Alerta de seguridad informática	8FPH20-0096-001
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de Enero de 2020
Última revisión	20 de Enero 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.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de phishing a través de un correo electrónico que intenta engañar a usuarios del correo electrónico corporativo Microsoft Outlook Web Access 2020.

El mensaje informa que se realizó una actualización de los sistemas de correo, acción que genera más espacio de almacenamiento y un acceso más fácil. El atacante disponibiliza un enlace que dirige a un sitio falso de correo corporativo donde se le solicita el nombre de usuario y contraseña.

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

Indicadores de compromisos

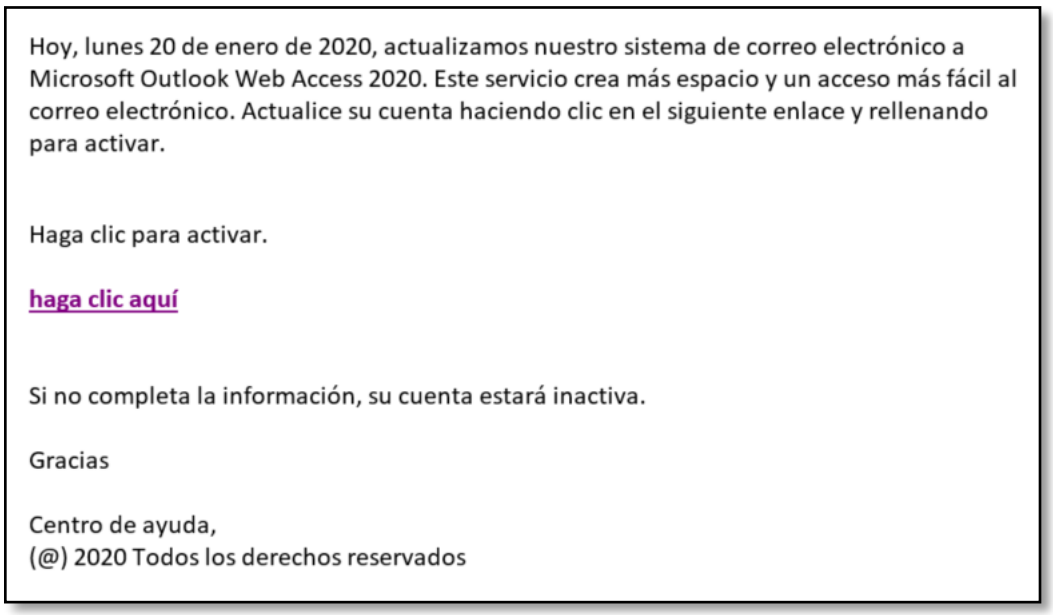
Url's:
https[:]//mynameman12[.]wixsite[.]com/mysite

Smtp Host
[213.177.9.251]

Sender
Simona[.]Matis@primariaclujnapoca[.]ro

Subject:
Microsoft !!!

Imagen Phishing Correo



Hoy, lunes 20 de enero de 2020, actualizamos nuestro sistema de correo electrónico a Microsoft Outlook Web Access 2020. Este servicio crea más espacio y un acceso más fácil al correo electrónico. Actualice su cuenta haciendo clic en el siguiente enlace y rellenando para activar.

Haga clic para activar.

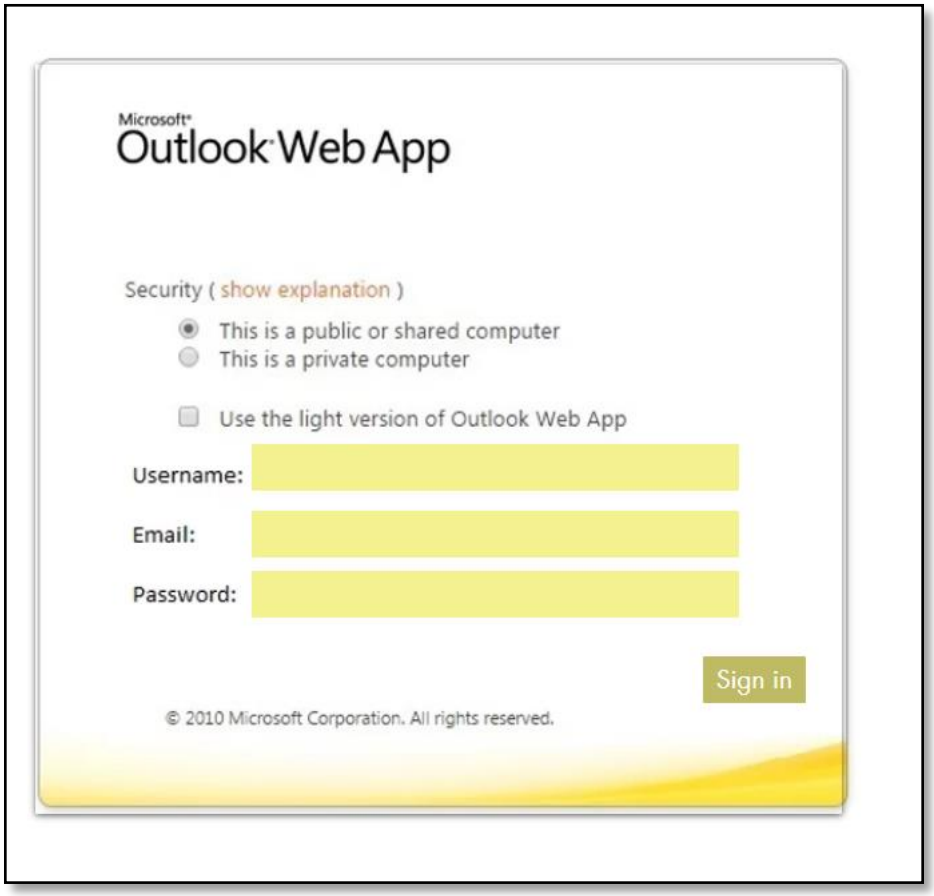
haga clic aquí

Si no completa la información, su cuenta estará inactiva.

Gracias

Centro de ayuda,
(@) 2020 Todos los derechos reservados

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: 2020.01.20 12:16:05 -03'00'