Alerta de seguridad informática	**2CMV-00029-001**
Clase de alerta	**Fraude**
Tipo de incidente	**Phishing - Malware**
Nivel de riesgo	**Alto**
TLP	**Blanco**
Fecha de lanzamiento original	**02 de Septiembre de 2019**
Última revisión	**02 de Septiembre 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 través de un correo electrónico que supuestamente proviene de la Tesorería General de la Republica. Los delincuentes buscan engañar a los usuarios advirtiéndoles sobre una supuesta liquidación tributaria impaga. A la potencial víctima se le ofrece la posibilidad de descargar desde el hipervínculo indicado el informe generado por el Servicio de Impuesto Internos. Al descargar el archivo y ser ejecutado, desencadena la infección de malware.

Indicadores de compromisos

Url's:

http[:]//documentsofc[.]com/styles/?ACAO=descargar[.]cgi
http[:]//documentsofc[.]com/Downl/?ACAO=descargar[.]cgi
http[:]//www[.]aguatimbu[.]com[.]br/novo/wp-content/plugins/message-cl[.]zip
http[:]//www[.]suzano[.]sp[.]gov[.]br/refis/downs/tf34a[.]btc
http[:]//www[.]suzano[.]sp[.]gov[.]br/refis/downs/tf34b[.]btc
http[:]//www[.]suzano[.]sp[.]gov[.]br/refis/downs/tf35a[.]btc
http[:]//www[.]suzano[.]sp[.]gov[.]br/refis/downs/tf35b[.]btc
http[:]//www[.]suzano[.]sp[.]gov[.]br/refis/downs/tf34-1[.]btc
http[:]//www[.]suzano[.]sp[.]gov[.]br/refis/downs/

Smtp Host

[92.119.114.57]
[92.119.114.95]
[92.119.114.128]
[45.88.76.165]
[85.209.88.42]
[45.88.76.228]
[45.88.78.36]
[45.88.78.6]

Sender

root@ubuntus[.]com
root@ubuntuzzz[.]com
root@ubuntux[.]com
root@r[.]com

Subject:

Segundo Aviso.
Segundo Aviso (TGR)

Archivos adjuntos.

Archivo : message-cl.zip
MD5 : 447655ffe1b63e11a33ea0c55bd33d2e
SHA256 : d8af589352e36f5def43deabee47fa3af7534a83265397234f07684cf216de9c

Archivo : message-cl.msi
MD5 : a245836673ca097a1d85cbf6db21df37
SHA256 : 513153c18c7aaaaf37b88f8c6f8e9b0399af9e4724bd9d2fd5ad610d6ee2eca6

Archivo : SA2HP3N7EJTKKURDRP7BIKGOOG
MD5 : 5d80e80c603311d2bbcabf7cff99cb41
SHA256 : f29448d67d9069b552ff633c51b096378bbc1433277266cfe74c679057ed1659

Archivo : D2Z9WXAMRUMEX2Y6YETQAX805A4
MD5 : b06e67f9767e5023892d9698703ad098
SHA256 : 8498900e57a490404e7ec4d8159bee29aed5852ae88bd484141780eaadb727bb

Archivo : ILZH97RQLYXRWIMT1MPQOV0PR8WFP
MD5 : ed98049e17891d72213f253fcb5b12f6

Otros IOC asociados.

64a751205446ba41cec0a1dcf0830ad4c69f5333fb0b7b935c9fcdf7053af118
39bcddee58154455bfcd3888bd77434d26ca7be659f21ac779c4a5af64b459ef
39bcddee58154455bfcd3888bd77434d26ca7be659f21ac779c4a5af64b459ef
6acecfc3063a16cbf9215dc454fed4debfea81b90d7b6c8e67176e912884ccbb
5cd47073e928da27d91a925151299308e8a91dc3ff25e29aee312a79b2181768
8498900e57a490404e7ec4d8159bee29aed5852ae88bd484141780eaadb727bb
d1de03a41b357198e1d65478c5171f4f9c50bfb38bf813cd8b611a1ed02eb2fc
c1ce6c3ad896acf57392f36135d039829033551b37f67fc381be73465e5dbccf
096f912caff09921f98df1a33cd074dcf955f60164096234bf47a59e92d8fc43
8498900e57a490404e7ec4d8159bee29aed5852ae88bd484141780eaadb727bb
c1ce6c3ad896acf57392f36135d039829033551b37f67fc381be73465e5dbc
096f912caff09921f98df1a33cd074dcf955f60164096234bf47a59e92d8fc43
8498900e57a490404e7ec4d8159bee29aed5852ae88bd484141780eaadb727bb
54ce6a08276e12017f753a3fbdab4422e9e9d919ff88d123e44d9f8f6e0e8442
b8ed18ed54fc0616060b06c6a79c37da72341ae617e4f03f8d28c7d070efa467
8498900e57a490404e7ec4d8159bee29aed5852ae88bd484141780eaadb727b

Imagen Phising de Correo

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: 2019.09.02
13:05:57 -04'00'