ALERTA DE SEGURIDAD CIBERNÉTICA

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT de Gobierno, informa que ha detectado una nueva campaña de correo electrónico que busca propagar el peligroso programa malicioso Emotet, la cual está siendo dirigida a distintas organizaciones que conforman la administración del Estado.

Según las últimas investigaciones, las nuevas apariciones de Emotet tienen un comportamiento diferente al de ocasiones anteriores. Esto, ya que con el objetivo de que el malware no sea detectado por los programas de ciberseguridad, el atacante adjunta a su correo electrónico un archivo con extensión .zip, junto a la contraseña para descomprimirlo. Una vez hecho esto, el usuario encontrará un archivo .doc, el que a su vez incorpora un script ofuscado.

Si el usuario ejecuta este documento, el script comienza a buscar en internet los sitios web donde se ha alojado previamente un archivo DLL malicioso para su descarga, realizando la infección del equipo. También se ha detectado Emotet en archivos de Excel (.xlsm), o directamente en enlaces de descarga.

Emotet es considerado altamente peligroso, debido a que no es fácil de identificar y es de rápida propagación. Por esto, el CSIRT de Gobierno recomienda estar alertas y reforzar las medidas de seguridad de cada de las instituciones. Para ello, sugerimos:

- Mantener actualizados los sistemas operativos, navegadores y complementos.
- Mantener antivirus e instalar sus actualizaciones periódicas.
- Aumentar las medidas de seguridad de los programas antispam o poner en cuarentena los archivos .zip que incluyan una contraseña, con tal de realizar una revisión preventiva.
- Educar a los funcionarios para que no descarguen archivos ni tampoco ingresen a enlaces de correos que provengan de un remitente desconocido. Para apoyar esta labor, adjuntamos una campaña de concientización realizada por el CSIRT de Gobierno sobre Emotet y compartir entre los trabajadores.

De igual manera, solicitamos informar al CSIRT de Gobierno si detectan este tipo de correos electrónicos o si sufren una afectación de los sistemas para apoyar cualquier incidente.

Indicadores de compromiso

IOC URLS

http://primtalent[.]com/wp-admin/9yt1u/
http://huskysb[.]com/wordpress/6f0qIQlWPaYDfa/
http://ridcyf[.]com/dm7vg/DGWFrJA0kutWTk/
http://manak.edunetfoundation[.]org/school-facilitator/qlwM2RAHhDG8N8/
http://ckfoods[.]net/wp-admin/wPInm2rgMu/
http://adorwelding.zmotpro[.]com/wp-content/Z8ifMTCM2VBWlfeSZmzv/
http://server.zmotpro[.]com/venkat/products/facebook-page/assets/kmIdeXnG/
http://vegandietary[.]com/wp-admin/IFtPKsn/
http://parentingkiss[.]com/wp-admin/LMgGsVXx02LX/
http://pibita[.]net/wp-admin/VLpfaG1/
http://vcilimitado[.]com/trendfit/aBER6PrBXc7/
https://thetrendskill[.]com/wpcontent/HbbVwxEkhvYdloXmjWeBb
https://onlinemanager[.]site/szrlo/XRL3pyAvQ9NoDug7wzAzyuL/
https://www.cursossemana[.]com/wp-content/zwfj5luCBBEL3RrbBgPsz

IOC Correo electrónico

kunitani@pro.odn.ne.jp
vargag@sp-steelmont.hu
urmil.shah@torqueholdings.in
sushma@inasolution.com

IOC Archivos DLL

Nombre : 0XcrLbkUok4.dll
SHA256 : b1872d1db76cc8777a35b41478c3e530f40d11e11710ecc4f360066a0d6175a6

Nombre : FW4y.dll
SHA256 : 05f251f9b66d86646b3f9886bbb525414580cf9698cd4918ec79c706fc679a38

Nombre : RAW2aukSucSwJb.dll
SHA256 : b8ad4931315f781e7abb33bb193e0ea2419dd4e9302b3ae6c0471ff51c2fc8c4

IOC Nombre archivo adjunto

Nombre : 34664544503.zip
SHA256 : fd121c02b770f85c40eecddffc9151f076d870072b814a81850c4e6af6a8d24d

Nombre : 1711.zip
SHA256 : 45147af5b75a5870b767c49d7e11fccb13eac5335cec528f7870d3d1705d540c

Nombre : 349715407767.zip
SHA256 : 0aa7959b910129c6c4b2239f1814c97bd481df23c01daaf60351f80ce31af79f

Nombre : 34664544503.doc
SHA256 : e5f3a7e75c03d45462992b0a973e7e25b533e293724590c9eb34f5ee729039b0

Nombre : 1711.doc
SHA256 : 74ff5ac7d5efe16714141ff9139f7cffde6c462050c67c58e1860d501e961cc1

Nombre : 349715407767.doc
SHA256 : ba4b86f4302e41521e17046e8bd75f59b1137b5e4a3881d460ee2c7655fed0d5

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.11.23 09:47:23 -03'00'