Alerta de seguridad informática	**2CMV-00031-002**
Clase de alerta	**Código Malicioso**
Tipo de incidente	**Malware**
Nivel de riesgo	**Alto**
TLP	**Blanco**
Fecha de lanzamiento original	**11 de Octubre de 2019**
Última revisión	**11 de Octubre de 2019**

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones, por lo cual se recomienda establecer una cuarentena preventiva respecto de los IoC mencionados, previa evaluación de impacto en servicios productivos; una vez que sus plataformas de monitoreo no detecten actividad maliciosa, se debe evaluar la posibilidad de liberar del bloqueo a los IoC consignados en el reporte respectivo, tales como servicios de hosting, de cloud o similares.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, ha detectado la activación de la campaña phishing malicioso asociada al script dirigido contra la ciudadanía y el sistema bancario nacional vía uso proxy y extensión de Chrome (JS/ProxyChanger). Esta campaña se identificó a través de correos electrónicos maliciosos, cuyo mensaje intenta suplantar a una empresa de abogados, indicando que ya sé realizo un transferencia a la cuenta del usuario por una compra anulada.

El atacante insta al usuario para que imprima el recibo adjunto en el vínculo del correo. Al seleccionar el vinculo se gatilla el proceso de infección, direccionado a la url https://servicionoreply[.]blognetkatay[.]com/recibo/, donde se descarga el archivo “AdbFlash.zip”. Posteriormente es direccionado a http://www.hardlopenvoorbeginners[.]com/media/AdbFlash[.]js y como etapa final se descarga el malware en el equipo de la víctima. En seguida, el usuario visualiza un mensaje que indica que la actualización de Flash Player se efectuó exitosamente.

Observación

Solicitamos tener en consideración las señales de compromiso en su conjunto

Indicadores de compromisos

Servidor Smtp

[139.99.220.164]
[51.79.140.143]

Sender

root@krim.blognetkatay[.]com [139.99.221.214]
root@krvm.blognetkatay[.]com [51.79.142.50]
root@krem.blognetkatay[.]com [51.79.140.143]
root@kram.blognetkatay[.]com [139.99.220.164]
root@krom.blognetkatay[.]com [139.99.222.182]
root@krum.blognetkatay[.]com [51.79.143.215]

Asunto

ReciboTransferencia

Url's:

https://dc586.4shared[.]com/download/y8BVJJy4ea/AdbFlash.zip
https://servicionoreply.blognetkatay[.]com/recibo?
http://www.thenewworking[.]info
http://novocontador[.]club
http://192.210.179.48/0bbva1/
http://192.210.179.48/0fala1/
http://192.210.179.48/0bice1/
http://192.210.179.48/0bci1/
http://192.210.179.48/0santa1/
http://192.210.179.48/0office1/
http://192.210.179.48/0bchile1/
http://192.210.179.48/0bbva1/
http://192.210.179.48/0bbva1/
http://192.210.179.48/0be1/
http://192.210.179.48/0ita1/
http://192.210.179.48/0rip1/
http://192.210.179.48/0bs1/

HASH

Nombre : AdbFlash.zip
MD5 : 178d136329592dd7f64a4424110e085d

Nombre : AdbFlas.js
MD5 : 266620d1b953131d1382b728fa3e1e2f

Nombre : Chrome.zip
MD5 : 37cdefb1020e06b5c6bb6c598766a352

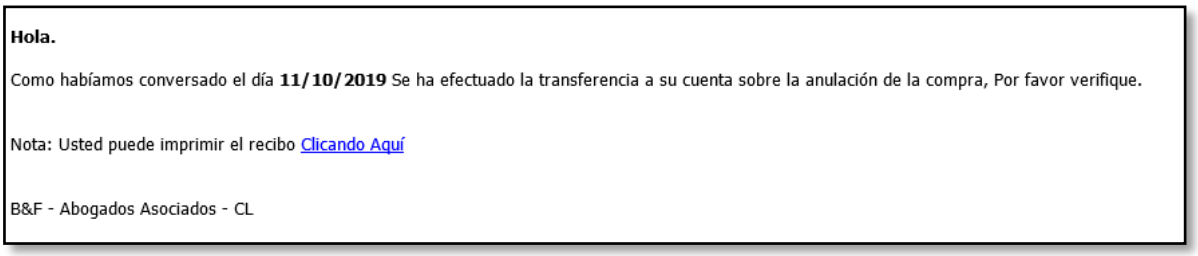
Nombre : Chrome.js
MD5 : add9d4ebde3ff2c9dba72414cf24b1d5

Nombre : manifest.json
MD5 : 9e8e19482f788f4ac8f4cc09d23fd2cd

IP Proxy Script

[104.36.2239.160]

Imagen Correo



Hola.

Como habíamos conversado el día **11/10/2019** Se ha efectuado la transferencia a su cuenta sobre la anulación de la compra, Por favor verifique.

Nota: Usted puede imprimir el recibo Clicando Aquí

B&F - Abogados Asociados - CL

Imagen de Script y proxy

```
var sitekkkkk = "http://ww.bbva.cl";                                  http://104.36.229.160/0bbva1/
var sitekkkkkk = "http://ww.bancofalabella.cl";                       http://104.36.229.160/0fala1/
var sitekkkkkkk = "http://ww.bice.cl";                                http://104.36.229.160/0bice1/
var sitekkkkkkkk = "http://ww.bci.cl";                                http://104.36.229.160/0bci1/
var site = "http://ww.santander.cl";                                  http://104.36.229.160/0santa1/
var sitek = "http://ww,officebanking.cl";                             http://104.36.229.160/0office1/
var sitekk = "http://ww.bancochile.cl";                               http://104.36.229.160/0bchile1/
var sitekkk = "http://ww.scotiabankchile.cl";                         http://104.36.229.160/0bbva1/
var sitekkkk = "http://ww.scotiabankchile.cl";                        http://104.36.229.160/0bbva1/
var sitekkkkz = "http://ww.bancoestado.cl";                           http://104.36.229.160/0be1/
var sitekkkkztt = "http://ww.banco.itau.cl";                          http://104.36.229.160/0ita1/
var sitekkkkzttaa = "http://ww.bancoripley.cl";                       http://104.36.229.160/0rip1/
var sitekkkkzttaab = "http://ww.personas.bancosecurity.cl";           http://104.36.229.160/0bs1/
```

Recomendaciones

- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras), desde los sitios oficiales de los fabricantes.
- Evaluar el bloqueo preventivo de los indicadores de compromisos
- Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas
- Revisar los controles de seguridad de los AntiSpam y SandBoxing
- Realizar concientización permanente para los usuarios sobre este tipo de amenazas
- Visualizar los sitios web que se ingresen que sean los oficiales

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.10.11 19:42:05 -03'00'