Alerta de seguridad cibernética	4IIA20-00020-01
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 Diciembre de 2020
Última revisión	18 de Diciembre 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

222.185.243.130	177.154.238.84	191.53.237.0
78.128.113.67	187.87.14.204	60.171.100.234
199.192.16.253	187.111.54.189	171.240.34.95
141.98.80.87	177.85.130.114	138.36.200.179
178.32.144.167	45.164.201.107	191.7.116.16
5.188.206.203	201.55.159.25	112.253.33.14
151.80.237.221	212.244.23.165	123.146.82.68
37.49.225.208	177.52.74.137	82.202.65.70
177.92.244.247	201.55.159.114	123.20.63.12
177.154.238.47	5.188.206.203	37.99.251.98
186.224.248.87	212.69.17.195	191.53.52.232
168.205.111.185	39.72.60.136	191.53.221.13
103.53.113.78	187.1.57.178	27.14.211.95
168.205.109.229	188.92.213.91	114.111.195.34
189.51.103.125	45.181.30.226	91.83.160.181
138.36.201.159	191.53.238.165	186.250.203.222
167.250.98.0	106.5.58.88	49.130.97.105
45.181.30.165	178.219.120.63	111.224.53.125
45.162.21.203	114.100.48.187	222.185.243.130
191.53.220.255	209.42.78.84	103.25.134.143
187.95.59.45	62.193.129.232	179.189.197.35
190.109.43.107	187.87.1.87	91.245.30.79
196.52.107.216	121.150.28.217	177.126.200.103
45.169.17.246	212.181.80.144	191.102.120.50
5.188.206.203	179.125.118.189	37.99.252.137
103.237.57.254	170.80.204.89	213.92.204.228
78.8.189.103	170.246.61.165	31.170.61.98
177.184.245.115	201.247.47.246	
45.4.170.82	198.36.30.144	
191.53.237.51	187.87.8.251	

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.