Ransomware NetWalker: análisis y medidas preventivas

incibe-cert.es/blog/ransomware-netwalker-analisis-y-medidas-preventivas

April 8, 2020

Como ya se expuso en otros artículos sobre el *ransomware*, estos ciberataques han alcanzado el primer puesto en importancia para usuarios y compañías, no tanto por el número de ataques en sí (en algunos casos sí pueden resultar masivos), sino por el gran beneficio económico que se obtiene con esta práctica, causando la aparición de muchos grupos especializados en su desarrollo, así como por el daño reputacional que supone para la víctima.

El objetivo de este post es aportar información sobre el *ransomware* NetWalker, también denominado Mailto o Koko, que se ha utilizado en una reciente campaña de *malware* distribuida bajo correos electrónicos que simulan aportar información sobre el estado de la actual situación de alerta sanitaria generada por el COVID-19.

Modelo de negocio RaaS

Antes de entrar en detalles técnicos, conviene entender el modelo negocio de los actores responsables de NetWalker. La amenaza comienza a operar en septiembre de 2019, pero no es hasta el 19 de marzo de 2020 cuando el usuario con el alias Bugatti abría la oportunidad a otros cibercriminales de unirse al grupo como parte de un modelo de negocio RaaS (*Ransomware as a Service*):

- Figura 1: Condiciones para unirse a NetWalker. Fuente: El Mundo -

Su correspondiente traducción al castellano es:

```
[SOCIO] Netwalker Ransomware
Abrimos un conjunto de anuncios para procesar redes y spam.
Interesados en personas que trabajen por la calidad, no por la cantidad.
Damos preferencia a aquellos que puedan trabajar con grandes redes y tener su propio
material.
Reclutamos un número limitado de socios y dejamos de reclutar hasta que queden
vacantes.
Le ofrecemos un ransomware rápido y flexible, un panel de administración en TOR y
servicio automático.
Acceso al servicio mediante archivos de cifrado desde AV.
Para anuncios verificados, entregamos material preparado (IP \ cuenta del dominio
admin \ acceso a NAS \ información sobre AV \ nombre de la organización \ ingresos)
para el procesamiento de redes.
El ransomware ha estado funcionando desde septiembre de 2019 y ha demostrado ser
bueno, no se puede descifrar.
Recibirá toda la información detallada sobre el ransomware y las condiciones de
trabajo después de compilar la aplicación en el mensaje privado.
Formulario de solicitud:
1) ¿En qué dirección estás trabajando?
2) Experiencia. ¿Con qué programas de afiliación ya trabajó y cuál fue su beneficio?
3) ¿Cuánto material tiene y cuándo está listo para comenzar, cuánto planea procesar
el material?
```

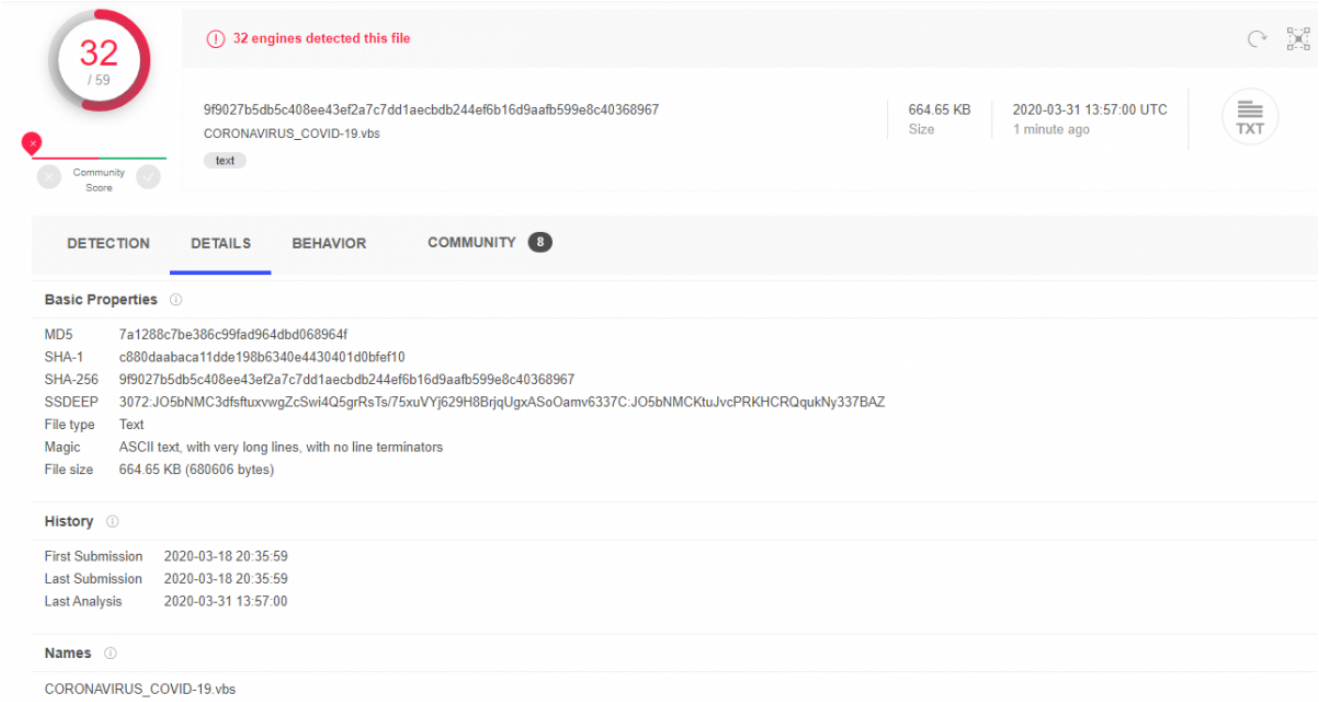
En un artículo del 18 de marzo en el portal BleepingComputer, se preguntaba a los operadores responsables de NetWalker si atacarían hospitales, y ellos respondieron lo siguiente, dejando claro que no son su objetivo:

```
"Hospitals and medical facilities? Do you think someone has a goal to attack
hospitals? We don't have that goal - it never was. It coincidence. No one will
purposefully hack into the hospital."
```

