Nuevo ataque **Ransomware SNAKE**

Ransomare SNAKE ha atacado nuevamente en el mes de junio y está vez tuvo como objetivo los sistemas de control industrial de Honda y la división de Enel Argentina.

Descripción

Detectado por primera vez en enero del 2020, SNAKE es un ransomware escrito en código GoLang con un nivel de ofuscación alto que busca comprometer sistemas de control industrial en sistemas operativos windows. Previamente había atacado a Fresenius, el cual es el mayor grupo hospitalario europeo, y en junio reporta ataques a Honda y la división Enel Argentina.

Este nuevo ataque fue dirigido, esto debido a que al ejecutarse de manera controlada una muestra del ransomware se identifica que este busca la IP del dominio mds.honda.com y de no poder encontrarla se cierra.

Publicación:
16/06/2020
Importancia:
Alta
Riesgo de explotación:
Media
Tipo de explotación:
Local

Fuentes:
DigiSOC

Como funciona:

Como todo ransomware cifra los datos del equipo infectado y a través de una nota de rescate pide una remuneración, donde se amenaza con publicar la información sensible en la Deep web de no llevarse a cabo el pago.

-Al iniciarse el ransomware SNAKE este elimina los procesos relacionados con SCADA, sistemas de control y software de administración, entre otros.
-Luego procede a cifrar los archivos en el equipo infectado, omitiendo las carpetas del sistema operativo.
-Finalmente deja la nota de rescate en la ruta C:UsersPublicDesktopFix-Your-Files.txt.

Recomendaciones:

http://	**Nunca abrir enlaces sin verificar** Evite hacer clic en enlaces en correos electrónicos no deseados o en sitios web desconocidos.
	No abrir contenido adjuntos de correos no confiables No abra archivos adjuntos de correo electrónico de remitentes en los que no confía. Mire de quién es el correo electrónico y confirme que la dirección de correo electrónico es correcta
	No conectar dispositivos USB de uso no corporativo Nunca inserte USB u otros dispositivos de almacenamiento de extracción en su computadora si no sabe de dónde provienen.
	Limitar el acceso remoto El acceso remoto a recursos internos de la compañía deben ser estrictamente limitado a lo que el usuario realmente requiera para el desarrollo de sus actividades.
	Copia de seguridad de sus datos Los datos permanecerán seguros si realizas una copia de seguridad de los mismos. Conserva todo lo que has copiado en un disco duro externo, pero asegúrate de no dejarlo conectado al ordenador cuando no lo estés utilizando.
	Cuentas con privilegios No utilizar cuentas con privilegios de administrador. El 86% de las amenazas contra Windows se pueden esquivar en caso de utilizar un usuario común en lugar de un administrador.
	Solo descarga desde sitios de confianza Evita hacer clic en los sitios web desconocidos. Las descargas que se inician al hacer clic en enlaces maliciosos son una forma de infectar el ordenador.
	Mantener actualizados el sistema operativo y aplicativos Mantener el software y el sistema operativo actualizados te ayudará a protegerte del malware. Porque cuando ejecutas una actualización, te aseguras de que te beneficias de los parches de seguridad más recientes, lo que dificulta que los cibercriminales aprovechen las vulnerabilidades de tu software
</>	**Bloqueadores de Javascript** bloquean la ejecución de todo código JavaScript sospechoso de poder dañar el equipo del usuario. Esto ayuda a minimizar la posibilidades de quedar infectado a través de la navegación web.
	Máquinas virtuales Emplear máquinas virtuales para aislar el sistema principal es otra técnica efectiva. En un entorno virtualizado la acción de los ransomware no suele materializarse al confundirlo con herramientas de sandboxing.

Acciones de recuperación ante una infección:

- Pedir ayuda calificada
- Trabajar con expertos
- Aislar la infección
- Cambiar las contraseñas de todos los usuarios
- Revisar todas las conexiones
- Priorizar la recuperación
- No pagar el rescate dado que incentiva y promueve este tipo de campañas.

Indicadores de Compromiso

Ransomware SNAKE

MD5: d659325ea3491708820a2beffe9362b8

SHA256: 09133f977931865425 46f439e518554a5bb17117689c83bc3978cc532ae2f138

MD5:3d1cc4ef33bad0e39c757fce317ef82a

SHA256: e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60

Acciones DigiSOC

El centro de operaciones basado en sus fuentes de inteligencia, mantiene un constante monitoreo de la actividad de fuentes de amenaza y nuevas variantes de ransomware que permiten identificar el accionar de las mismas, haciendo uso de los IoC como parte del servicio de detección y notificación de actividad relacionada.

Red Queen Lab Report | DigiSert | Centro de Investigación e Inteligencia de Amenazas | Digiware

Este comunicado DigiHelp es una alerta de ciberseguridad, incluye información sensible, puede afectar el objetivo del negocio de su compañía. Este contenido que se encuentra en proceso, esta bajo investigación y análisis de las áreas de Digiware, compuestas por DigiSOC, DigiSert y el Centro de investigación e Inteligencia de Amenazas, por lo tanto se desarrollarán << **informes llamados RQL -Red Queen Lab Report** >>, enviados posteriormente por medio de un comunicado oficial.

#Digiware | #DigiwareSuAliado
#DigiwareSecurity | #DigiwareVisionDay