Alerta de seguridad informática	2CMV22-00379-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de noviembre de 2022
Última revisión	07 de noviembre de 2022

NOTA SOBRE EL CORRECTO USO Y DIVULGACIÓN DE ESTE DOCUMENTO

La información contenida en este informe fue procesada por 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 de 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 Alsea. En este correo malicioso, el victimario adjunta un archivo [.]xls que supuestamente contendría una cotización.

Si la víctima interactúa con el archivo adjunto su equipo sufrirá la explotación de la vulnerabilidad CVE-2017-11882, que abusa de un proceso llamado EQNEDT32.EXE por medio de un buffer overflow del stack, lo que permite la ejecución de código remoto.

Analizando las tácticas y técnicas asociadas a la muestra detectada, descubrimos las de **acceso inicial** (mediante phishing), **ejecución** (el usuario ejecuta el fichero malicioso), **descubrimiento** (enumeración de archivos y directorios y descubrimiento de llaves de registro), **evasión defensiva** (desofuscacion/ofuscación de archivos o información, modificación de registros, ejecución de binarios firmados).

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 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
COTIZACION ARTICULOS DE OFICINA PARA PRODUCCION	yazmin.sepulveda@alsea.com.mx	[187.217.245.25]

Indicadores de Compromiso Asociados

Archivos que se encuentran en la amenaza

Tipo	Indicador	Relación
SHA256	141db01f957472533d9791c5fb883b442d25d557497c0b6b94961fb64330a57f	##COTIZACION ARTICULOS DE OFICINA PARA PRODUCCION.xlsx
SHA256	2a93ae1bd54ea0587fac5a180e8f098cb5e5db2ff877ce5d8c82e1db1844c4fd	vbsss.vbs
URL	http://20.106.255[.]48/dll/nostartup.pdf	Malware Config
URL	"http://195.178.120[.]24/bdsbfdbjfbhjsfsdbfjds.txt"	Malware Config

Imagen del mensaje

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.

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.11.08 16:04:58 -03'00'