Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

DARK POWER, NUEVO RANSOMWARE ACTIVO.

30/Marzo/2023

CONTENIDO

INTRODUCCIÓN

Ha aparecido una nueva operación de ransomware llamado “Dark Power”, y ya ha enumerado a sus primeras víctimas en un sitio de fuga de datos de la dark web, amenazando con publicar los datos si no se paga un rescate.

El cifrador de la banda de ransomware tiene una fecha de compilación del 29 de enero de 2023, cuando comenzaron los ataques. Además, la operación aún no se ha promocionado en ningún foro de crackers o espacio web; por lo tanto, es probable que sea un proyecto privado.

DARK POWER, NUEVO RANSOMWARE ACTIVO.

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

ID de alerta:	DSOC-CERT_2023_03_30_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	30/03/2023
Es día cero (0 day):	No

RESUMEN

Ha aparecido una nueva operación de ransomware llamada 'Dark Power', y ya ha enumerado a sus primeras víctimas en un sitio de fuga de datos de la dark web, amenazando con publicar los datos si no se paga un rescate.

Además, la operación aún no se ha promocionado en ningún foro de hackers o espacio web oscuro; por lo tanto, es probable que sea un proyecto privado.

PROCESO DEL RANSOMWARE.

Tras la ejecución inicial, el ransomware crea una cadena ASCII aleatoria de 64 caracteres para inicializar el algoritmo de cifrado con una clave única en cada ejecución.

Luego, el ransomware finaliza servicios y procesos específicos en la máquina de la víctima para liberar archivos y minimizar las posibilidades de que algo bloquee el proceso de cifrado de archivos.

Durante esa etapa, el ransomware también detiene el Servicio de instantáneas de volumen (VSS), los servicios de respaldo de datos y los productos antimalware en su lista codificada.

Después de eliminar todos los servicios anteriores, el ransomware «duerme» durante 30 segundos y borra los registros de la consola y del sistema de Windows para evitar el análisis por parte de expertos en recuperación de datos.

El cifrado utiliza AES (modo CRT) y la cadena ASCII generada al iniciarse. Los archivos resultantes se renombran con la extensión «.dark_power».

PROCESO DE INFECCIÓN.

Si un usuario desprevenido abre el archivo adjunto HTML o PDF recibido en su bandeja de correo electrónico no deseado, este documento malicioso efectuará una comprobación verificando que fue abierto en un dispositivo de escritorio para posteriormente establecer una comunicación con su servidor remoto y descargar un archivo comprimido en RAR o ZIP, iniciando con ello el proceso de infección.

Adicionalmente al descomprimir y ejecutar este archivo se cargan dos certificados de validación falsos que contienen las cargas útiles maliciosas, una es el troyano Mispadu y el otro un instalador de AutoIT que tiene como función principal decodificar y ejecutar el troyano haciendo uso de la línea de comandos certutil legítima de Windows.


WHATS HAPPEN?
Your files are encrypted, and currently unavailable.
you can check it:
all files in backup is deleted . your outlook server and databases have been encrypted By the way, everything is possible to recover (restore), but you need to follow our instructions.
Otherwise, you can't return your data (NEVER).


HOW TO RETRIEVE FILES
1
send 10K $ to this address (XMR) :
85D16UodGeva
2
You have to download qTox chat in your PC For PC: https://qtox.github.io
TOX
3
Create a new chat and write down our qTox ID:
EBBB598994
ID
4
To know who you are just tell us the name of your company
5
Visit our tor website : powerj
.onion

VICTIMAS Y ACTIVIDAD.

Trellix informa que ha visto diez víctimas de los EE.UU., Francia, Israel, Turquía, la República Checa, Argelia, Egipto y Perú, por lo que el alcance de la orientación es global.

El grupo Dark Power afirma haber robado datos de las redes de estas organizaciones y amenaza con publicarlos si no pagan el rescate, por lo que es un grupo más de doble extorsión.

LAS MEJORES PRÁCTICAS INDICAN NO PAGAR RESCATE.

Organizaciones como CISA, NCSC, FBI y HHS advierten a las víctimas de ransomware que no paguen un rescate, en parte porque el pago no garantiza que se recuperarán los archivos. De acuerdo con un aviso de la Oficina de Control de Activos Extranjeros (OFAC) del Departamento del Tesoro de EE. UU ., los pagos de rescate también pueden animar a los adversarios a apuntar a organizaciones adicionales, alentar a otros actores criminales a distribuir ransomware y/o financiar actividades ilícitas que podrían ser potencialmente ilegales.

El lenguaje elegido por los autores de malware muestra que los atacantes están mejorando sus enfoques de defensa para expandir sus actividades maliciosas. Dado que el ransomware Dark Power se dirige agresivamente a organizaciones de todo el mundo, se recomienda tener la postura de seguridad adecuada para vencer el ataque en la etapa inicial. Además, los IOC que incluyen firmas, hash y direcciones URL maliciosas se pueden aprovechar para comprender el patrón de ataque del ransomware.

INDICADORES DE COMPROMISO

INDICADORES DE COMPROMISO.

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