Alerta de seguridad informática	**2CMV-00027-001**
Clase de alerta	**Código Malicioso**
Tipo de incidente	**Malware**
Nivel de riesgo	**Alto**
TLP	**Blanco**
Fecha de lanzamiento original	**29 de Agosto de 2019**
Última revisión	**29 de Agosto de 2019**

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 sitios web nacionales clonados con malware asociado, a continuación se enumeran los sitios web y los IoC relacionado al archivo que inyecta el malware.

Observación

Solicitamos tener en consideración las señales de compromiso en su conjunto

Indicadores de compromisos

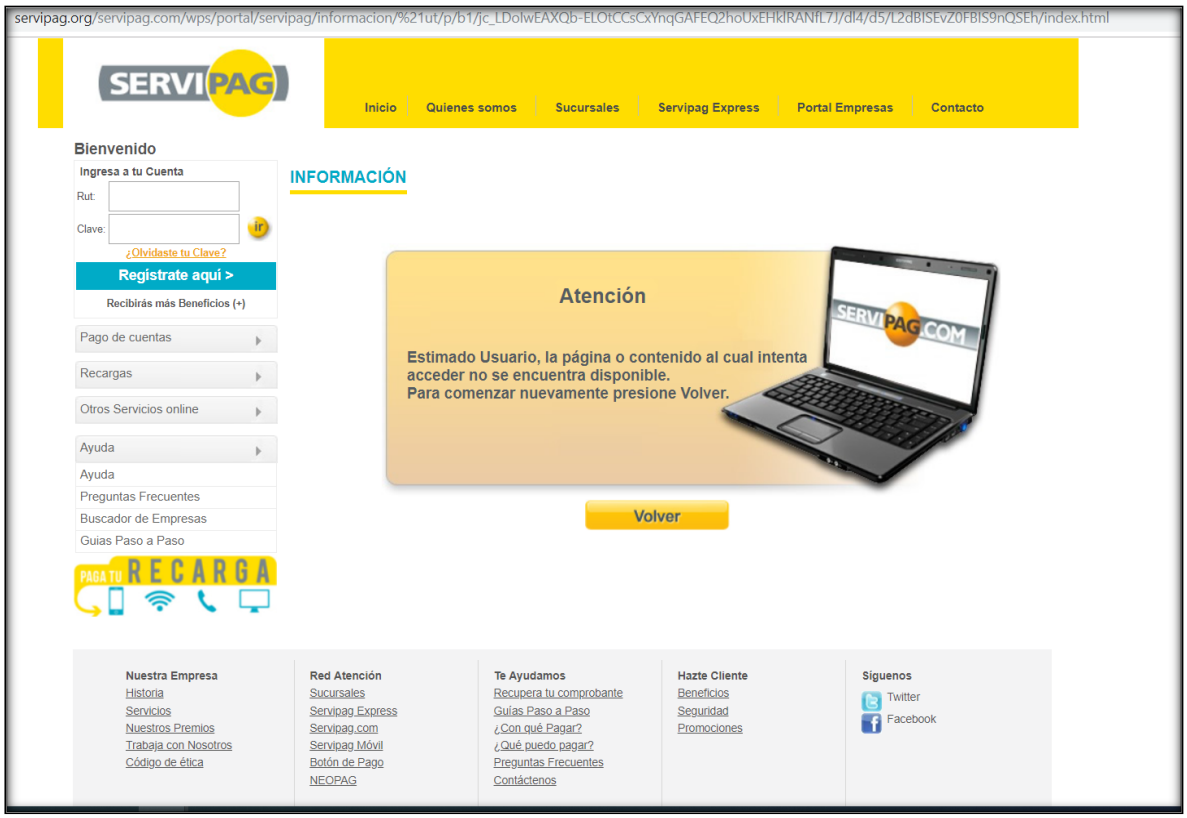
Dominios:

Clyapo[.]net
Siicl[.]net
Emolcl[.]com
Whatsappl[.]net

Archivos:

Nombres	:	actualizacion_servipago.cl.cmd
	:	actualizacion_yapo.cl.cmd
	:	nuevo_sii.cl.cmd
MD5	:	7f6192b5499d503531977c457162f7f6

Imagen de sitios clonados




No seguro | clyapo.net
yapo.cl
Publicar aviso
La idea es simple
Encuentra clasificados en tu región
1.497.131 avisos disponibles
26.186 productos vendidos en los últimos 7 días
Es muy fácil encontrar lo que buscas
1 Busca en tu región
2 Contacta con el vendedor
3 Haz un buen negocio
Región Metropolitana
XV Arica & Parinacota
I Tarapacá
II Antofagasta
III Atacama
IV Coquimbo
V Valparaíso
VI O'Higgins
VII Maule
XVI Ñuble
VIII Biobío
IX Araucanía
XIV Los Ríos
X Los Lagos
XI Aisén

Recomendaciones

- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras)
- Evaluar el bloqueo preventivo de los indicadores de compromisos
- Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas
- Revisar los controles de seguridad de los AntiSpam y SandBoxing
- Realizar concientización permanente para los usuarios sobre este tipo de amenazas
- Visualizar que los sitios web a los que se ingresen sean los oficiales

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.08.29 17:32:55 -04'00'