Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

Ataque de Quantum Ransomware en República Dominicana.

25/Agosto/2022

Contenido

INTRODUCCIÓN

En las ultimas horas se ha reportado un ataque exitoso de Quantum Ransomware a una organización gubernamental en República Dominicana, los atacantes piden un alto valor monetario como rescate.

QUANTUM RANSOMWARE

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

ID de alerta:	DSOC-CERT_2022_08_25_01
Clasificación de alerta:	Noticia
Tipo de Impacto:	ALTO
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	08/25/2022
Es día cero (0 day):	No

RESUMEN

El Instituto Agrario Dominicano de República Dominicana sufrió un ataque de ransomware Quantum que cifró múltiples servicios y estaciones de trabajo en toda la agencia gubernamental.

El Instituto Agrario Dominicano (IAD) es parte del Ministerio de Agricultura y es responsable de ejecutar los programas de Reforma Agraria en el país.

Los medios locales informan que el ataque de ransomware ocurrió el 18 de agosto, lo que ha afectado la operación de la agencia.

“Piden más de 600 mil dólares. Nos afectaron cuatro servidores físicos y ocho servidores virtuales, prácticamente todos los servidores”, dijo a medios locales el director de Tecnología del IAD, Walixson Amaury Nuñez .

El Centro Nacional de Ciberseguridad (CNCS), que ha estado ayudando a la agencia a recuperarse del ataque, dice que las direcciones IP de los atacantes eran de EE. UU. y Rusia.

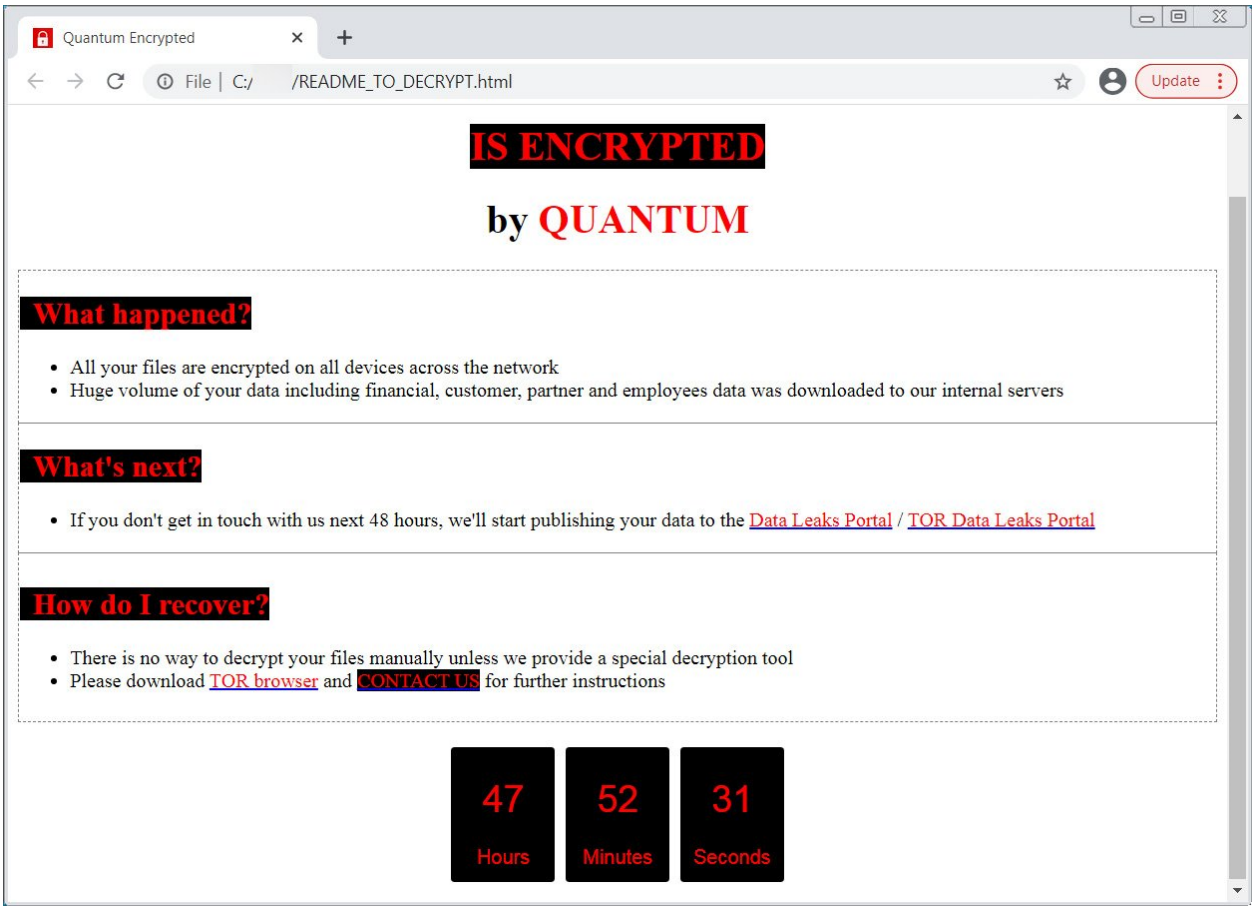
“La información quedó totalmente comprometida, porque se afectaron las bases de datos, aplicaciones, correos, etc.”, aseguró Núñez.