Análisis de archivos asociados

La muestra de *ransomware* NetWalker analizada ha sido distribuida utilizando un *dropper* desarrollado en Visual Basic Script (VBS), que se incluye como fichero adjunto en la campaña de spam. Es un *ransomware* de cifrado (*encrypting ransomware*), es decir, impide el acceso a los datos del usuario cifrando los archivos del dispositivo, aunque se mantiene el acceso al mismo.

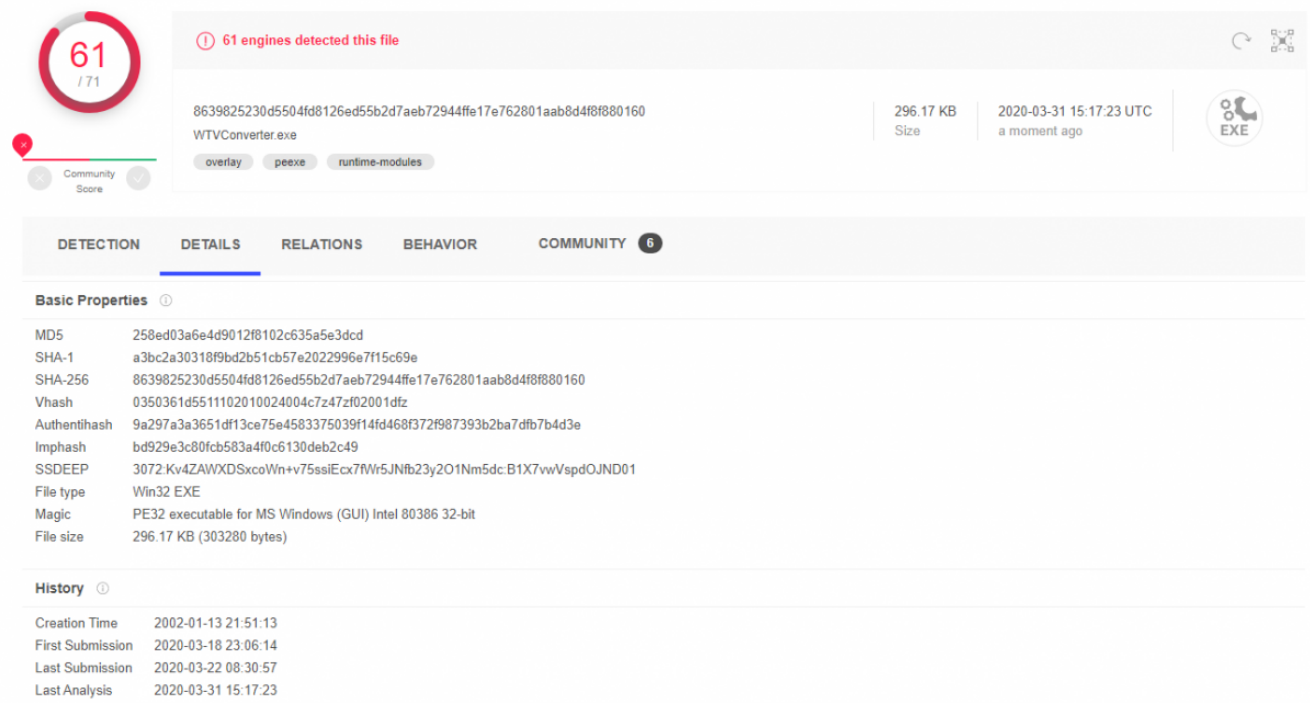
El 18 de marzo de este año se analizó, por primera vez, el archivo *CORONAVIRUS_COVID-19.vbs* en la herramienta VirusTotal y, a fecha de 31 de marzo, 32 de los 59 motores antivirus que gestiona VT han clasificado la muestra como maliciosa, tal y como se aprecia en la siguiente imagen:



