CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 5 | N.º 220

semana del 15 al 21 de septiembre de 2023

LA SEMANA EN CIFRAS

IP INFORMADAS

2

IP advertidas en múltiples campañas de phishing y de fraude.

URL ADVERTIDAS

5

URL asociadas a sitios fraudulentos y campañas de phishing y malware

PARCHES COMPARTIDOS

13

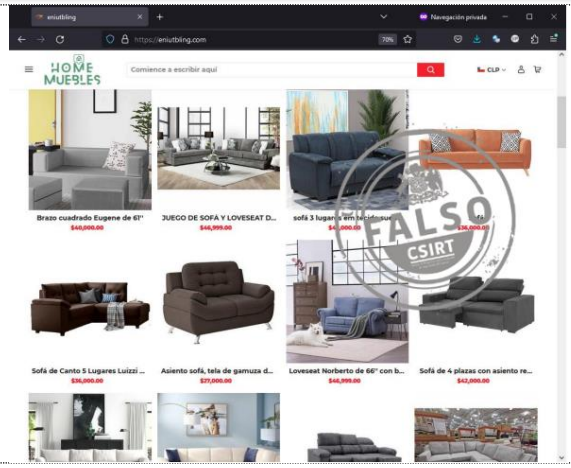
Las mitigaciones son útiles en productos de Atlassian, GitLab, Fortinet, Nagios y Trend Micro.

CONTENIDO

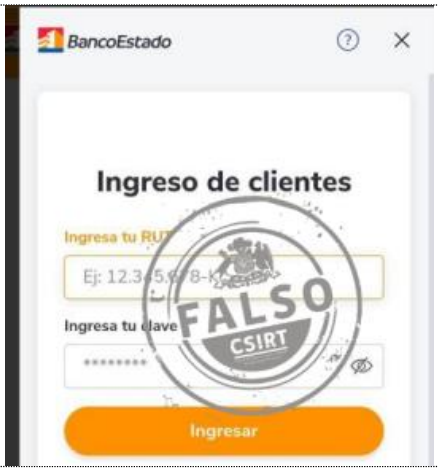
1. Sitios fraudulentos 3
2. Phishing 4
3. Vulnerabilidades 5
4. Noticias y concientización 8
5. Recomendaciones y buenas prácticas 10
6. Muro de la Fama 11

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

1. Sitios fraudulentos



CSIRT alerta de nuevo sitio fraudulento que simula ser web de venta de muebles	
Alerta de seguridad cibernética	8FFR23-01531-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 septiembre, 2023
Última revisión	20 septiembre, 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//eniutbling.com/	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01531-01/	



CSIRT alerta de nuevo sitio fraudulento que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FFR23-01532-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 septiembre, 2023
Última revisión	21 septiembre, 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//cl.bonoife-cliente[.]com/	
IP del sitio falso	
[104.21.14.218]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01532-01/	

2. Phishing

CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH23-00892-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 septiembre, 2023
Última revisión	20 septiembre, 2023
Indicadores de compromiso	
URL redirección	
http[:]//prevemed[.]com.ar/1695241888/imagenes/_personas/home/default.asp	
URL sitio falso	
https[:]//promezclas.com/activacion/cuenta-wckh/	
Dirección IP sitio falso	
[107.180.26.179]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00892-01/	

3. Vulnerabilidades

CSIRT informa de parche para nueva vulnerabilidad crítica en GitLab	
Alerta de seguridad cibernética	9VSA23-00901-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 septiembre, 2023
Última revisión	20 septiembre, 2023
CVE	
CVE-2023-5009	
Fabricante	
GitLab	
Productos afectados	
GitLab Enterprise Edition (EE) versiones anteriores a la 16.2.7 GitLab Community Edition (CE) versiones anteriores a la 16.3.4	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00901-01/	