El IAD ha dicho a los medios locales que solo tenían software de seguridad básico en sus sistemas, como antivirus, y carecen de un departamento de seguridad dedicado.

Quantum Ransomware detrás del ataque.

Se rumora que la agencia no pagara el rescate, ya que no tienen los fondos suficientes para cubrir ese gasto y se confirma que Quantum estaba detrás del ataque, que inicialmente exigió un rescate de $ 650,000 de la agencia.

Los actores de amenazas afirmaron haber robado más de 1 TB de datos y amenazaron con liberarlos si IAD no pagaba un rescate públicamente.



Quantum se está convirtiendo en un jugador importante entre las operaciones de ransomware dirigidas a empresas, vinculadas a un ataque a PFC que afectó a más de 650 organizaciones de atención médica.

Se cree que la pandilla de ransomware se convirtió en una rama de la operación de ransomware Conti, que asumió el cambio de marca anterior de la operación de ransomware MountLocker .

MountLocker se implementó por primera vez en ataques que comenzaron en septiembre de 2020, pero se renombró varias veces con varios nombres , incluidos AstroLocker, XingLocker y, finalmente, Quantum.

El cambio de marca a Quantum ocurrió en agosto de 2021, cuando su encriptador de ransomware cambió para agregar la extensión de archivo .quantum a los nombres de los archivos encriptados. Después de eso, sin embargo, el cambio de marca nunca se volvió particularmente activo, con la operación mayormente inactiva.

Eso fue hasta que la operación de ransomware Conti comenzó a cerrarse y sus miembros comenzaron a buscar otras operaciones para infiltrarse.

Según Yelisey Boguslavskiy de Advanced Intel, algunos miembros del sindicato de delitos cibernéticos Conti se unieron a las filas de la operación Quantum, que también vio inmediatamente un aumento en los ataques.

RECOMENDACIONES

- Implemente un plan de recuperación que mantenga y conserve múltiples copias de datos confidenciales o de propiedad y servidores en una ubicación segura, segmentada y separada físicamente (es decir, disco duro, dispositivo de almacenamiento o la nube).

- Implemente la segmentación de la red y mantenga copias de seguridad fuera de línea de los datos para garantizar una interrupción limitada de la organización.

- Realice copias de seguridad de los datos con regularidad y proteja con contraseña las copias de seguridad almacenadas sin conexión. Asegúrese de que las copias de los datos críticos no sean accesibles para su modificación o eliminación desde el sistema donde residen los datos.

- Instale, actualice periódicamente y habilite la detección en tiempo real del software antivirus en todos los hosts.

- Instale actualizaciones para sistemas operativos, software y firmware siempre que estén disponibles y el historial de cambios no indique vulnerabilidades o bugs críticos.

- Revise los controladores de dominio, los servidores, las estaciones de trabajo y los directorios activos en busca de cuentas nuevas o no reconocidas.

- Auditar cuentas de usuario con privilegios administrativos y configurar controles de acceso según el principio de mínimo privilegio.

- Deshabilite los puertos no utilizados.

- Considere agregar un banner de correo electrónico a los correos electrónicos recibidos desde fuera de su organización.

- Hacer cumplir la autenticación multifactor (MFA).

- Considere instalar y usar una red privada virtual (VPN) para establecer conexiones remotas seguras.

- Examine el tráfico de red entrante y saliente, en busca de actividad sospechosa dentro de su red.

- Utilizar escritorio remoto solo cuando es necesario

Noticia Completa

https://devel.group/actualizaciones-de-seguridad-de-apple-corrigen-2-dias-cero-utilizados-para-hackear-iphones-macs/

Visualizar IOC's

https://github.com/develgroup/SOC_IOCs/tree/main/20220506_02_QuantumRansomware

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