Alerta de seguridad informática	2CMV21-0250-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de noviembre de 2021
Última revisión	22 de noviembre de 2021

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 malware, donde el atacante busca persuadir a las personas de descargar un archivo adjunto y ejecutarlo, para de esta forma infectar el equipo. El mensaje del correo solo muestra la contraseña de un archivo adjunto con extensión .ZIP

Familia de malware: EMOTET

Observación

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

IoC Correo Electrónico

Datos del encabezado del correo

Servidor de Correo
p3plsmtpa11-10.prod.phx3.secureserver.net - [68.178.252.111]

Asunto
Integra Botón de Pago

IoC Archivo

Archivos que se encuentran en la amenaza

Nombre : 704.zip
SHA256 : c99fea9f7c41af8a448c38aeaf85d200bd508bb84a08a584fa82765104d03e92

Nombre : 704.doc
SHA256 : d05ec2a0134518ec74fcbee94a522c3837d82b7b5d2f162b8466850fc4f1be0d

Nombre : RAW2aukSucSwJb.dll
SHA256 : b8ad4931315f781e7abb33bb193e0ea2419dd4e9302b3ae6c0471ff51c2fc8c4

Nombre : FW4y.dll
SHA256 : 05f251f9b66d86646b3f9886bbb525414580cf9698cd4918ec79c706fc679a38

Nombre : 0XcrLbkUok4.dll
SHA256 : b1872d1db76cc8777a35b41478c3e530f40d11e11710ecc4f360066a0d6175a6

IoC Red

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/

Imagen del Mensaje

Mitre ATT&CK

Mitre ATT&CK es una metodología en la que se clasifican las tácticas o técnicas utilizadas por un atacante. Con esto, es posible identificar y entender la manera que tienen de operar basándose en observaciones reales.

En el caso del malware Emotet, publicado en este informe, las técnicas usadas fueron:

T1059 : Command and Scripting Interpreter
T1064 : Scripting
T1203 : Exploitation for Client Execution
T1059.001 : PowerShell
T1055 : Process Injection
T1036 : Masquerading
T1562.001 : Disable or Modify Tools
T1497 : Virtualization/Sandbox Evasion
T1055 : Process Injection
T1140 : Deobfuscate/Decode Files or Information
T1406 : Obfuscated Files or Information
T1518.001 : Security Software Discovery
T1057 : Process Discovery
T1083 : File and Directory Discovery
T1082 : System Information Discovery
T1105 : Ingress Tool Transfer

Más información sobre Mitre ATT&-CK en https://attack.mitre.org/

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: 2021.11.22 12:57:17 -03'00'