Alerta de seguridad informática	**1ASP-00010-001**
Clase de alerta	**Contenido Abusivo**
Tipo de incidente	**Spam**
Nivel de riesgo	**Alto**
TLP	**Blanco**
Fecha de lanzamiento original	**29 de Agosto de 2019**
Última revisión	**29 de Agosto 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 dos campañas de Spam que aprovecha la configuración automática del calendario de Google, que en realidad intentan engañar a los usuarios para seleccionar un hipervínculo adjunto que, al ser seleccionado redirecciona a sitios no confiables. Si el usuario ingresa al enlace, este se expone a ser víctima de un fraude, robo de información personal o posible malware.

La primera de las campañas comunica que sortea gratuitamente un iPhone Xs. La segunda, menciona que existe una oferta del día que tiene como regalo una tarjera de Amazon con US $700 (Dólares) para clientes leales. El regalo tiene un tiempo limitado de 12 horas para reclamado.

De la primera campaña no se pudieron obtener los índices de compromisos pues se encontraban desactivados los enlaces que direccionaban a los sitios supuestamente maliciosos. CSIRT presume que podrían volver a activarse. La segunda campaña está activa. De esta se pudieron identificar 4 dominios con 375 subdominios que tienen relación a la campaña de spam. Este ataque aprovecha la configuración automática del calendario de Google.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.08.29 18:10:30 -04'00'

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

Indicadores de compromisos

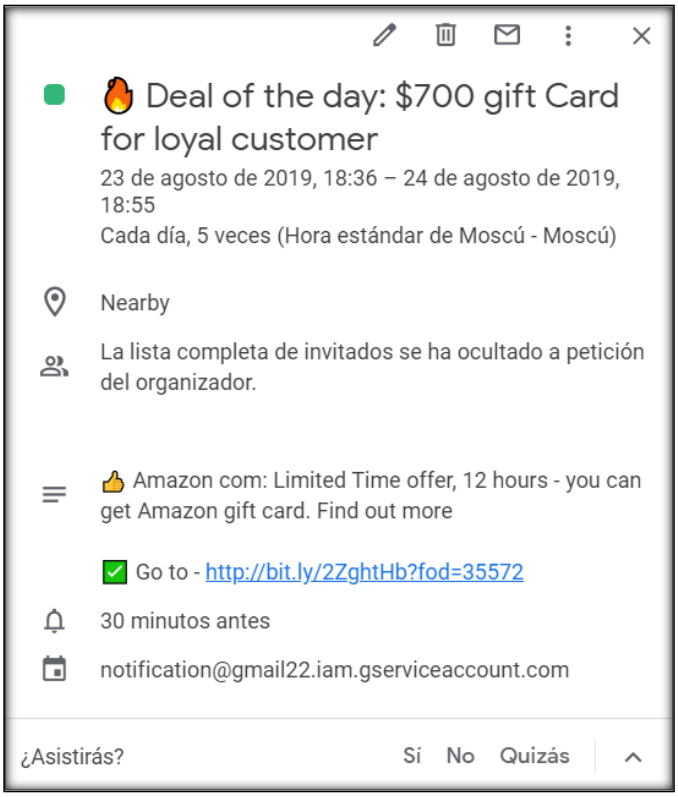
Dominios:

