Port scan
88[.]198[.]139[.]4	Port scan
54[.]38[.]142[.]234	Port scan
190[.]158[.]19[.]141	Malware
80[.]240[.]141[.]141	Malware
181[.]123[.]0[.]125	Malware
104[.]236[.]185[.]25	Malware
159[.]203[.]193[.]252	Port scan
208[.]115[.]237[.]90	Port scan
83[.]97[.]20[.]188	Port scan
159[.]203[.]197[.]31	Port scan
54[.]38[.]142[.]226	Port scan
204[.]136[.]108[.]30	Port scan
88[.]198[.]139[.]3	Port scan
212[.]83[.]142[.]49	Port scan
146[.]112[.]133[.]19	Port scan
83[.]97[.]20[.]166	Port scan
146[.]112[.]133[.]64	Port scan
112[.]121[.]158[.]217	Port scan
158[.]69[.]242[.]232	Port scan
186[.]148[.]209[.]58	Port scan
38[.]102[.]150[.]27	Malware
193[.]112[.]242[.]156	Port scan
103[.]45[.]178[.]73	Port scan
103[.]42[.]183[.]71	Port scan
5[.]61[.]42[.]103	Malware
37[.]1[.]221[.]156	Malware
37[.]252[.]8[.]85	Malware
37[.]252[.]10[.]66	Malware
91[.]247[.]36[.]14	Malware
92[.]187[.]110[.]52	Malware
185[.]243[.]114[.]53	Malware
193[.]201[.]224[.]76	Port scan
37[.]49[.]230[.]31	Port scan
62[.]210[.]162[.]83	Port scan
77[.]247[.]108[.]226	Port scan
94[.]101[.]95[.]221	Malware
42[.]231[.]162[.]209	Malware
191[.]252[.]30[.]26	Malware
185[.]53[.]88[.]71	Port scan
185[.]53[.]88[.]61	Port scan
194[.]63[.]143[.]189	Port scan

51[.]89[.]17[.]205	Port scan
157[.]245[.]6[.]140	Port scan
193[.]29[.]15[.]246	Port scan
195[.]154[.]113[.]115	Port scan
92[.]118[.]37[.]97	Port scan
27[.]151[.]29[.]21	Port scan
185[.]175[.]93[.]103	Port scan
45[.]136[.]109[.]186	Port scan
45[.]136[.]109[.]185	Port scan
81[.]22[.]45[.]53	Port scan
185[.]176[.]27[.]166	Port scan
185[.]176[.]27[.]18	Port scan
92[.]118[.]37[.]99	Port scan
92[.]119[.]160[.]143	Port scan
167[.]86[.]120[.]21	Port scan
93[.]174[.]93[.]178	Malware
159[.]203[.]197[.]15	Port scan
51[.]15[.]161[.]176	Port scan
106[.]12[.]126[.]119	Port scan
119[.]29[.]153[.]245	Port scan
190[.]18[.]146[.]70	Malware
186[.]156[.]52[.]78	Malware
82[.]118[.]21[.]139	Malware
186[.]10[.]243[.]70	Malware
42[.]231[.]162[.]198	Port scan
190[.]85[.]152[.]186	Malware
78[.]189[.]76[.]2	Malware
89[.]32[.]150[.]160	Malware
201[.]183[.]247[.]58	Malware
68[.]169[.]49[.]14	Malware
69[.]162[.]169[.]173	Malware
186[.]1[.]41[.]111	Malware
206[.]212[.]248[.]178	Malware
78[.]189[.]76[.]2	Malware
119[.]159[.]150[.]176	Malware
109[.]104[.]79[.]48	Malware
103[.]31[.]232[.]93	Malware
42[.]231[.]162[.]203	Port scan
42[.]231[.]162[.]197	Port scan
47[.]89[.]234[.]36	Malware
182[.]61[.]189[.]87	Malware
185[.]53[.]88[.]67	Port scan

188[.]212[.]101[.]121	Port scan
91[.]205[.]215[.]57	Malware

URL	Motivo
http[:]//www[.]adoulaspromise[.]com/www/Bancoestado/	Phishing
https[:]//bancoestado[.]cc	Phishing
https[:]//www[.]scotiabankchile[.]net/choose[.]php	Phishing
hxxp[:]//37[.]1[.]223[.]178/qmuw3fwdfw/tell2[.]dat	Malware
hxxp[:]//1065695240[.]rsc[.]cdn77[.]org/aefgwehh/05sall[.]dat	Malware
hxxp[:]//1118069275[.]rsc[.]cdn77[.]org/aefgwehh/05sall[.]dat	Malware
hxxp[:]//bo0uiomeglecaptures[.]net	Malware
hxxp[:]//uoibppop[.]tk	Malware
www[.]robertjkenner[.]com/tmp_files/Activacion[.]php	Phishing
http[:]//nanara[.]jp/modules/www[.]bancoestado[.]cl/imagenes/comun2008/banca-en-linea-personas[.]html	Phishing
http[:]//bancooestado[.]xyz/imagenes/comun2009/en-linea-personas[.]php	Phishing
http[:]//topcopytrader[.]000webhostapp[.]com	Phishing
http[:]//nasal-invoices[.]000webhostapp[.]com	Phishing
http[:]//chile4464[.]000webhostapp[.]com	Phishing
https[:]//marketingdigital101[.]com[.]br/Bancoestado/	Phishing
https[:]//www[.]webportal[.]live/consulting/bancochile//wcm/connect/Personas/Portal/2w7ddyl4ar/u1ax4_persona/login_ju3o/index/loginkd0j/	Phishing
https[:]//www[.]bancooestadoocl[.]xyz/imagenes/comun2009/en-linea-personas[.]php	Phishing
http[:]//ftp[.]apricotprint[.]co[.]uk/	Malware
http[:]//www[.]bancoestado[.]cl[.]banca-en-linea-personas[.]cl[.]pedidocentral[.]cl/profesional/imagenes/comun2008/banca-en-linea-personas[.]html	Phishing

Recomendaciones

- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java, entre otras)
- 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

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 públicos del Estado, al informar problemas de seguridad y vulnerabilidades descubiertas.
El CSIRT de gobierno destaca en este segmento a quienes reportaron incidentes utilizando canales formales (en el sitio web https://www.csirt.gob.cl y/o al teléfono +(562) 2486 3850) siempre que hayan aportado con información relevante, manteniendo la reserva del incidente durante el análisis y hasta la certificación de la solución del mismo.

- Pablo Olivares
- Alejandro Farías
- Juan López

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.10.11 20:33:48 -03'00'