Alerta de seguridad informática	**2CMV-00026-001**
Clase de alerta	**Código Malicioso**
Tipo de incidente	**Adware**
Nivel de riesgo	**Alto**
TLP	**Blanco**
Fecha de lanzamiento original	**23 de Agosto de 2019**
Última revisión	**23 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 relacionados con anuncios publicitarios no deseados (Adware). Este ataque de ingeniería social intenta persuadir a los usuarios para que seleccionen “permitir” en el mensaje que aparece en el navegador, lo que como consecuencia multiplicará el envío de anuncios no deseados directamente al equipo del afectado.

El anuncio puede ser activado al ingresar en algún sitio no confiable. El usuario será bombardeado de mensajes para ver contenidos o para descargar información.

También cabe la posibilidad que un usuario haya instalado algún software gratuito que contenga un Adware, por ejemplo, a través de una “Play Store” con aplicaciones (APK), ofreciendo anuncios no deseados. Dichas aplicaciones se hacen pasa por aplicaciones legítimas especialmente centrada en juegos y fotografías.

Observación

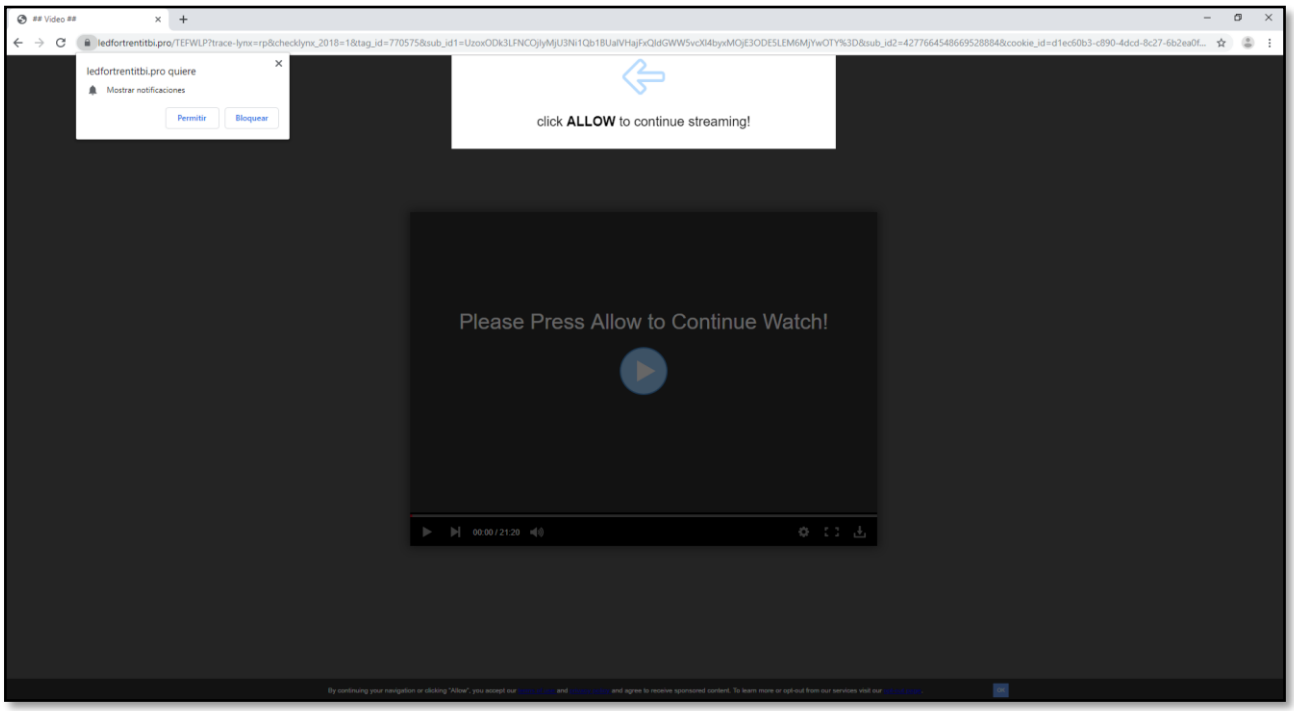
Solicitamos tener en consideración las señales de compromiso en su conjunto

