Alerta de seguridad cibernética	4IIA21-00041-01
Clase de alerta	Intentos de Intrusión
Tipo de incidente	Intentos de acceso – Fuerza bruta
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de julio de 2021
Última revisión	28 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), 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:

N°	IP	Etiqueta de sistema autónomo
1	37.0.10.7	Serverion BV
2	5.188.206.234	Technology Advanced Investment Limited
3	5.188.206.235	Technology Advanced Investment Limited
4	109.95.180.76	BDINET TYLSKI spolka jawna
5	45.144.225.205	Serverion BV
6	203.159.80.190	Transferred to the RIPE region on 2017-11-22T23:30:38Z.
7	31.210.21.220	Serverion BV
8	45.133.1.102	Serverion BV
9	170.239.54.81	Latin American and Caribbean IP address Regional Registry
10	45.133.1.58	Serverion BV
11	5.188.206.199	Technology Advanced Investment Limited
12	103.25.86.61	ApnaTeleLink pvt. Ltd.
13	136.144.41.70	RIPE Network Coordination Centre
14	87.107.159.144	Pardazeshgar-raay-azma
15	195.133.40.83	Des Capital B.V.
16	43.224.182.88	Panchsheel Broadband Services Private Limited
17	31.210.20.48	Serverion BV
18	5.188.206.197	Technology Advanced Investment Limited
19	45.144.225.204	Serverion BV
20	5.188.206.196	Technology Advanced Investment Limited
21	37.0.11.124	Serverion BV
22	103.241.243.9	Apna telelink pvt ltd
23	185.24.233.168	ServeByte VPS
24	136.144.41.87	RIPE Network Coordination Centre
25	91.192.207.68	Niles sp. z o.o.
26	196.0.86.62	Uganda Telecom Ltd
27	45.144.225.206	Serverion BV
28	103.156.91.43	Representative office No. 2 of VietServer Services technology Ltd.
29	45.133.1.109	Serverion BV
30	138.122.37.41	Latin American and Caribbean IP address Regional Registry
31	45.133.1.100	Serverion BV
32	5.188.206.195	Technology Advanced Investment Limited
33	2.56.59.87	Serverion BV

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: 2021.07.29 10:58:26 -04'00'