Alerta de seguridad informática	2CMV23-00399-01
Clase de alerta	Fraude
Tipo de incidente	Phishing-Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de febrero de 2023
Última revisión	06 de febrero de 2023

NOTA SOBRE EL CORRECTO USO Y DIVULGACIÓN DE ESTE DOCUMENTO

La información contenida en este informe fue procesada por el CSIRT de Gobierno analizando múltiples fuentes. La información puede ser modificada o actualizada a partir de nuevos antecedentes y análisis.

Las personas y organizaciones víctimas de suplantación, en los casos que corresponda, no tienen responsabilidad sobre esa acción ejecutada por el atacante. El uso de la imagen de los suplantados en este informe tiene el específico propósito de evitar que terceras partes sean afectadas por atacantes.

Las alertas de seguridad cibernéticas del CSIRT de Gobierno contienen información sobre incidentes y acciones maliciosas que podrían impactar en las organizaciones. Los receptores de esta información tienen la responsabilidad de evaluar la eventual aplicación de cuarentenas preventivas sobre los indicadores de compromiso (IoC) que se comparten en este documento, teniendo presente los impactos que pueda tener en la entrega de sus servicios o en la continuidad operativa de sus negocios. Una vez que sus plataformas de monitoreo no detecten actividad maliciosa sobre los IoC compartidos, se debe evaluar la posibilidad de levantar el bloqueo.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT de Gobierno) ha identificado una nueva campaña de phishing con malware suplantando a la Superintendencia de Pensiones.

De hacer clic en el enlace incluido en el email se llega a una web preparada por los ciberdelincuentes, la cual descarga un archivo tipo rar con otro fichero en su interior, de extensión cmd. Este último inyecta código malicioso.

El código malicioso en cuestión se conoce como Mispadu, parte de una familia de malware bancarios que amenaza la información de los titulares de las cuentas bancarias. Además, tiene capacidades de actualización a través de un archivo Visual Basic Script (VBS), que se descarga y ejecuta automáticamente. Durante el proceso de infección, el malware recopila los siguientes datos de la computadora de la víctima: Versión del sistema operativo, Nombre de la computadora, Idioma del dispositivo, Antivirus instalado.

Advertencia sobre gestión de IoC

Los patrones expresados en forma de hash de un archivo pueden ser administrados con herramientas centralizadas y distribuidas, como firewall y antimalware. Las organizaciones deben tomar resguardo de incorporar un hash que pudiere estar vinculado a un archivo o DLL válida dentro de un sistema.

Al gestionar patrones potencialmente maliciosos con nombres de host o IP, se debe considerar que la relación entre nombre FQDN e IP puede cambiar en el tiempo, y que una dirección IP específica puede estar siendo usada por un proveedor de web hosting que puede tener más de un dominio asociado a dicha IP.

En consecuencia, se recomienda tener un orden de prioridades a la hora de ejecutar un bloqueo, considerando al menos:

- El uso de un dispositivo WAF que pueda discriminar el nombre FQDN potencialmente malicioso por sobre la IP.
- El uso de un firewall que permita integrar listas de bloqueo FQDN sin necesitar conversión a IP.
- El uso de sistemas proxy que permitan bloquear el FQDN sin necesitar la conversión a IP.
- En última instancia, incorporar el bloqueo de la IP verificando que no corresponda a un esquema de web hosting, porque existe la posibilidad de bloquear los restantes dominios implementados que utilizan la misma dirección IP.

IoC Correo Electrónico

Antes de aplicar bloqueos, tenga presente lo indicado en el punto sobre advertencia de gestión de IoC.

