

Alerta de seguridad cibernética	4IIA21-00034-01
Clase de alerta	Intentos de Intrusión
Tipo de incidente	Intentos de acceso – Fuerza bruta
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de Marzo de 2021
Última revisión	26 de Marzo 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 afectada 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 de Gobierno), ha identificado una serie de intentos de acceso a servidores de correos del sector público y privado. Estos ataques de fuerza bruta intentan vulnerar la autenticación del protocolo para transferencia simple de correos (SMTP) para suplantar a los remitentes originales para depositar correos con contenido o enlaces maliciosos en las bandejas de entrada de sus potenciales víctimas.

Indicadores de compromiso

IP detectadas y activas

IP	Etiqueta de sistema autónomo
45.227.253.115	Global Layer B.V.
27.255.75.16	EHOSTICT
5.188.206.246	Krez 999 Food
78.128.113.131	Miti 2000 EOOD
185.24.233.76	Sternforth Ltd.

IP reportadas en informes anteriores y que aún se encuentran activas hasta la fecha de este reporte:

5.188.206.235
193.169.255.72
87.246.7.226
212.70.149.85
212.70.149.55

Recomendaciones

- Evaluar el bloqueo preventivo de los indicadores de compromisos.
- Utilizar los registros SPF, DKIM y DMARC
- Revisar o configurar correctamente los filtros de AntiSpam
- Revisar los controles de seguridad de los AntiSpam y SandBoxing.
- Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas.
- 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).
- Realizar concientización permanente para los usuarios sobre este tipo de amenazas.