Alerta de seguridad informática	2CMV23-00397-01
Clase de alerta	Fraude
Tipo de incidente	Phishing-Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de enero de 2023
Última revisión	19 de enero 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 Servipag.

Por medio de correo masivo, que menciona la existencia de un falso pago de un total de $79.030 a la cuenta de la víctima. En el email, el ciberdelincuente deja una URL para la descarga de un archivo .zip con un archivo msi en su interior.

Si este fichero es ejecutado se carga Mekotio, un malware bancario que se dirige específicamente a la información bancaria. Este troyano representa una amenaza significativa para las finanzas y la privacidad de las víctimas.

Por lo general, los troyanos bancarios se dirigen a las credenciales de cuentas bancarias online, como ID, inicios de sesión, contraseñas, etc. Por lo tanto, los datos sustraídos son a menudo utilizados para realizar transacciones fraudulentas, compras online y se venden a terceros.

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
☑ Fw: Comprobante de Pagos. - (4797762)	angel4.me@angel4.me	[46.231.200.155]

Indicadores de Compromiso Asociados

Archivos que se encuentran en la amenaza

Tipo	Indicador	Relación
SHA256	6e6d0b550377356b6fa234f06a7f8348f48abec68b14396c713fd0aecb9cc075	8000217HJX5SD71253A2.zip
SHA256	d27fc5641cadee2fe89f1a23264ae10879cde5702397a4bb3c6ace6e583bc4b7	8000217HJX5SD71253A2.msi
URL	http://ec2-15-228-254-149.sa-east-1.compute.amazonaws[.]com/0001254877FBCVTE52115DUR5/?/=test@csirt.gob.clhttps://outlook.live.com/mail/0/inbox	Malware Config

Imagen del mensaje

✓✓ Fw: Comprobante de Pagos. - (4797762)

S SERVPAG <No-Responder-ServPag15050287@mc19o2702.dnl
Para [redacted]

Responder | Responder a todos | Reenviar | ...

ju. 19/01/2023 5:17

SERVIPAG

Estimado(A) [redacted]

(Portal ServPag) Junto con saludar y agradecer su preferencia, a justamos comprobante de pago de la cuenta pagada a través de Servipag.

Transaccion realizada en 18/01/2023 hemos procedido a realizar una transacción en su banco que alcanza un total de $ 79.000 por concepto de la segyuinte cuenta

.

Descargar Comprobante detallado

FALSO
CSIRT

Para mayor informacion, comuniquese con nosotros al 600 4822 444 de lunes a viemes de 08:30 a 19:30

horas

Si ya realizo el pago, no considere el presente mensaje.

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: 2023.01.20 10:15:26 -03'00'