- Figura 2: Análisis de VirusTotal para CORONAVIRUS_COVID-19.vbs -

En la Figura 2, se pueden identificar los distintos códigos hash (MD5, SHA-1 y SHA-256) asociados al *dropper*.

Este archivo *dropper* contiene, a su vez, un binario embebido, ejecutable para sistemas Windows, que tiene varios alias (*WTVConverter.exe*, *qesw.exe* y *qeSw.exe*) y cuyo análisis para VirusTotal puede verse a continuación:



- Figura 3: Análisis de VirusTotal para qeSw.exe -

La ejecución del *ransomware* NetWalker se divide en cuatro fases:

1. El código malicioso importa las funciones de las librerías de Windows que usará durante el resto de la ejecución.
2. El fichero de configuración del *ransomware*, donde se encuentran diversos parámetros relativos al cifrado y rescate, se extrae de los recursos del ejecutable.
3. Inicialización de variables, tales como el identificador del usuario afectado.
4. Procedimiento principal donde se llevaría a cabo el proceso de cifrado de archivos.

Antes de proceder al cifrado, se eliminarán las *shadow copies* (instantáneas de volumen) ejecutando vssadmin.exe en una ventana oculta, con el objetivo de impedir que se puedan recuperar los ficheros cifrados desde la copia de seguridad generada por el servicio VSS (*Volume Shadow Copy*):

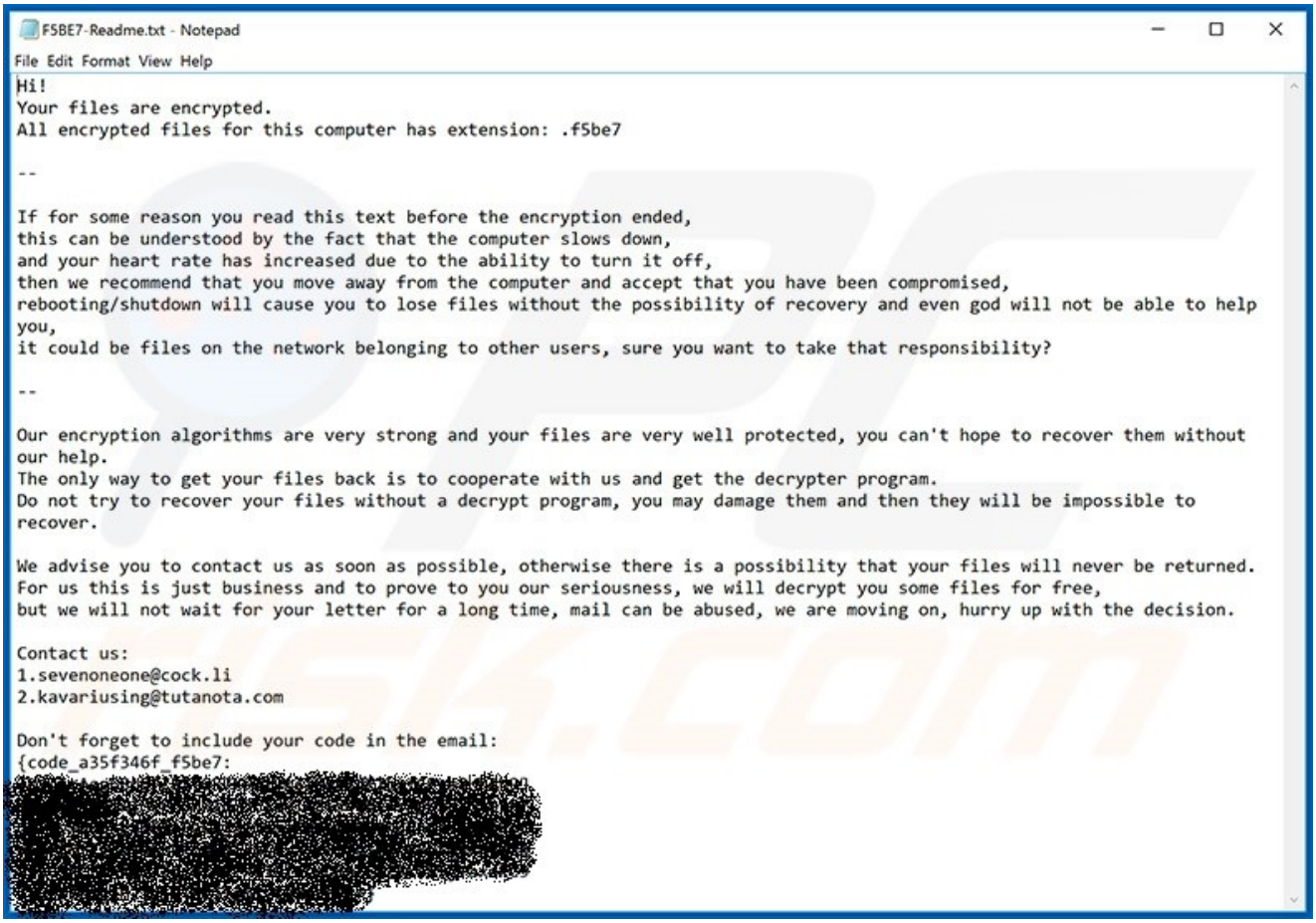
```
<SYSTEM32>\vssadmin.exe delete shadows /all /quiet
```

