Alerta de seguridad informática	2CMV23-00414-01
Clase de alerta	Fraude
Tipo de incidente	Phishing-Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de mayo de 2023
Última revisión	23 de mayo de 2023

PARA EL CORRECTO USO Y DIVULGACIÓN DE ESTE DOCUMENTO LEER ACÁ

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT de Gobierno) ha identificado una nueva campaña de phishing con malware, que se difunde a través de un falso aviso judicial. El malware incluido en esta campaña es conocido como Grandoreiro.

Grandoreiro es un troyano bancario dirigido a los países de Latinoamérica, usado como puerta trasera para permitir a un atacante acceder a los dispositivos de la víctima y así robar su información personal y bancaria de las sesiones de banca online que inicien.

Indicadores de Compromiso Asociados

Archivos que se encuentran en la amenaza

SHA256

Indicador	Relación
3a053c761405b390b821dcfa246aef4e77f9bfa991ec5980ae58150793c1a8ba	AttatchmentFacturXGZRQOSURNNAOGCsoerh.zip
9a8bff65411c24aa7df8cb56053f21aad2868613fc84cf44bae06692bae0da06	Arc_Digital_AdjuntosBYRBGZMTJKLPACFmjfhhLBCGC.exe
0604388f107d1ed9abbb13912e5cdc2f9a2da8d0e528fbb4546c23b2f08c6f15	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~CDNYGVMAYT.xml

URL-Dominio

Dominio	Relación
https://atlinkwifiprogramado.australiacentral.cloudapp.azure[.]com/	Descarga del Fichero
https://www.dropbox[.]com/s/aagvp0fccnb8sk8/AttatchmentFacturQEDGDCLYXHEEAYDdqjvo.zip	Directorio del Malware
http://ip-api[.]com/json	Whois
20.54.89[.]15:443	IP
208.95.112[.]1	IP
67.27.158[.]126	IP

MITRE ATT&CK

Descripción	ID
Acceso Inicial (Mediante Phishing)	T1566.002
Descubrimiento (Descubrimiento de información del sistema)	T1082
Descubrimiento (Registro de consultas)	T1012
Persistencia (Carga lateral de DLL)	T1574.002

Imagen del Mensaje

Accion legal en proceso: Resolucion de Archivo Provisional (761791)

Importante <avisosjudicial@funcionpublica.com>
Para [redacted]

Responder | Responder a todos | Reenviar | ...

ma. 23/05/2023 7:53

Estimado Sr. Sra.

Tengo el honor de dirigirme a usted en calidad de Alejandra Solano, Asistente Operativa de la Sección de Decisión y Litigación Temprana del Ministerio Público. El motivo de mi comunicación es notificarle sobre la Resolución de Archivo Provisional adjunta, la cual reviste gran importancia.

Adjunto encontrará la mencionada Resolución de Archivo Provisional, la cual le solicito que revise detenidamente:

Resolución de Archivo Provisional

Quedo a su disposición para cualquier consulta o aclaración que pueda surgir una vez haya tenido la oportunidad de leer detenidamente la mencionada Resolución.

Aprovecho la ocasión para enviarle un cordial saludo y desearle una tarde exitosa.

Atentamente,
Alejandra Solano
Asistente Operativa
Sección de Decisión y Litigación Temprana
Ministerio Público

FALSO
CSIRT

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.05.24 10:02:47 -04'00'