CSIRT informa de parche a vulnerabilidad en Trend Micro Apex One y WFBS	
Alerta de seguridad cibernética	9VSA23-00902-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 septiembre, 2023
Última revisión	20 septiembre, 2023
CVE	
CVE-2023-41179	
Fabricante	
Trend Micro	
Productos afectados	
Apex One Apex One as a Service Worry-Free Business Security (WFBS) Worry-Free Business Security Services (WFBSS)	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00902-01/	

CSIRT informa de vulnerabilidades parchadas en FortiWeb, FortiProxy y FortiOS de Fortinet	
Alerta de seguridad cibernética	9VSA23-00903-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 septiembre, 2023
Última revisión	20 septiembre, 2023
CVE	
CVE-2023-29183 CVE-2023-34984	
Fabricante	
Fortinet	
Productos afectados	
FortiWeb 6.3.6 a 7.2.1. FortiProxy 7.0.0 a 7.2.4. FortiOS 6.2.0 a 7.2.4.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00903-01/	

CSIRT informa de vulnerabilidades críticas que afectan a Nagios XI y para las cuales existen parches disponibles	
Alerta de seguridad cibernética	9VSA23-00904-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 septiembre, 2023
Última revisión	21 septiembre, 2023
CVE	
CVE-2023-40931 CVE-2023-40932 CVE-2023-40933 CVE-2023-40934	
Fabricante	
Nagios	
Productos afectados	
Nagios XI 5.11.1 y anteriores	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00904-01/	

CSIRT informa de nuevas vulnerabilidades de riesgo alto en Jira, Confluence, Bitbucket y Bamboo de Atlassian	
Alerta de seguridad cibernética	9VSA23-00905-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 septiembre, 2023
Última revisión	21 septiembre, 2023
CVE	
CVE-2023-22513 CVE-2023-22512 CVE-2023-28709 CVE-2023-24998 CVE-2023-25647	
Fabricante	
Atlassian	
Productos afectados	
Bitbucket 8.0.0 a 8.14.0. Confluence Data Center y Server de 5.6 hasta e incluyendo 8.5.0.. Bamboo de 8.1.12 a 9.2.4. Jira desde 4.20.0, parchado en 4.20.25, 5.4.9, 5.9.2, 5.10.1 y 5.11.0.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00905-01/	

4. Noticias y concientización

Empresa del Estado frustra «fraude del CEO»: aquí les contamos cómo lo hicieron

Esta nota también fue publicada en: https://www.csirt.gob.cl/noticias/empresa-del-estado-frustra-bec/

Recientemente, una empresa pública logró detectar a tiempo un ejemplo de un tipo estafa virtual que ha ganado prominencia y logrado sustraer cuantiosos montos a compañías de todo tipo alrededor del mundo. Se trata del denominado fraude del CEO, o Business Email Compromise (BEC), un ataque de ingeniería social en el que, a grandes rasgos, delincuentes se hacen pasar por altos ejecutivos de una compañía (como puede ser el gerente general, CEO en inglés) para lograr que sus empleados, o los de una empresa cliente o proveedora, realicen acciones perjudiciales (transferencia de fondos no autorizados, la divulgación de información confidencial o la realización de acciones que benefician al atacante), lo que puede resultar en pérdidas financieras significativas y daños a la reputación de las organizaciones afectadas.

En este caso, fue un jefe de departamento de la que llamaremos Empresa A, quien recibió un mensaje de WhatsApp de alguien que se hacía pasar por el exgerente general de otra firma pública (que llamaremos Empresa B), usando para ello una imagen del ejecutivo obtenida de sus redes sociales. Se aprovechó de que el jefe de departamento es un exfuncionario de la Empresa B, lo que aumentó su confianza y ayudó a que no sospechara de ser contactado por esta persona.

El falso ejecutivo le pidió al jefe de departamento la dirección de email de algún contacto en la Empresa A que pudiera dar curso a una supuesta negociación financiera entre ambas compañías. La persona que recibió el WhatsApp no sospechó, y le entregó la dirección de email de la una persona que trabaja con un alto ejecutivo de la Empresa A, y que cumple un rol muy relevante en el flujo de aprobaciones de la compañía.

