Alerta de seguridad informática	2CMV23-00398-01
Clase de alerta	Fraude
Tipo de incidente	Phishing-Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de enero de 2023
Última revisión	23 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 Autopase, sistema de pago del TAG. La campaña es difundida por medio de correo masivo, buscando que el receptor abra el mensaje al mencionar una falsa deuda de TAG, que supuestamente hará que el dispositivo sea deshabilitado.

Los delincuentes incluyen un enlace malicioso, el cual descarga un fichero tipo rar con otro archivo en su interior, este de extensión cmd, el que inyecta un código malicioso conocido como Mispadu. Misdapu pertenece a una familia de malware bancarios recientes, los cuales representan un riesgo para la información de los titulares de cuentas bancarias. Además, tiene capacidades de actualización a través de un archivo de Visual Basic Script (VBS), que se descarga y ejecuta automáticamente. Durante el proceso de infección, el malware recopila los datos de la computadora de la víctima como la versión del sistema operativo usado, el nombre de la computadora, el idioma del dispositivo, y si hay un 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
Su tag está inhabilitado por deuda.	postmaster@ashley-howard.co.uk	[185.26.148.57]

Indicadores de Compromiso Asociados

Archivos que se encuentran en la amenaza

Tipo	Indicador	Relación
SHA256	f669aba8e7621d7c21ad4553d6899311ecdff561fda86261a496a46c7604d4cc	DeudaAutopistas_193466.rar
SHA256	d016b039526f23dcddeeac7c511bd7ef439177541504e2998e19d7892481aa7d	DeudaAutopistas.cmd
SHA256	b753a9dc95ffc2fde9e31d8cbf7b44b59d25e393e7ad6a1effff6122011b4fef	~~
SHA256	593d0e89345ac495b7ab40fb789a51fd68c4f2f582de7c17c96f52ffa21e00e1	~~
SHA256	bb2a3bbc876eb671233d6980826be466464e7026fd3e2f71c8a825c0de2fa106	DriverAudio.lnk
SHA256	206a789ac6eaca1d44d4d89fa77d7e0407cfc9c9fcf5917ce4fc2a947328a8fc	DeudaAutopistas.a3x
SHA256	98e4f904f7de1644e519d09371b8afcbbf40ff3bd56d76ce4df48479a4ab884b	feldman.exe
SHA256	b3ce811fb696b94f9117ee7fe725ae6b907d695636beceeb1672d5d5eeb81df4	sqlite3.dll
URL	https://facturasnet[.]store/?uQNaBDB6VMlMEOBOuKU4UTuOJAvdL36I6gJMHTGD	Malware Config
URL	http://germogenborya[.]top/rest/?h=FA46E43C	Malware Config
URL	https://www.autoitscript[.]com/autoit3/pkgmgr/sqlite/sqlite3.dll	Malware Config
URL	http://vaadiandkoh[.]com/ue/app/do/it.php?f=9&w=Windows%207	Malware Config
URL	http://vaadiandkoh[.]com/ue/app/do/it.php?b1&v1=1033&v2=1033&v3=&v4=Windows%207&v5=Admin&v6=X64	Malware Config

Imagen del 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 incidente
  - 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: 2023.01.23 13:00:44 -03'00'