Alerta de seguridad informática	8FPH20-00112-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de Febrero de 2020
Última revisión	13 de Febrero de 2020

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), ha identificado una campaña de phishing a través de un correo electrónico supuestamente de un proveedor de servicio de correo.

El mensaje informa a la víctima que ha excedido el tamaño del buzón y no podrá enviar o recibir correos. El atacante ofrece como solución actualizar la cuenta y de esta forma aumentar el tamaño de la cuenta. Además indica que si no lo realiza dentro de tres próximos días se cerrará la cuenta permanentemente. Al seleccionar el vínculo para actualizar la cuenta, la víctima es dirigida a un sitio donde le solicitan su correo, su usuario y contraseña.

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

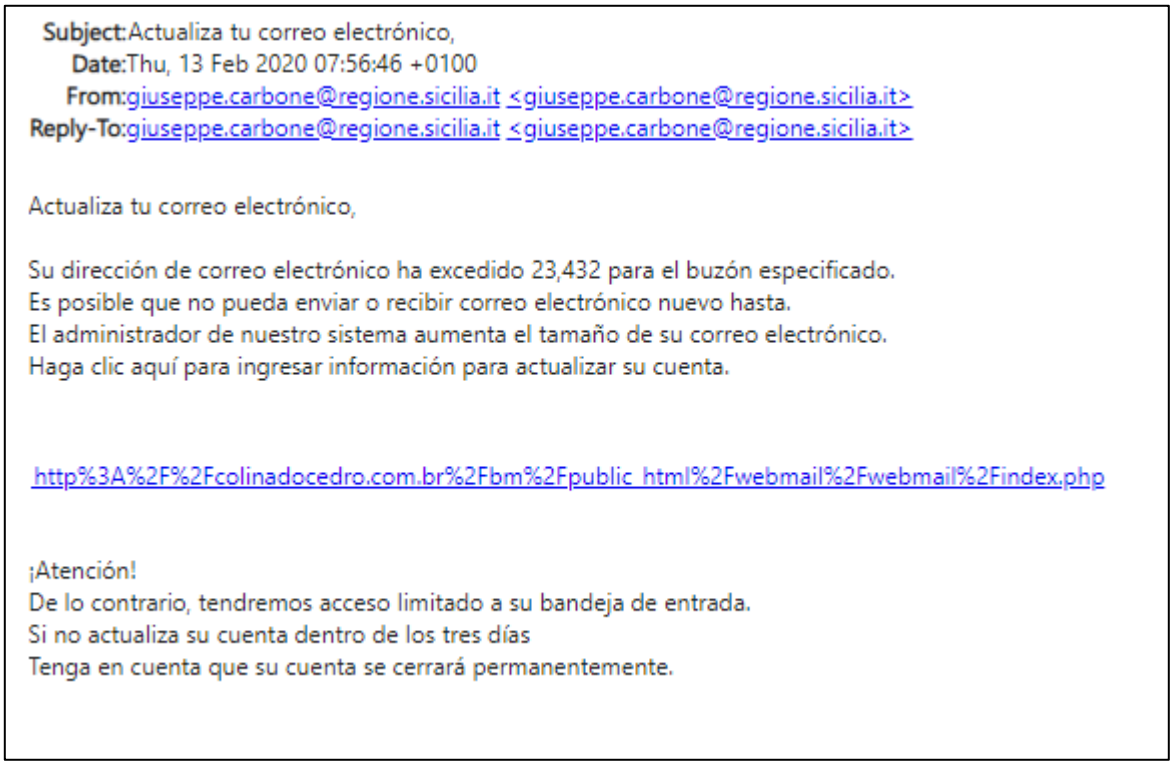
Indicadores de compromisos
Url's
http[:]//colinadocedro[.]com[.]br/bm/public_html/webmail/webmail/index[.]php

Sender
giuseppe[.]carbone[@]regione[.]sicilia[.]it

Smtp Host
[151.0.254.154]

Subject
Actualiza tu correo electrónico,

Imagen del correo



Subject: Actualiza tu correo electrónico,
Date: Thu, 13 Feb 2020 07:56:46 +0100
From:giuseppe.carbone@regione.sicilia.it <giuseppe.carbone@regione.sicilia.it>
Reply-To:giuseppe.carbone@regione.sicilia.it <giuseppe.carbone@regione.sicilia.it>

Actualiza tu correo electrónico,

Su dirección de correo electrónico ha excedido 23,432 para el buzón especificado.
Es posible que no pueda enviar o recibir correo electrónico nuevo hasta.
El administrador de nuestro sistema aumenta el tamaño de su correo electrónico.
Haga clic aquí para ingresar información para actualizar su cuenta.

http%3A%2F%2Fcolinadocedro.com.br%2Fbm%2Fpublic_html%2Fwebmail%2Fwebmail%2Findex.php

¡Atención!
De lo contrario, tendremos acceso limitado a su bandeja de entrada.
Si no actualiza su cuenta dentro de los tres días
Tenga en cuenta que su cuenta se cerrará permanentemente.

Imagen Sitio Web

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
- Visualizar los sitios web que se ingresen que sean los oficiales

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.02.13 13:44:42 -03'00'