Alerta de seguridad informática	2CMV23-00401-01
Clase de alerta	Fraude
Tipo de incidente	Phishing-Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de febrero de 2023
Última revisión	24 de febrero de 2023

NOTA SOBRE EL CORRECTO USO Y DIVULGACIÓN DE ESTE DOCUMENTO

La información contenida en este informe fue procesada por CSIRT 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 de CSIRT 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 Fiscalía General de la República.

El falso correo se trata de un "último aviso prejudicial" en el que se le indica a la víctima que existe un pago de obligaciones, por lo que tiene dos días hábiles para realizar este supuesto pago y así evitar acciones judiciales. Para revisar la resolución, el atacante adjunta una URL, al ingresar, se descarga un malware.

Al analizar el malware, las tácticas, técnicas y procedimientos asociados a la muestra, el CSIRT de Gobierno descubrió la presencia de 7 tácticas y 10 técnicas. Entre ellas, destacamos: el **acceso inicial** (mediante phishing), **ejecución** (el usuario ejecuta un fichero malicioso), **persistencia** (carga de programa en llave de registro GoogleLLCcDriversgStudio.exe), **elevación de privilegios** (bypass del control de cuentas de usuarios de windows), **acceso a credenciales** (capturas de credenciales a través de programa PDF_Arc_hivo_DocumtPNQNSEOJRQRJFPAfudvg.exe), **descubrimiento** (enumeración de la configuración de red del sistema, descubrimiento de llaves de registro, enumeración de información del sistema y enumeración de datos personales) y **comando y control** (utilización de canales de comunicación alternativos o de puertos no comunes).

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's, 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 la 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
Mensaje importante! ID: (205969)	root@vghj27.adslmails.com	[185.202.93.17]

Indicadores de Compromiso Asociados

Archivos que se encuentran en la amenaza

Tipo	Indicador	Relación
SHA256	8c2e2fede8c77f25b1555daf88461e0346c76218cba0ed6ada937c303e5cd8e8	PDF_Archivo_Adju_ntoBXPJFVTSGKLFPMPlmiumFHVCN.zip
SHA256	68f74d929f9a07e87fa3927a1f762d9ce8611532345c2bc4c6e443dbfcbe24e8	PDF_Arc_hivo_DocumtPNQNSEOJRQRJFPAfudvg.exe
SHA256	be9f858306daf9c886fbe579db2f788a21a5531c7d0028b6d663fac43ffaeb0c	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~VEUOSUZAUY.xml
SHA256	447670a3d9e3843a7d1758eb77842c8b5a9cd817ee1bc335c5adce43df64fa8b	sShYZOGGX.xml
URL	ia.from-ia[.]com	Malware Config
URL	http://107.20.86[.]83:9479/A5AAC6203DBB22B136BC48C749D864E61E2C32CF60E462ED3CD76AFD08060E3127213926F66CFA0F68B192ABB5BC422B342707DD4AE61EC266968E42352F12DD5FFB0E1068EA0B6CDF160F313EC2B972D356C8126CCBB06DDF4826F27FC380D472C39FA4BD81DD4E0B263B2A5E93E5544D4FB0E656DE4C342D1C1779E856DF59C4BDA780E72D170CCBA5	Malware Config
URL	http://107.20.86[.]83:9479/BBBC39B2AFCD105F97DC72ED6D8690A7B04BE27CB748DD67FA66F772F9046FBEBC4BDF4F9F8493AFA5A0839FA99559C06D81B87AAB9842241179B9ABA6A8BE938291F05096829FBD4224EC4B3F20CBBCA29E55D556D7137CEA44253008460B38015FCD89A7B588A398A6432C6E9299F91E7D9CF569CAA8938F8AE254CCB6A4874D3BD41CC6659E49D472E01F2AD911C979AE4726EA5AEA1CC66A99AEACA0A049D80221D575A844E877A64AE71EC6AC5183BD	Malware Config
URL	http://107.20.86[.]83:32621/sShYZOGGX.xml	Malware Config
URL	http://144.217.0[.]33/1498144785074000085.php?MD=0&OUT=SIM&PG=0&SO=7&AV=SEM%20AV.&US=admin&PC=USER-PC&PST=GoogleLLCtDriving&EXE=GoogleLLCcDriversgStudio.exe&ST=INFECTADO&DTF=24/02/2023%2013:07:05	Malware Config
IP	107.20.86[.]83	C2
IP	5.181.159[.]22	C2

Imagen del mensaje

Mensaje importante! ID: (205969)

UA ULTIMO AVISO PRE-JUDICIAL <info@gcagroup.com.ar>
Para [redacted]

Responder | Responder a todos | Reenviar | ...
vi. 24/02/2023 9:18

ADMINISTRACIÓN FEDERAL DE INGRESOS PÚBLICOS

Cancelacion obligaciones fiscales reclamadas en juicio de ejecucion fiscal com sumas embargadas.
Reforma Fiscal. Ley 27.430 Condiciones y procedimiento

EVITE INCONVENIENTES en su DOMICILIO

Usted cuenta con un plazo de 2 días háblies para cancelar su obligación. Vencido el plazo concedito sin que se hubiera efecttuado el pago, nuestro mandante se reserva los derechos para iniciar posiblems acciones judiciales tendentes a obtener el pago de su acreencia, ló que le acasionará mayores gastos

Con el fin de ofrecerle una solución y detender este processo, el estudio le informa que cuenta con facilidade para efectuar el pago y cancelar su deuda.

Resolución de Archivo General

Esta e su ultima oportunidade para solucionar la mima en una etapa extrajudicial y de esta forma evitar afrontar un proceso judicial con las consecuencias mencionadas anteriormente.

Recomendaciones

- Los usuarios deberían procurar:
  - No abrir correos ni mensajes de dudosa procedencia.
  - 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.
  - No descargar software que no cuente con la autorización del equipo de informática (cracks, antivirus, utilitarios, juegos, aplicaciones de oficina, etc.).
  - 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:
    - Mi equipo presenta alto consumo de CPU y de memoria.
    - Accedí a un portal y entregué mis credenciales, y luego me percaté que no era un sitio institucional u oficial.
    - Mis archivos están inaccesibles (parece que están encriptados).
    - En mi computador aparece una nota o mensaje que solicita un rescate por recuperar mis archivos.
    - Mi ejecutivo de finanzas u otras personas dicen que desde mi correo les he enviado un mail y no he sido yo.
- 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 2FA.
  - Proteger a sus usuarios de sitios maliciosos usando proxy servers y manteniendo actualizados sus browsers.

- Proteger sus dispositivos del malware.
- Tener un protocolo de respuesta rápido ante estos incidentes.
- Detectar rápidamente estos incidentes instando a los usuarios a que reporten rápidamente cualquier actividad sospechosa.

- Para obtener los IoC de este reporte favor visitar la siguiente URL:
  - https://github.com/csirtcl/CodigoMalicioso/blob/main/Phishing-Malware_2CMV23-00401-01.txt

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.02.24 12:45:33 -03'00'