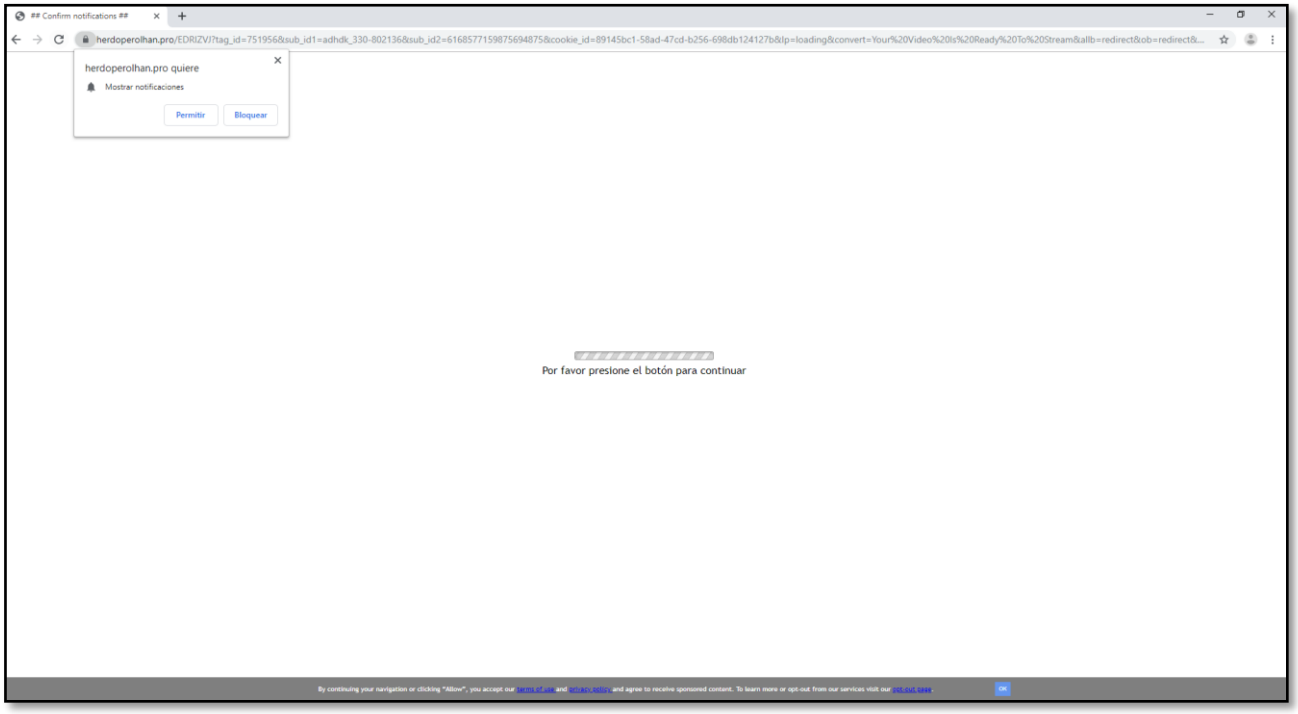
Indicadores de compromisos

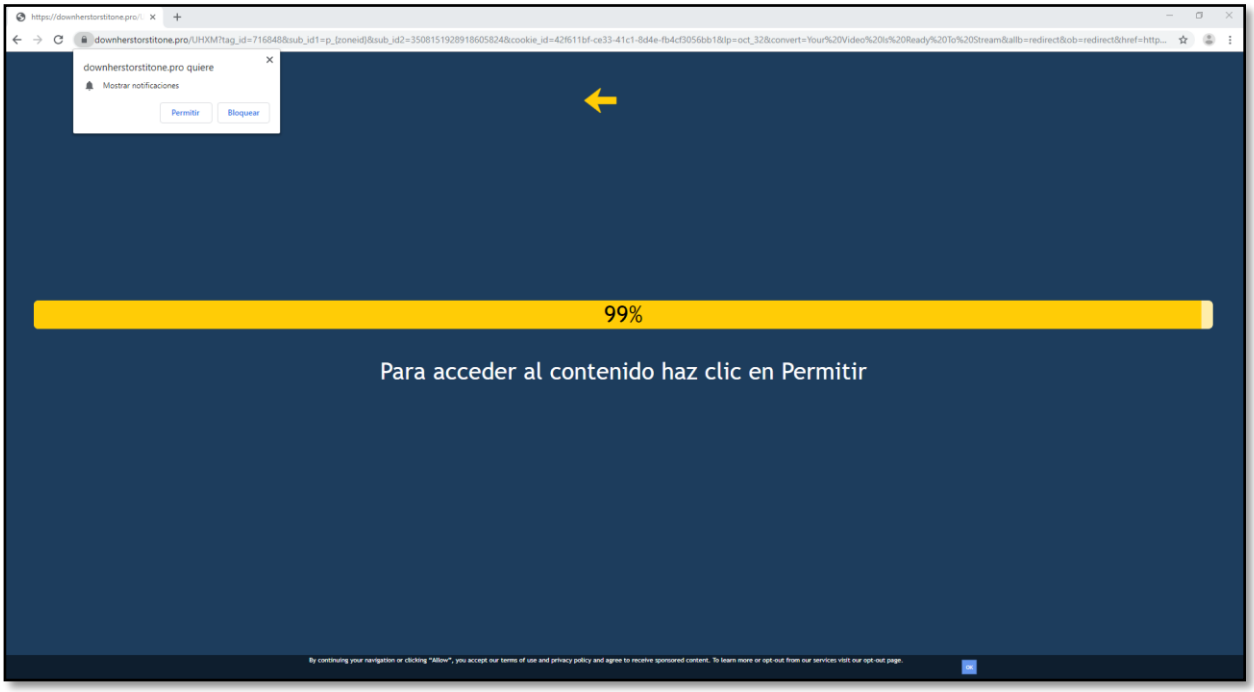
Url's:

Butenlachisbe[.]pro
Nerinlelighda[.]pro
Rephantedditont[.]pro

Imagen Publicidad




herdoperolhan.pro quiere
Mostrar notificaciones
Permitir
Bloquear
Por favor presione el botón para continuar


downherstorstitone.pro quiere
Mostrar notificaciones
Permitir
Bloquear
99%
Para acceder al contenido haz clic en Permitir

Recomendaciones

- Atender a los procesos de instalación, ya que podría estar disponible la opción de “No instalar” el Adware vinculado a la aplicación.
- 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: 2019.08.23 19:50:02 -04'00'