Alerta de seguridad cibernética	2CMV21-00137-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Enero de 2021
Última revisión	25 de Enero 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.

Estos casos de phishing no involucran directamente a las entidades ni al sistema bancario, sino que son técnicas de fraude indirecto, en las que en infraestructura externa a éstas se arma el mencionado phishing, para construir el engaño. Las entidades, en general, al tomar conocimiento de estos portales maliciosos articulan, dentro de sus potestades y marco legal vigente, las acciones necesarias para poder desarticularlos, pero ciertamente los usuarios también estamos llamados a estar atentos a estos intentos de engaño.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), comparte una serie de Indicadores de Compromiso (IoC) obtenidos del análisis realizado a múltiples campañas de phishing con archivos adjuntos que contienen malware catalogado como **EMOTET**, los que están circulando en el ciberespacio nacional y representan un riesgo para los sistemas informáticos, así como para los usuarios en general.

CSIRT recomienda a los administradores y usuarios bloquear los hash publicados en este informe, y mantener un permanente monitoreo sobre el resto de los Indicadores de Compromiso.

Observación

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

IoC hash

Hash SHA-256 de los archivos adjuntos en los correos electrónicos:

93c786b73d5a68527bfa3630ed9578fa6706cc9be21c746852baf913281825e2
ad2d3f962576e50cdece1884fb9584e0b6269c551eafe565e3062ff01b2b33b9
225dada2c55351dee296d9491814c30a9d0e2ddfaeaa742ae6e65c1373cf7006
49308d0126ffd48ff35716a5ae47551d1f438df17fd32fb704f9f4c4ecf0a204
e3a69d01de9b2730ba45903580e9e6a0add7228fdf3f1e63afae1154d10e2994

IoC nombre de archivo

Nombres de archivos con malware:

copy payment.doc
8J1-059.doc
75NX0762943614.doc
1UE084418.doc
B9W26394452.doc

IoC descarga malware URLs

Comunicación de los archivos adjuntos de los correos electrónicos al ser ejecutados:

URI Activas

http://nightlifemumbai.club/x/0wBD3/
http://traumfrauen-ukraine.de/bin/JyeS/
http://covisiononeness.org/new/F9v/
http://190.55.186.229/1yid8fz5mq2apkp4/3fxjy9ckyo4/0il4ohv3x1/uhmzki0pup8u/zvo830vx422oud4bu5y/

IoC servidor SMTP

Direcciones IP de servidor SMTP. Se debe tener consideración que podrían aparecer direcciones de Servicios Cloud reconocidos, ya que este apartado informa desde donde salieron los correos electrónicos maliciosos.

79.101.22.73
153.138.238.39
153.138.238.41
153.149.228.33
153.149.228.36
153.149.232.32
153.153.67.33
153.138.238.38
153.153.67.35
153.138.237.38
153.153.67.34
206.123.6.133
202.191.118.236

IoC Correo Electrónico

Correo electrónico de donde fue enviado:

radeivanovic@dmdm.rs
edi@taiheidenki.co.jp
f.kondoh@eiwa-bussan.com
onestcool@aei.ca
suzuki@ekouwa.co.jp

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.