El proceso de cifrado genera un identificador único de 6 caracteres (ID del usuario afectado) que utiliza como extensión para los archivos cifrados y como parte del nombre de las notas de rescate:

```
Nombre original: file93.docx
Nombre tras el cifrado: file93.docx.46X19p
Nota de rescate generada en la misma ruta "46X19p-readme.txt"
```

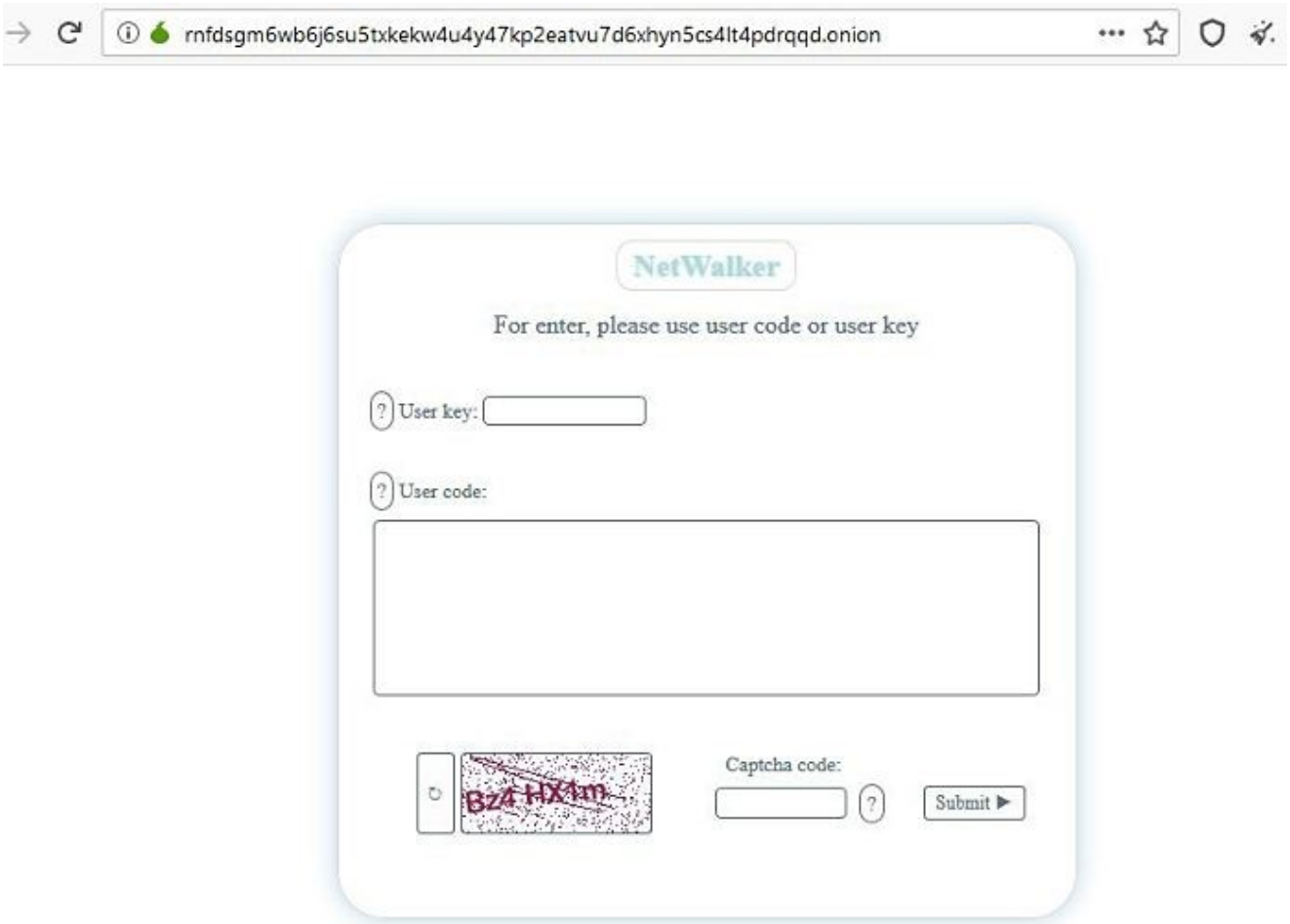
Instrucciones de rescate

Cuando un equipo se ve afectado por el *ransomware* NetWalker, las instrucciones para descifrar los ficheros se muestran a continuación:



- Figura 4: Nota de rescate de NetWalker. Fuente: PCrisk -

En esta nota se pide la instalación de Tor Browser, se facilita el sitio web accesible desde la red TOR, así como el código personal de la víctima de NetWalker, que debe introducir en la siguiente web:



- Figura 5: Portal de pago accesible desde la red TOR. Fuente: El Mundo -

Una vez que se ha identificado el usuario, se indica que el precio inicial del rescate comienza en 1.000 dólares, pero que se duplicará esa cantidad de no realizarse el pago antes de una semana. La dirección que se proporciona para el pago es única para cada infección.

Persistencia

Analizando el *modus operandi* de NetWalker, y dada la naturaleza de su código, no intenta establecer persistencia en el sistema afectado, tampoco realiza propagación lateral, ni se aprecia tráfico de red hacia otras máquinas. Además, el ejecutable responsable del cifrado se autoelimina tras finalizar su ejecución.

Recuperación

La primera y principal recomendación que se realiza en los casos de *ransomware* es **no pagar nunca el rescate** solicitado por los ciberdelincuentes, ya que esto no garantiza que respondan una vez se realice el pago, para devolver la normalidad al equipo infectado mediante la entrega de la clave de descifrado.

Desafortunadamente, en este momento no se conoce ninguna solución de descifrado de este *ransomware*, por lo que deben considerarse las siguientes medidas de carácter general:

