Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

RANSOMWARE QILIN/AGENDA AFECTA A EMPRESAS DE LA REGIÓN

15 / 02 / 2024

CONTENIDO

INTRODUCCIÓN

El grupo de ciberdelincuentes "QiLin" ha hackeado una importante parte de Latinoamérica, comprometiendo información confidencial de varios usuarios. Utilizando tácticas sofisticadas como phishing y ransomware, han accedido a bases de datos sensibles, exponiendo datos personales y financieros. La filtración ha generado preocupación entre los usuarios y destaca la necesidad de invertir en seguridad cibernética y tener planes de contingencia ante tales amenazas.

RANSOMWARE QILIN/AGENDA AFECTA A EMPRESAS DE LA REGIÓN

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2024_02_15_2
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	15/02/2024
Es día cero (0 day):	No

RESUMEN

Recientemente, en países cómo: Brasil, Colombia, Guatemala y México , han sido víctimas hackeos del grupo "QinLin" que ha dejado al descubierto información confidencial de múltiples empresas e instituciones.

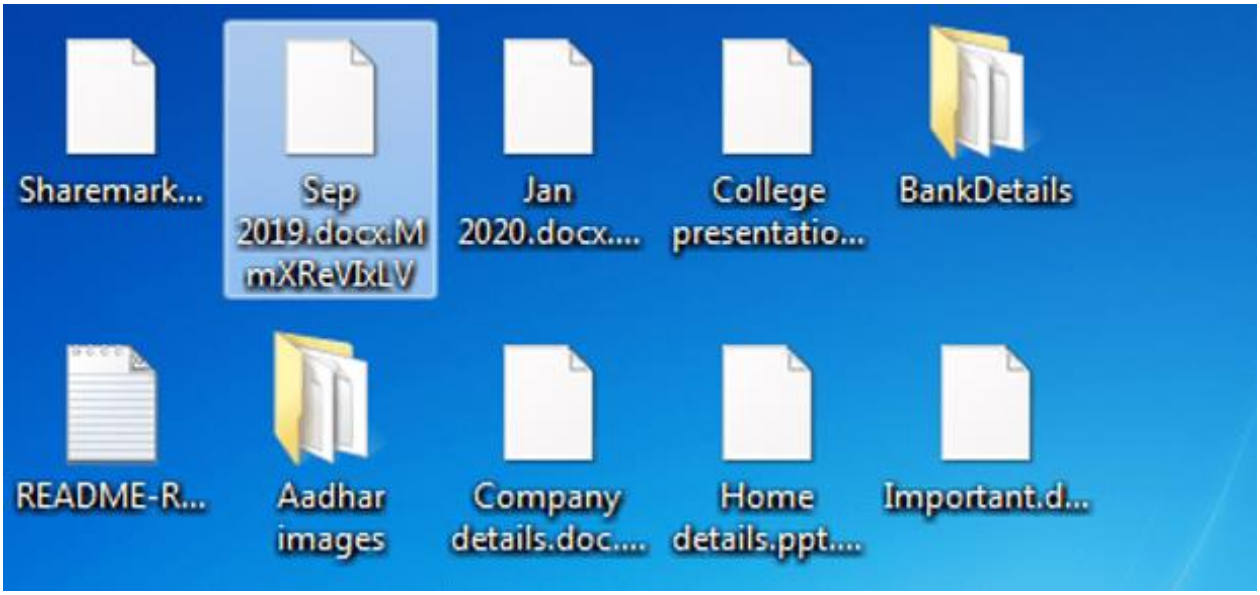
QiLin busca obtener credenciales de administrador para ampliar su acceso y realizar acciones como el robo de datos y el despliegue de ransomware.

QiLin emplea tácticas de phishing, tanto convencional como específico (Spear Phishing), para dirigirse a sus objetivos. Mediante correos electrónicos fraudulentos, incluye enlaces maliciosos que, al ser accionados, inducen a la descarga de software maligno. Este método tiene como propósito infiltrar la red

de la víctima y extraer información confidencial. Una vez que QiLin logra acceder inicialmente, suele desplazarse lateralmente dentro de la infraestructura del objetivo, procurando obtener credenciales de administrador. Antes de implementar el ransomware, procede a exfiltrar los datos obtenidos, y posteriormente lleva a cabo una doble extorsión, presionando a las víctimas para que paguen por el rescate bajo la amenaza de revelar la información comprometida.

El modus operandi de QiLin revela una sofisticación y adaptabilidad excepcionales en el mundo del ransomware.Desde su aparición en agosto de 2022 hasta la fecha, esta amenaza ha perfeccionado su enfoque para maximizar el impacto y asegurar el éxito de sus ataques.

QiLin no se limita simplemente a cifrar archivos; su estrategia implica una infiltración cuidadosa en redes empresariales, el robo de datos valiosos y la propagación lateral antes de desencadenar el ransomware. La obtención de credenciales de administrador es crucial en su proceso, lo que le permite acceder de forma privilegiada y ampliar el alcance de sus acciones.



Después de llevar a cabo los ataques de cifrado y extracción de información clasificada, los ciberdelincuentes publican a sus víctimas en un blog de la red Tor bajo un dominio .onion, exigiendo el rescate y exponiéndolas públicamente a otros posibles compradores de dicha información.

La filtración de datos ha generado preocupación entre los usuarios, quienes temen por la seguridad de su información personal y financiera.

Este hackeo destaca la importancia de invertir en seguridad cibernética y mantener sistemas actualizados.

Las empresas deben estar preparadas de enfrentar amenazas digitales y tener planes de contingencia en caso de un ataque.

En resumen, este incidente es un recordatorio de que ninguna organización está exenta de riesgos cibernéticos, y la seguridad de los datos debe de ser una prioridad constante.

INDICADORES DE COMPROMISO

https://github.com/develgroup/SOC_IOCs/tree/main/20240215_1_QilinRansomware

NOTICIA COMPLETA

https://devel.group/blog/aseguradora-en-guatemala-hackeada-por-grupo-qilin/

CONTACTOS DE SOPORTE

Correo electrónico: cert@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://www.devel.group/reporta-un-incidente