Identificador
[colCERT AD-0519-005]

19/05/2022

Advertencia de Seguridad Digital

[TLP: WHITE]
[PAP: WHITE]

Ransomware Vice Society viene realizando campañas de afectación a entidades privadas y gubernamentales de Colombia.

Contexto

Día a día los atacantes en la internet realizan ejercicios de reconocimiento hacia portales web para encontrar brechas de seguridad en donde puedan explotar vulnerabilidades ya sean conocidas o zero-day. A través de las últimas investigaciones y reportes, se ha evidenciado un aumento en el uso del software malicioso tipo Ransomware para comprometer activos confidenciales de la entidad e información suministrada por clientes, proveedores y usuarios. En esta ocasión se presenta el modo de operar del Ransomware ***Vice Society*** y cómo viene afectando a Europa y a LATAM.

Contexto histórico

La primera evidencia de este Ransomware se remonta hacia finales del 2021, la tienda Spar de Reino Unido informa acerca de cierre de varias de sus sucursales debido a un ataque a sus sistemas IT, dentro de las afectaciones más significativas es la imposibilidad de procesamiento de pagos a través de tarjetas de crédito.

Según investigaciones realizadas , se ha podido establecer que hay una alta probabilidad que Vice Society sea un derivado del conocido HelloKitty, dadas sus similitudes en funcionalidades y operaciones.