- Aislar el equipo de la red para evitar que el ciberataque se propague a otros dispositivos, teniendo en cuenta discos duros, unidades de red o servicios en la nube que estuvieran conectados.
- Clonar de manera completa el disco duro para conservar el dispositivo original y, de esta manera, intentar recuperar los datos sobre el disco clonado. Si no existe solución actualmente, como es en el caso de NetWalker, es posible que se desarrolle en el futuro, por lo que se podrían recuperar los ficheros cifrados.
- Desinfectar el disco clonado para intentar recuperar los datos posteriormente, utilizando una herramienta adecuada.
- Por último, una vez confirmado que el *malware* ha sido eliminado del ordenador, se recomienda cambiar todas las contraseñas que se hayan usado en el equipo afectado.

Medidas preventivas y de protección

Dentro de las medidas de prevención a adoptar, es muy importante puntualizar lo siguiente:

- No descargar archivos sospechosos o de un remitente desconocido o no habitual.
- Realizar *backups* periódicamente para que se puedan restablecer los sistemas rápidamente, con la menor pérdida de información y el menor impacto en la operativa posibles.
- Mejorar la segmentación de la red para evitar una propagación masiva de la amenaza.
- Revisar y reforzar, en caso de que sea necesario, las políticas de seguridad de la organización.
- **Nunca se debe pagar el rescate**, se debe comunicar el incidente a través del CSIRT (*Computer Security Incident Response Team*) de referencia.

Conclusiones

NetWalker es un *ransomware* relativamente reciente (septiembre 2019) que ha evolucionado en los últimos meses, aunque hasta el momento no hay evidencias de víctimas afectadas o que sufrieran las consecuencias.

También cabe destacar que, aunque se ha intentado aprovechar la situación de alarma generada por el COVID-19, los propios creadores del *ransomware* han manifestado claramente que los hospitales no son el objetivo.