Alerta de seguridad cibernética	4IIA21-00040-01
Clase de alerta	Intentos de Intrusión
Tipo de incidente	Intentos de acceso – Fuerza bruta
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de julio de 2021
Última revisión	21 de julio 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 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 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 con tal de depositar correos con contenido o enlaces maliciosos en las bandejas de entrada de sus potenciales víctimas.

Indicadores de compromiso

IP detectadas y activas

N°	IP	Etiqueta de sistema autónomo
1	191.240.25.118	Rede Brasileira de Comunicacao SA
2	37.49.225.14	PEENQ.NL
3	190.152.71.34	MORQUECHO GARCIA SEGUNDO JUAN
4	45.118.34.23	IMPERIAL COMMUNICATION ENTREPRENEURS PVT LTD
5	212.70.149.88	InternetHosting-LTD
6	191.53.193.100	Rede Brasileira de Comunicacao SA
7	45.183.93.105	NEWNET TECNOLOGIA E PROJETOS LTDA
8	212.70.149.56	InternetHosting-LTD
9	213.92.194.243	NORNET-PL Gniezno
10	5.188.206.146	Technology Advanced Investment Limited
11	37.130.26.99	INTERKAM SZCZEPANIK SPOLKA KOMANDYTOWA
12	187.87.3.214	M4.NET ACESSO A REDE DE COMUNICACAO LTDA - ME
13	87.246.7.228	InternetHosting-LTD
14	176.101.131.69	Biznes Swiatlowodem Sp. z o.o.
15	92.242.199.131	Respina Networks & Beyond PJSC
16	186.250.196.57	IBL Telecomunicacoes Ltda.
17	103.41.197.16	Zenox Solutions Pvt. Ltd
18	191.240.114.66	Rede Brasileira de Comunicacao SA
19	200.12.31.114	HomeNet LTDA
20	45.227.34.49	COOPERATIVA DE OBRAS Y SERVICIOS PUBLICOS DE CANALS LIMITADA
21	138.94.119.105	Latin American and Caribbean IP address Regional Registry
22	191.240.115.1	Rede Brasileira de Comunicacao SA
23	94.241.165.24	Rayasepehr Vira Co.
24	190.109.74.32	RG.COM - INFORMATICA & COMUNICACAO LTDA - ME
25	45.179.189.71	J. CALUX & CIA LTDA
26	177.44.89.119	Rede Brasileira de Comunicacao SA
27	45.165.213.90	W M S FONTES INFORMATICA - LTDA
28	192.162.179.35	INFOELTECH s. c.
29	189.201.196.82	Global Web Master Ltda - EPP

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.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.07.21 18:12:50 -04'00'