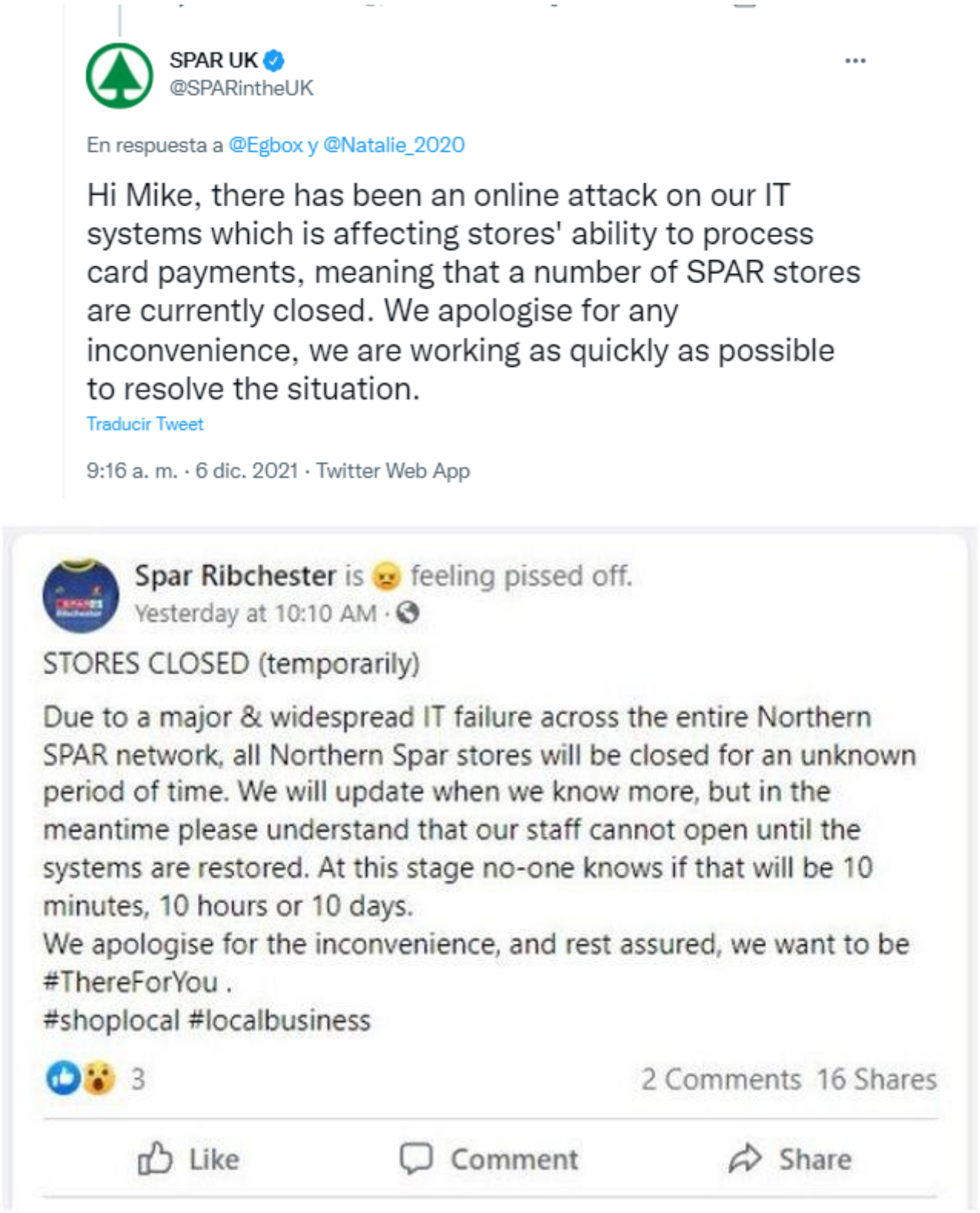

Figura No. 1. *Spar informa acerca de ataque digital.* ***Fuente:*** *Twitter.*

Ataque doxing

Los antecedentes característicos manifiestan que ***Vice Society*** opera en ataque de doxing o doble extorsión, en donde exfiltra datos para exponerlos en foros clandestinos y luego los cifra para impedir el acceso a estos a no ser que se pague el rescate pactado.

Vice Society enfoca sus esfuerzos de ataque hacia proveedores de salud pública como Junta de Salud del Distrito de Waikato de Nueva Zelanda y Eskenazi Health en Indiana, EE.UU. El catálogo es amplio ya que las organizaciones afectadas son de todos los sectores económicos, políticos e industriales de una nación. Este tipo de extorsiones como el doxing ha incrementado el número de víctimas de 300 a 1,000 en un mes.