Datos del encabezado del correo

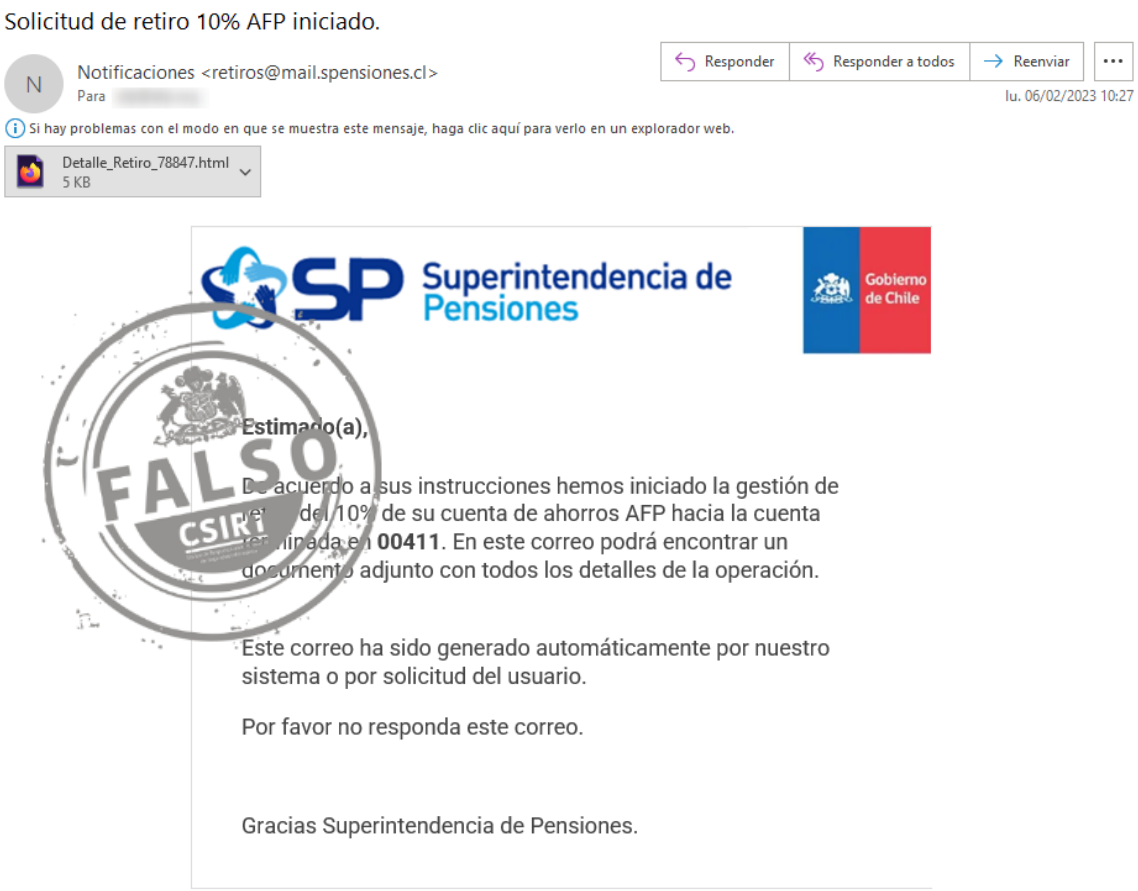
Asunto	Correo de Salida	SMTP
Solicitud de retiro 10% AFP iniciado.	retiros@mail.spensiones.cl	[116.74.186.200]

Indicadores de Compromiso Asociados

Archivos que se encuentran en la amenaza

Tipo	Indicador	Relación
SHA256	082d50bdaa7400e1e9c1e4c38e7c854ee28f03ec7fe8b9db36e0b60fd0bb06ee	Detalle_Retiro_257999.rar
SHA256	8f9bff6c9819040a6ebe473017a84640bd365c219559c0e416162f2b33ee9bef	Detalle_Retiro_875427.cmd
SHA256	ee70262f3d132d4b7b0475f1e8f865ae0eae4c5c45f79e7db9d33ab01fb90278	StartupProfileData-NonInteractive
SHA256	b3ce811fb696b94f9117ee7fe725ae6b907d695636beceeb1672d5d5eeb81df4	sqlite3.dll
SHA256	09c938d64248a8ddd18b5e1cea2c7376a3f5caa967bc760050ce84617c0587c2	~~
SHA256	6af0c5267d221d7972611ded914ede25d188d046278aceb94d9ada0ff87de153	~~
SHA256	de1c86d0d942570fbd63ac3dcd2e397cf0df0a677abc01588a6e9a2591e07ad6	DriverAudio.lnk
SHA256	d6fbabfea8eeecd4436d5de5113e057215f7f31e1725aedc1fb125e086d63e2d	Detalle_Retiro_875427.a3x
SHA256	98e4f904f7de1644e519d09371b8afcbbf40ff3bd56d76ce4df48479a4ab884b	blalock.exe
URL	https://www.sxconstructions.com[.]au/wp-content/img2/do/it.php?b1&v1=1033&v2=1033&v3=&v4=Windows%2010&v5=Admin&v6=X64&v7=	Malware Config
URL	https://www.sxconstructions.com[.]au/wp-content/img2/do/it.php?f=2&w=Windows%2010	Malware Config
URL	https://www.autoitscript[.]com/autoit3/pkgmgr/sqlite/sqlite3.dll	Malware Config
URL	http://portaconexao8.top/rest/?h=C3749E07	Malware Config