.pushs-routg[.]com
.routgpushs[.]com
.soptarroutg[.]com
.newsfacce[.]com

IP

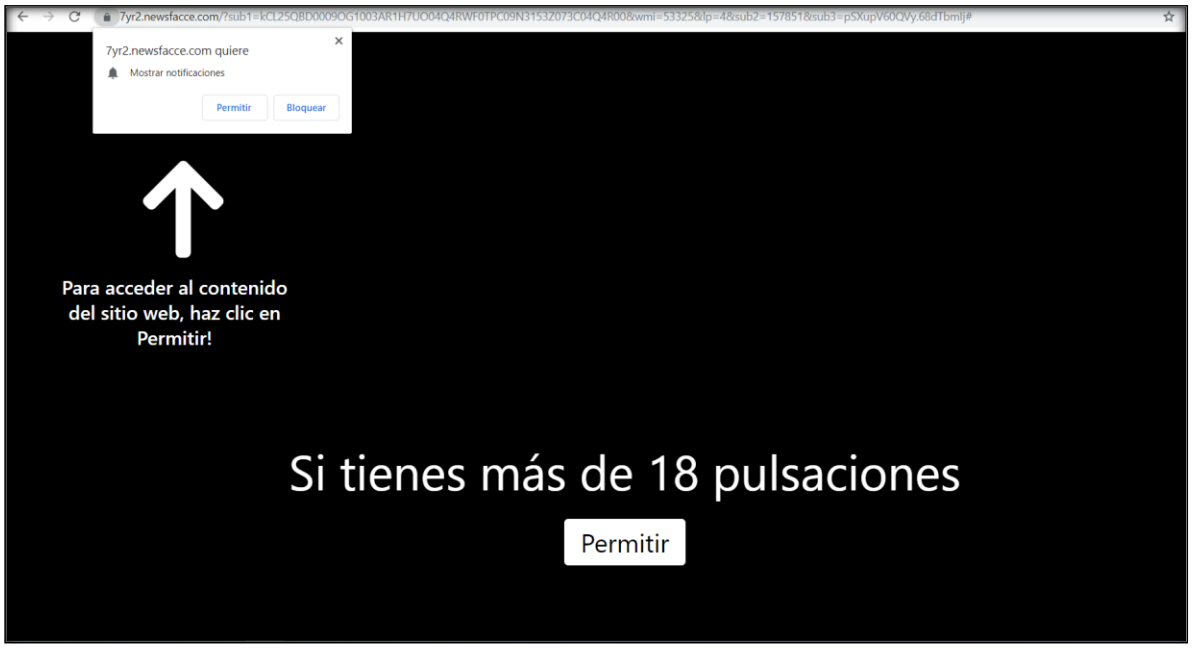
[108.61.69.28]

Imagen SPAM


Deal of the day: $700 gift Card for loyal customer
23 de agosto de 2019, 18:36 – 24 de agosto de 2019, 18:55
Cada día, 5 veces (Hora estándar de Moscú - Moscú)
Nearby
La lista completa de invitados se ha ocultado a petición del organizador.
Amazon com: Limited Time offer, 12 hours - you can get Amazon gift card. Find out more
Go to - http://bit.ly/2ZghtHb?fod=35572
30 minutos antes
notification@gmail22.iam.gserviceaccount.com
¿Asistirás?
Sí
No
Quizás

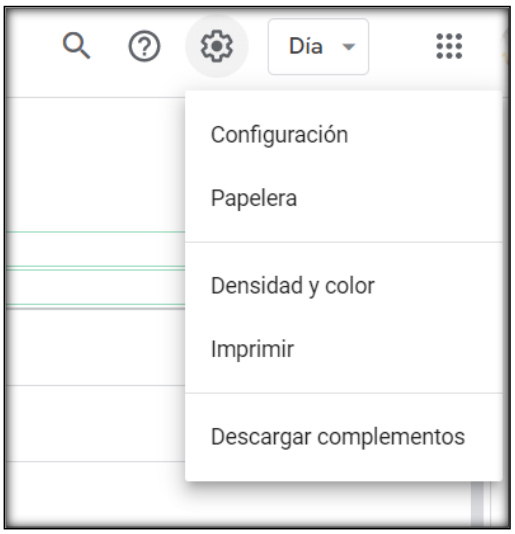

19:49 – mié 28 de ago 11:49
iPhone Xs Free Giveaway before launching a new model (► Near You - http://amznsale.mobi/f?i=16994)

Imagen Sitio Web



Recomendaciones

- Desactivar agendamiento automático.
- Seleccione la opción configuración en la parte superior derecha de la pantalla



- Luego ir “Configuración de los eventos” y en el campo “Añadir invitaciones de forma automática” seleccionar la opción que dice “No mostrar únicamente las invitaciones a las que he respondido”