Alerta de seguridad cibernpetica	2CMV20-00070-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de Agosto de 2020
Última revisión	05 de Agosto de 2020

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 malware a través de un correo electrónico que utiliza el nombre del Servicio de Impuestos Interno (SII).

El atacante intenta persuadir a quien recibe el mensaje para descargar un archivo adjunto.

El mensaje del correo informa que la Tesorería General de la Republica ha encontrado una liquidación impaga. Si bien el mensaje utiliza el logo del SII, el mensaje indica que el procedimiento es de Tesorería General. Otro vector a considerar es la presencia de errores en la redacción y ortografía.

Al seleccionar el enlace para descargar el informe se produce la descarga de un archivo ZIP, el cual al ser descomprimido, permite obtener otro archivo con extensión MSI. Al ser ejecutado, se gatilla un script y se procede a la descarga del malware bancario.

Indicadores de compromisos

Servidor Smtp

[20.151.19.230]
[20.151.19.218]
[20.151.22.30]
[20.151.19.235]
[20.151.3.149]
[20.48.144.53]
[20.151.20.217]
[20.151.20.174]
[20.151.19.238]
[20.151.21.59]
[20.151.20.70]
[20.151.21.53]
[20.151.22.94]
[20.151.22.78]
[20.151.22.61]
[20.48.145.211]
[20.48.144.105]
[20.48.145.38]
[20.48.144.122]
[20.48.145.177]
[20.48.145.1]
[20.48.144.177]
[20.48.144.115]
[20.48.145.219]
[20.48.145.163]
[20.48.145.60]

Sender

root@webmasterfox01.superattescl[.]com
root@webmasterfox04.superattescl[.]com
root@webmasterfox07.superattescl[.]com
root@webmasterfox16.superattescl[.]com
root@webmasterfox21.superattescl[.]com
root@webmasterfox24.superattescl[.]com
root@webmasterfox25.superattescl[.]com
root@webmasterfox26.superattescl[.]com
root@webmasterfox29.superattescl[.]com
root@webmasterfox31.superattescl[.]com
root@webmasterfox32.superattescl[.]com
root@webmasterfox33.superattescl[.]com
root@webmasterfox36.superattescl[.]com
root@webmasterfox41.superattescl[.]com
root@webmasterfox48.superattescl[.]com
root@webmasterfox62.superattescl[.]com
root@webmasterfox64.superattescl[.]com
root@webmasterfox67.superattescl[.]com
root@webmasterfox70.superattescl[.]com
root@webmasterfox74.superattescl[.]com
root@webmasterfox75.superattescl[.]com
root@webmasterfox83.superattescl[.]com
root@webmasterfox88.superattescl[.]com
root@webmasterfox90.superattescl[.]com
root@webmasterfox94.superattescl[.]com
root@webmasterfox99.superattescl[.]com

Asunto

Estimado(a) Contribuente-SII

Url's

- hxxps://takarada-lab.ees.st.gunma-u.ac[.]jp/website/wp-content/themes/twentynineteen/classes/000012989018087978947891287312 89TR/index1.php
- hxxp[:]//wwwfox.supremetearmazenfoxweb[.]com/tr/

Hash

Nombre	MD5
006303911090820122ID-.zip	829c57f49f43ef8a08c2285731995c2c
090129090318480802.msi	17e59eb8a5cb7df1ecbc0d4a012a014a
64tr0099090090224.ogo	2244e2e08fa12937cfd832c0c9607014
EOR56CQENDMSW6O78YDRPZTVSOPHA2	7dc005b3f95938f307b590e3aac5010d
PDBQSOMNBVK70TS5RO0B2N60EM522GJE9	830d938d575de3df6c7d3c0ee751ad9b
XPX9ODM9S6416RE633Q4CECBLI7LW1F857	7e0315ba03606af593aa331c4522654a

Imagen del mensaje

Recomendaciones

- No abrir correos ni mensajes de dudosa procedencia.
- Desconfiar de los enlaces y archivos en los mensajes o correo.
- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen por internet
- Prestar atención en los detalles de los mensajes o redes sociales
- 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 sean los oficiales.