Alerta de seguridad informática	2CMV-00041-001
Clase de alerta	Fraude
Tipo de incidente	Malware - Emotet
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de Diciembre de 2019
Última revisión	13 de Diciembre de 2019

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), ha identificado una campaña de Malware-Emotet. La campaña se activa a partir de archivos .doc que se encuentran almacenados en sitios nacionales vulnerados, los que al ser ejecutados por el usuario, gatillan un script que establece contacto con sitios internacionales desde los que se descargan archivos que desencadenan la infección.

Indicadores de compromisos

Url's:

https[:]//boiler-horizontal[.]com/wp-admin/SdTBtO/
http[:]//fedomede[.]com/wp-content/danvv6/
http[:]//acqua[.]solarcytec[.]com/rtsbgs/XiWmtYYur/
https[:]//blog[.]learncy[.]net/wp-admin/user/oxZqQp/
https[:]//sg771[.]kwikfunnels[.]com/phpmyadmin_bck/x9tfn-lv1h4-174129596/
http[:]//www[.]4celia[.]com/wp-admin/2z8/
http[:]//capsaciphone[.]com/wp-admin/q07360/
http[:]//www[.]yadegarebastan[.]com/wp-content/mhear/
http[:]//bikerzonebd[.]com/wp-admin/89gw/
http[:]//110[.]143[.]84[.]202/eZnS
http[:]//75[.]80[.]148[.]244/LQtlmwgJUA
http[:]//64[.]53[.]242[.]181[:]8080/LBHZCloioAjiBTTtrf
http[:]//37[.]59[.]24[.]177[:]8080/9CJLOGHy8aBTYmTGj

http[:]//66[.]34[.]201[.]20[:]7080/dwWKHTQmvtj
http[:]//shptoys[.]com/_old/bvGej/
http[:]//www[.]vestalicom[.]com/facturation/qgm0t/
http[:]//theaustinochuks[.]com/personal_array/kvrmif
http[:]//vikstory[.]ca/h/f2cgrvw
http[:]//faustosarli[.]com/wp-admin/myzw0
http[:]//sarafifallahi[.]com/wp-admin/uuxtplhi
http[:]//173[.]91[.]11[.]142
http[:]//47[.]6[.]15[.]79
http[:]//73[.]60[.]8[.]210
http[:]//190[.]146[.]14[.]143
http[:]//110[.]143[.]84[.]202

Hash-MD5

76fdabc2468d659a03fe7c21508eeec2
01055706487a3ca32c1dbe0f0699a64f
cc7d6d8e28fce962e81a6ba5c82f29bb
06df51681e60a644a166b39dd56de541
55e5f07ada51fb94cc0825b17161632d
2c0dd945e2a2b8397943be49fe09382e
bae1aba27189aa73a57073322c71f9e6
927589f49455119ee3d49ef128390e76
59dd089b9fcc95533b3ecebed74ee682
e3fb481130256c5a5cc3b72443174f8d
4ff5dfcf428d3b968499eabf42e74adc
73812beee6e54f303e57b2059f7aa7cc

Recomendaciones

- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras)
- 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

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.12.13 20:07:14 -03'00'