Alerta de seguridad cibernética	4IIA20-00014-01
Clase de alerta	Intentos de Intrusión
Tipo de incidente	Intentos de acceso – Fuerza bruta
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Noviembre de 2020
Última revisión	18 de Noviembre 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 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

1.225.101.152	213.108.162.237	177.87.212.234	218.82.119.170
14.164.136.176	220.179.231.250	178.254.171.89	220.233.4.53
14.169.193.239	1.52.160.220	178.254.179.49	221.3.236.94
37.221.178.155	110.16.85.62	181.176.222.68	222.138.10.46
37.221.179.146	110.39.184.42	185.100.13.251	222.141.18.29
37.221.179.206	111.224.166.20	185.246.8.189	222.223.56.116
60.174.118.123	111.224.166.30	185.246.8.190	222.67.113.123
81.250.162.238	114.108.125.98	185.246.8.197	24.209.64.71
97.104.206.212	114.95.146.116	185.246.9.19	27.128.193.90
103.141.138.120	118.121.41.19	185.39.25.124	37.221.181.31
111.224.166.214	121.200.88.226	185.49.168.32	37.99.250.11
141.105.104.170	122.7.216.73	185.92.194.60	37.99.253.141
141.105.105.222	123.27.174.100	186.31.118.76	37.99.255.113
178.254.171.130	125.117.28.184	187.84.18.223	37.99.255.176
178.254.171.173	134.90.250.91	188.255.132.13	41.193.22.146
182.189.201.233	134.90.252.156	188.255.132.35	58.221.42.231
186.190.224.116	134.90.253.173	188.255.132.53	58.221.44.163
188.255.131.167	14.177.59.181	188.255.237.62	59.57.253.66
188.255.131.232	14.48.200.79	190.86.37.170	60.29.197.152
188.255.131.236	141.98.80.79	193.169.252.60	61.19.246.25
188.255.132.115	154.0.53.50	197.237.161.13	69.144.99.202
188.255.132.119	156.96.44.183	197.237.243.68	77.109.177.12
188.255.132.125	156.96.56.184	2.186.53.137	83.209.236.79
188.255.132.211	168.121.72.148	202.134.118.30	94.200.172.30
188.255.237.163	171.242.233.29	202.165.236.71	
188.255.237.189	175.117.79.125	212.69.22.121	
188.255.237.234	175.126.84.168	212.69.24.59	
200.216.159.230	177.47.140.133	218.25.31.150	

Recomendaciones

- Evaluar el bloqueo preventivo de los indicadores de compromisos.
- Utilizar los registros SPF, DKIM y DMARCK
- 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: 2020.11.18 14:35:32 -03'00'