Alerta de seguridad informática	**2CMV-00034-001**
Clase de alerta	**Fraude**
Tipo de incidente	**Phishing - Malware**
Nivel de riesgo	**Alto**
TLP	**Blanco**
Fecha de lanzamiento original	**02 de Octubre de 2019**
Última revisión	**02 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 identificado una campaña de phishing con malware asociado a Emotet. Estos correos contienen documentos tipo Word adjuntos, donde el atacante intenta persuadir a las víctimas para que abran el documento. Dichos correos se han identificado en campañas dirigidas a Chile.

Indicadores de compromisos

Smtp Host

srvin[.]franchiseindia[.]com [180[.]179[.]213[.]95]
peewee[.]webdevworld[.]com [129[.]232[.]213[.]67]
tokai-seimitsu[.]co[.]jp [114[.]147[.]32[.]97]
relay1[.]telco[.]co[.]zw [41[.]191[.]236[.]19]
mail[.]hosting[.]co[.]zw [196[.]44[.]177[.]101]
srvk123[.]allytech[.]com [190[.]210[.]196[.]123]
200-105-174-170[.]acelerate[.]net [200[.]105[.]174[.]170]
server[.]kielsa[.]com[.]ni [198[.]1[.]67[.]110]
static-200-105-174-170[.]acelerate[.]net ([200[.]105[.]174[.]170]
ip190-5-139-146[.]intercom[.]com[.]sv [190[.]5[.]139[.]146]
cm11[.]websitewelcome[.]com [100[.]42[.]49[.]5]

Sender

kmohit@franchiseindia[.]net
toto@nicmart.co[.]zw
tdp-impex@tokai-seimitsu.co[.]jp
admin@prodorite.co[.]zw
toto@nicmart.co[.]zw
kbadilla@kielsa[.]cr
pmedoro@renaultlumiere.com[.]ar
asistente@ccci.com[.]sv

Subject:

RV: Aviso de Transferencia de Fondos Nro. 7010485
Enviando por correo electrónico: 201910021648136
Adjunto le enviamos información, de fecha 02/10/2019

Archivos Adjuntos

Declaración de nomina.doc
Declaración de nómina mensual.doc
02-10-2019_1648136.doc
Nomina.doc
Documento_20191002 45346.doc
20191002 29188.doc

Hash

2991e2843045df8dd0feec4b5ff83f2c
3ede45ee3dacb64701dad58f8023ee3d
d88dd86c60b490af77a57128858a6c34
cc17ed43a035bd33d81376fe5d434e69

Url's:

http://www[.]sangsnagissue[.]net/wp-admin/3vp5/
http://www[.]devotionalline[.]com/wp-content/2uet0lo44207/
http://www[.]n01goalkeeper[.]com/wp-content/kwwg-06b-09/
http://www[.]themilkconcept[.]com/cgi-bin/gXLEOznm/
http://www[.]littlepoppetschildcare[.]com/wp-content/d0u884f-z1cajbo9s-36678/
http://www[.]energysensorium[.]com/33b52n/OgtNMZM/
http://www[.]russvet[.]net/wp-admin/KrcbLxRv/
http://www[.]sangsnagissue[.]net/wp-admin/3vp5/
http://www[.]devotionalline[.]com/wp-content/2uet0lo44207/
http://pinnacleclinic[.]com/others/9z7paz795/
http://reposesionbancaria[.]com/wp-content/plugins/9f342/
https://riversidehoanghuy[.]com/cgi-bin/oodz286/
http://sangsnagissue[.]net/wp-admin/

Recomendaciones

- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras)
- 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

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.10.02 13:00:27 -03'00'