Imagen del mensaje



Solicitud de retiro 10% AFP iniciado.

N Notificaciones <retiros@mail.spensiones.cl>
Para [redacted]

Responder | Responder a todos | Reenviar | ...

lu. 06/02/2023 10:27

Si hay problemas con el modo en que se muestra este mensaje, haga clic aquí para verlo en un explorador web.

Detalle_Retiro_78847.html
5 KB

Superintendencia de Pensiones

Gobierno de Chile

FALSO
CSIRT

Estimado(a),

De acuerdo a sus instrucciones hemos iniciado la gestión de retiro del 10% de su cuenta de ahorros AFP hacia la cuenta terminada en **00411**. En este correo podrá encontrar un documento adjunto con todos los detalles de la operación.

Este correo ha sido generado automáticamente por nuestro sistema o por solicitud del usuario.

Por favor no responda este correo.

Gracias Superintendencia de Pensiones.

Recomendaciones

- Los usuarios deberían procurar:
  - No abrir correos ni mensajes de dudosa procedencia, pues pueden re direccionarlos a sitios web fraudulentos.
  - Desconfiar de los enlaces y archivos en los mensajes o correo.
  - Solicitar que sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras) estén actualizadas.
  - Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen por internet.
  - Prestar atención en los detalles de los mensajes o redes sociales.
  - Solicitar que todas las plataformas de tecnologías y de detección de amenazas estén actualizadas.
  - Siempre intentar verificar que los sitios web que se visitan sean los oficiales.
  - Notificar oportunamente a sus encargados de ciberseguridad para que investiguen el incidente, comprueben si ha llegado a otros usuarios y apliquen las mitigaciones pertinentes. Algunas señales que debieran gatillar un informe inmediato:
    - Accedí a un sitio web y luego de entregar mis credenciales no permite acceder al sitio y sus servicios.
    - Realicé una transacción (compra de producto, reporte en una institución del estado, acceso a un servicio, entre otras posibilidades) en un sitio o sistema web que parece oficial, pero no lo es.
    - He identificado un sitio o sistema web que a mi entender es fraudulento.
- Los administradores deben:
  - Implementar controles anti spoofing (DKIM, SPF y DMARC).
  - Revisar la información que se expone de sus usuarios en sus sitios y sistemas web.
  - Filtrar o bloquear los correos entrantes que sean clasificados como phishing.
  - Evaluar el bloqueo preventivo de los indicadores de compromisos.
  - Revisar los controles de seguridad de los antispam y sandboxing.
  - Instruir a sus usuarios sobre el phishing y ayudarlos a reconocerlos. Realizar concientización permanente para los usuarios sobre este tipo de amenazas.
  - Crear mecanismos amistosos para el reporte y el feedback, en un entorno donde no se busque la culpabilidad, sino que la solución.
  - Implementar y promover el uso de segundo factor de autenticación (2FA).
  - Proteger a sus usuarios de sitios maliciosos usando proxy servers y manteniendo actualizados sus browsers.
  - Proteger sus dispositivos del malware.
  - Activar la protección de filtro de sitios web en sus sistemas de seguridad, en particular aquellas categorías de sitios maliciosos o fraudulentos.
  - Tener un protocolo de respuesta rápido ante estos incidentes.
  - Detectar rápidamente estos incidentes instando a los usuarios a que reporten rápidamente cualquier actividad sospechosa.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.02.06 11:25:25 -03'00'