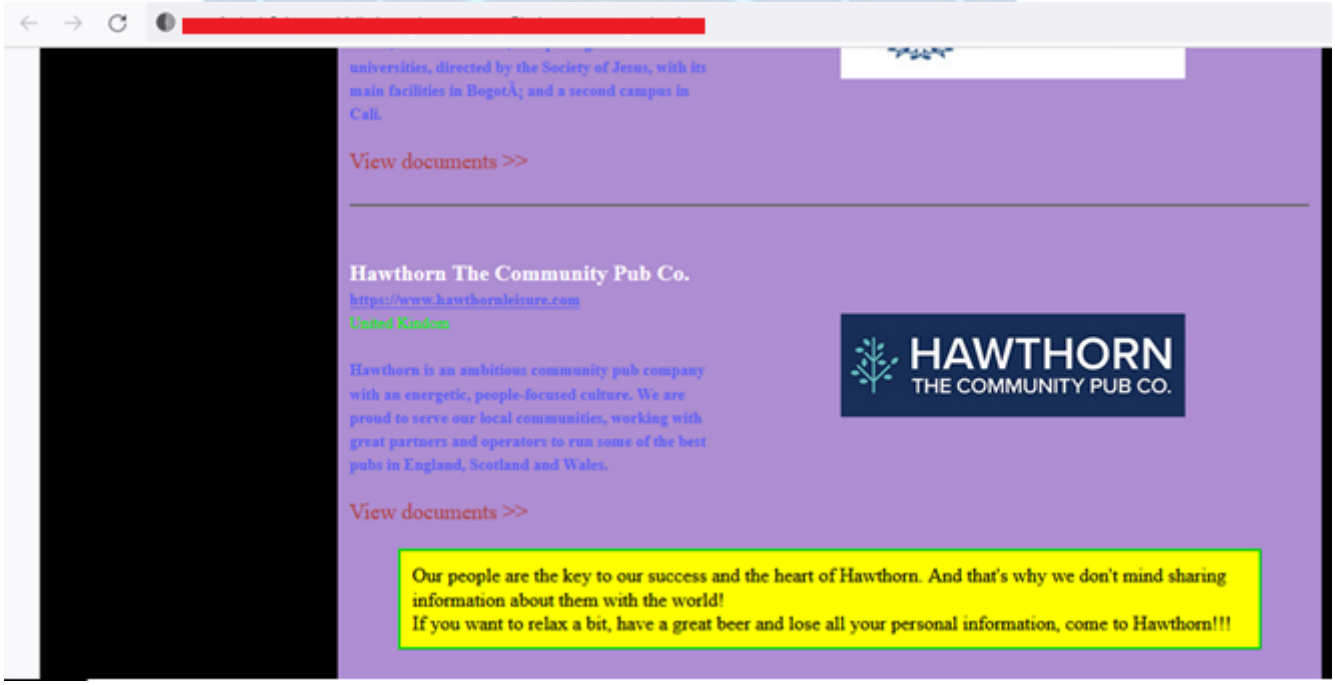

Figura No 2. *Blog de Vice Society.*

Luego de exfiltrar la información de la entidad y cifrarla, **Vice Scociety** deja una nota de rescate anunciando que se tiene un plazo de 7 días para pagar el rescate. Para demostrar su pericia y el poder para descifrar la información, solicitan a la víctima remitan dos de los archivos cifrados que desofuscarán con las herramientas y llave privadas. La extensión característica de este Ransomware es *v-society.[victim's_ID]*

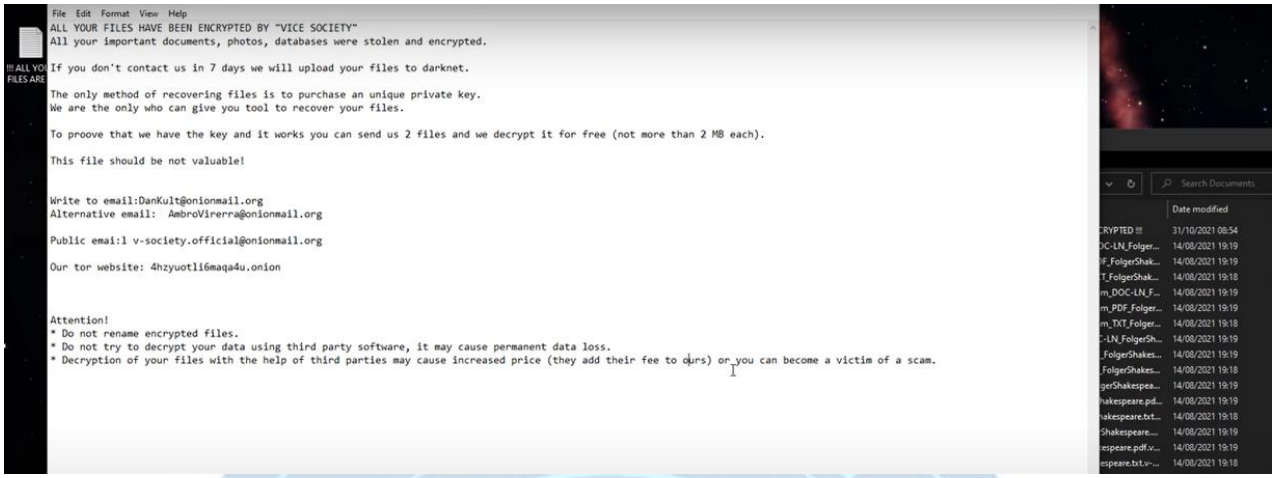

Figura No 3. *Nota de rescate con instrucciones de Vice Society.*

Vector de infección

Dentro de los posibles vectores de infección se encuentran:

- Explotación de vulnerabilidades conocidas y zero-day.
- Ataque directamente sobre protocolos como RDP o Telnet.
- Envío de adjuntos y/o enlaces maliciosos como cebo para las víctimas.
- Descarga de software de sitios de terceros o no oficiales.

Principales afectaciones

- Movimiento lateral.
- Escalado de privilegios.
- Ejecución de malware.
- Exfiltración de datos.
- Cifrado de la información.
- Logra persistencia a través de servicios legítimos.
- Exposición de los datos exfiltrados.

Establecimiento de persistencia (parámetros a observar)

Uno de los objetivos más perseguidos por los atacantes es convivir dentro del sistema vulnerado sin ser detectado, crea entonces sus propios procesos, rutas, directorios o inclusive modifica claves de registro y servicios para persistir y continuar perjudicando la infraestructura sin que la entidad se percate de esto.

Es de vital importancia monitorear constantemente las rutas y claves de registro en donde se puede alojar el software malicioso. Según la arquitectura de sistemas operativos, las claves de registro más atacadas son las que poseen permisos de administrador como las LOCAL MACHINE y las de usuario como CURRENT USER, es por ello que se debe prestar especial atención a estas claves.

