Alerta de seguridad informática	2CMV22-00300-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de mayo de 2022
Última revisión	26 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 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 de Gobierno) ha identificado una campaña de phishing con malware. El mensaje que proviene falsamente del Ministerio de Transporte y Telecomunicaciones indica a la víctima que tiene una multa de hace más de dos meses por andar a exceso de velocidad y que no ha sido pagada. Para revisar la falsa multa, el atacante adjunta un documento en formato PDF con una contraseña, sin embargo, al descargar el archivo realmente descarga un programa malicioso que infectará el equipo.

Observación

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

IoC Correo Electrónico

Datos del encabezado del correo

Asunto

MTT - Atencion Ciudadano, le Informamos sobre Multas Pendentes a su nombre Verifique ahora - (963936576154)

Servidor de correo

177.70.106.69
177.70.106.248
162.215.210.185
60.43.176.211

Correo Electrónico

sub1552_63@lin05.mandichost.com.br
lynxaviacao@lynxaviacao.com.br
mssce@server.ony.oyo.mybluehostin.me
mw2pqgpp93@kawahara-law.jp

IoC Archivo

Archivos que se encuentran en la amenaza

Nombre: MTT002140001451.zip
SHA256: 078e67fd81467f42d9ce1d65904e9dea2a84cab29975815ec7a03fdc2c740cc1

Nombre: MTT002140001451.msi
SHA256: 9830bd16aedd4387da7bbe79c4e036b60b005df5d2964626c10be2d30257c35f

Nombre: normer.ahk
SHA256: 33d4ef958d813f813d0bc789726d7503200bf280caceb4667d99a144e634dbfd

Nombre: JSON.ahk
SHA256: bb85e4530ccd6355b3ef3506548b4f513bea844d1af37a69624c9c455521c70f

Nombre: normer.exe
SHA256: 3242e0a736ef8ac90430a9f272ff30a81e2afc146fcb84a25c6e56e8192791e4

Nombre: R1ewB32bi97tH.duc
SHA256: 69bea5a467e532fbc06965b0d15f0bfbe5245c9f4f5009a3b4854762cb7454d4

Nombre: bed0rx63lm32i71hjc29cfx1ggg
SHA256: 3242e0a736ef8ac90430a9f272ff30a81e2afc146fcb84a25c6e56e8192791e4

Nombre: uelrzutvji.ejj
SHA256: 5c8c5586ccb204e4c0826e2bfd883985c7c7cff83c2bb4295d7bb4a69a1e57b8

Nombre: k25ekw8qh8fa5j870uieq6p79hhh
SHA256: c4fa0cda59435c48dd1ea003e9739a12a1c69c934d8ffcf1a522e16110e3d33c

Dominios / URLs:

famelic[.]com
csie.npu.edu[.]tw
vanyapaperproducts[.]com

https://csie.npu.edu[.]tw/wp-content/languages/MTT002140001451.zip
https://www.vanyapaperproducts[.]com/common/img/next/R1ewB32bi97tH.duc

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: 2022.05.27 09:18:20 -04'00'