Alerta de seguridad informática	2CMV22-00297-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	4 de mayo de 2022
Última revisión	4 de mayo de 2022

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigación propia del CSIRT de Gobierno. 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 de Gobierno) ha identificado una campaña de phishing con malware. El mensaje que proviene, supuestamente, de la Tesorería General de la República (TGR) informa que existen obligaciones impagas y que puede revisar el informe generado por la TGR en el archivo adjunto, ingresando la contraseña que se indica en el correo. Al descargar el archivo y ser ejecutado, se gatilla la infección del equipo.

Observación

Solicitamos tener en consideración las señales de compromiso en su conjunto.

IoC Correo Electrónico

Datos del encabezado del correo

Asunto

✓Tesorería General de la Republica (TGR) informa que existen obligaciones pendiente.

Correo Electrónico

[meyers_bjoern@web.de]
[webmaster@24service.co.il]
[lynxaviacao@lynxaviacao.com.br]
[mssce@server.ony.oyo.mybluehostin.me]
[sub1552_63@lin05.mandichost.com.br]
[allcarem@server2.lbshost.com]

Servidor de correo

[sh11689.ispgateway.de]
[vmi827000.contaboserver.net]
[plesklinux01.mandic.com.br]
[server.ony.oyo.mybluehostin.me]
[lin05.mandichost.com.br]
[66-7-223-5.static.hostdime.com]

IoC Archivo

Archivos que se encuentran en la amenaza

Nombre: SII63301220.zip
SHA256: 4a2d4e8907797a94e5cd032cc67c7a1116f9f640c6aaed531afc60578385adf5

Nombre: SII63301220.msi
SHA256: 20eb84bc76f6da4eff41a66dfcc0b4c5372233d1568f73d701b9f9f8e8c98da1

Nombre: batger.ahk
SHA256: 2182ac079032bc9e21f20646ff5be6f9a8536a70ce2824b1c2783178e8f2f723

Nombre: lock.txt
SHA256: 6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b

Nombre: libeay32.dll
SHA256: cb7f180d74dd744fe32260026cc12d051af0c5f6e1ef31adc387773a1b44f967

Nombre: JSON.ahk
SHA256: bb85e4530ccd6355b3ef3506548b4f513bea844d1af37a69624c9c455521c70f

Nombre: ssleay32.dll
SHA256: 754aadc3aa19e07f2ba20217ddb0412d90e686e9965100ec7dc16475dea2077f

Nombre: batger.exe
SHA256: 3242e0a736ef8ac90430a9f272ff30a81e2afc146fcb84a25c6e56e8192791e4

Nombre: TD821YEJSDM813UJR.zip
SHA256: 8941f7cc75ae085f5b45c94b831ecc0f8a2aeba792d75b98292660feda2b8775

Nombre: HSQMDJHviL.aoc
SHA256: fd99e83a1161f3cf6bc07f5f973d0272e42e7f1aa9fa7ae22c9c9b1378b3d6c5

Nombre: VKXc7tb8Ff4IccFmggg
SHA256: 3242e0a736ef8ac90430a9f272ff30a81e2afc146fcb84a25c6e56e8192791e4

Nombre: raO01Fqx7RW42i0fy6H11ZaHhhh
SHA256: 5ee419a1bda6b3d9ed3c5ffcaa2b4763bd7e7c57d40caa4f89ceebcd689ac840

IoC URLS

hXXps://physionormandie[.]com/wp-content/languages/--/https:/www.tgr.cl/?cliente=

hXXps://www.stt.eesc.usp[.]br/wp-content/languages/SII63301220.zip

hXXps://www.hardam[.]biz/stats/awsindex/TD821YEJSDM813UJR.zip

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.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.05.04 13:58:57 -04'00'