Contando con su dirección de correo, los malhechores enviaron un email argumentando que necesitaban cerrar con urgencia un negocio de alto nivel, solo conocido por las más altas esferas de ambas compañías, indicando también el monto de la transacción necesaria. Incluso mencionan en el email a un abogado de una prestigiosa firma, con la intención de darle mayor credibilidad al mensaje.

LA DETECCIÓN

Es en este punto en el que comienzan las sospechas que permitirían a Empresa A detectar el esquema delictual. Una persona responsable de la secretaría general, que recibe el email, nota que la dirección del remitente que se muestra en el correo termina en @empresaA, debiendo realmente provenir de una dirección @empresaB. Además, el texto del correo se refiere al abogado con el honorífico de “doctor”, algo que no es costumbre hacer en Chile.

El texto estaba planteado además en términos de urgencia por cerrar el convenio, e insistía en mantener la conversación de forma confidencial, ambas características de este tipo de ataques.

Estos indicios hicieron a la persona receptora del mensaje sospechar y contactar al Subgerente de TI de Empresa A, quien derivó el tema al Oficial de Seguridad de la firma.

Tras revisar el correo electrónico, el oficial de Seguridad instruyó al personal de Empresa A a cancelar toda comunicación o contacto con los actores maliciosos.

Finalmente, el Oficial de Seguridad informó de lo sucedido al Comité de Seguridad de Empresa A, incluyendo el potencial alcance del ataque frustrado y los mecanismos que fueron utilizados.

Empresa A determinó, como pasos a seguir, el gestionar una nueva sesión de concienciación de la primera línea ejecutiva sobre los ataques de tipo BEC, y coordinar una sesión con los directores de la compañía, para formalizar el proceso de concientización, y tomó contacto con el CSIRT de Gobierno

CONCLUSIONES

- Es crucial que todos los miembros de la organización tengan conciencia de los riesgos de este y otros tipos de estafa, y que sepan a qué detalles estar pendientes para detectarlas.

- En este caso, fue determinante que la persona de la secretaría general notara la dirección electrónica del remitente, y leyera con detención el mensaje, notando errores de redacción sutiles, pero determinantes.

- Se debe reforzar entre los trabajadores que, tal como en el caso planteado, ante alguna duda o sospecha en un correo electrónico se debe avisar cuanto antes a los encargados de seguridad de la información en la compañía.

- El Oficial de Seguridad de la empresa también actuó correcta y decisivamente, al llamar a cortar comunicación con los delincuentes al observar las inconsistencias denunciadas por la persona que recibió el email.

- Es necesario que transacciones de alta relevancia, como la realización de pagos a otras compañías, siga siempre los procedimientos regulares establecidos por la organización. Por ejemplo, en el caso de Empresa A, que exige la autorización por parte de distintos ejecutivos de la compañía para aprobar un pago de los montos requeridos por los delincuentes, un esquema como el planteado en este BEC, con casi total certeza no hubiera podido prosperar, incluso de no ser detectado cuando lo fue.

- Dado lo anterior, se debe concienciar a los trabajadores de nunca saltarse los procedimientos regulares, por mucha urgencia o secreto que exija un mensaje que reciban, o que este diga provenir de sus superiores jerárquicos o incluso del gerente general de la empresa.

Siempre que exista un incidente que haya presentado afectación o revista de características especialmente peligrosas se debe notificar al CSIRT de Gobierno. Guía sobre el BEC y cómo protegernos: https://www.csirt.gob.cl/recomendaciones/bec-2023/

5. 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.

6. 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.

- Alonso Ignacio Villalobos González
- Óscar San Martín
- Cristián Herrera Jara
- Nicolás Contador
- Krysthel Unda

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.09.22 17:01:03 -03'00'