Verifique que los procesos sospechosos con nombres anómalos o diferentes.

HKEY_CURRENT_USER\Software\[Ransomware]\Paths
HKEY_CURRENT_USER\Software\[Ransomware]\Paths\0

Creación de procesos
HKEY_CURRENT_USER\Software\[Ransomware]\Process
HKEY_CURRENT_USER\Software\[Ransomware]

Monitoreo de lo registrado en el teclado, audio o cámara para almacenar esta actividad en archivos remitidos a C2
HKEY_CURRENT_USER\Software\[Ransomware]\\Log
HKEY_CURRENT_USER\Software\[Ransomware]\\Log\0

Un programa puede simular ser uno legítimo para ejecutarse constantemente cuando es solicitado, de esta manera el malware hace su propia monitorización dentro del sistema al suplantar un servicio que comúnmente se usa
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\Debug\ExceptionRecord

Dentro de los primeros pasos del ransomware es el de eliminar copias de seguridad o backups almacenados en el mismo sistema vulnerado, los comandos ejecutados a nivel de consola o línea de comandos son los siguientes:

C:\Windows\system32\cmd.exe" /C wmic shadowcopy delete
C:\Windows\system32\cmd.exe" /C vssadmin delete shadows /all /quiet

Los CVE que explota para realizar el movimiento lateral a través de las redes son la CVE-2021-1675 y CVE-2021-34527

Recomendaciones de prevención:

- Siempre tenga a la mano copias de seguridad por lo menos 3 off-site y en la nube, manténgalas actualizadas periódicamente. En lo posible que esto sea un procedimiento documentado.
- Mantenga actualizados con los últimos parches el sistema operativo, aplicaciones y software empleado en la entidad.
- Realice capacitaciones orientados a los funcionarios para dar a conocer los últimos vectores de ataque empleados por los atacantes.
- Realice jornadas de auditoría a sus aplicativos webs para encontrar vulnerabilidades, mitíguelas inmediatamente al evidenciarlas.
- No abra correos de procedencia sospechosa o que no ha solicitado, no ejecute adjuntos ni enlaces embebidos en el mensaje de correo electrónico.
- Bloquee sitios emergentes o sitios web catalogados como maliciosos.
- Deshabilite el protocolo RDP si no lo usa, los atacantes usan a menudo este protocolo para su ejecución remota.
- Implemente el uso de VPN (Red virtual privada).
- Identifique sus activos críticos y determine el impacto de llegarse a materializar un ataque.

- Identifique archivos DLL o PE que sean anómalos o desconocidos.
- Supervise procesos que puede abusar del Shell de comandos de Windows y restrinja permisos elevados solo a personal administrativo.
- Si está en sus posibilidades, restrinja las comunicaciones de uso compartido de archivos como SMB.
- Utilice contraseñas robustas, largas y complejas, al igual que cámbielas periódicamente.
- ¡No pague el rescate! Esto patrocina las acciones delictivas de los atacantes y no garantiza la devolución de la información.

Recomendaciones de respuesta a un indicente de ransomware:

- Si ha sido víctima de ransomware y desea restaurar los archivos en un backup, escanee el backup para encontrar posibles rastros del malware, ya que el ransomware puede estar infiltrado en su red por un cierto tiempo, hallar los backups almacenados en el sistema e infectarlos.
- Desconecte ya sea de manera física o inalámbrica los dispositivos y equipos afectados.
- Inclusive apague su wifi, desconecte switches y el proveedor de internet.
- Resetee credenciales de usuarios, sobre todo de administradores.
- Reconecte los equipos a una red limpia para realizar la reinstalación de aplicativos y sistema operativo.
- Monitorice con su antivirus de preferencia nuevamente el sistema para asegurarse de que no exista rastro del ransomware ni de sus mecanismos de persistencia.
- Implemente un plan de Recuperación ante desastres DRP.

Referencias

- Twitter.
- MITRE ATT&CK.

Canales de Atención

Si tiene alguna consulta técnica, puede comunicarse con CSIRT Gobierno de tratarse de una entidad del Estado, o con ColCERT si pertenece a cualquier otro sector de la economía, a través de los siguientes canales:

Bogotá: +57 601 344 22 22
Línea Gratuita Nacional: 018000952525 Opción 2

contacto@colcert.gov.co,
csirtgob@mintic.gov.co

@colCERT