Fecha: 18/2/2022

Reporte de incidente: 14-01-2022 8:15

Incidente resuelto: 26-01-2022

## Resumen de análisis de impacto de ataque Ramsomware

## Deteccion

El día 18-1-2022 Roman Cottone reporto que no se podía acceder al sistema SIGA, Leandro Ortiz procede a recibir y validar el incidente encontrando en todos los servidores lo siguiente:

Interfaz de usuario gráfica, Sitio web

Descripción generada automáticamente

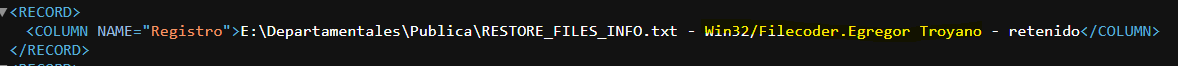
Muestra del inicio sesión servidor

Todos los recursos alojados en el Datacenter de Bogotá 166 quedaron inaccesibles.

Algunos sistemas como SIGA o ACQUA respondían PING ICMP, pero el acceso era denegado.

El análisis de los servidores arrojo que los accesos habían sido cifrados por un ransoware, como así también toda información dentro de los servidores, y algunos sistemas habían sido comprometidos y modificada su configuración.

Un análisis posterior revelo que los atacantes explotaron una vulnerabilidad en los equipos de los usuarios, para luego disparar una ejecución remota de código a los servidores el cual proveyó acceso remoto a los atacantes quienes robaron una clave de administrador para luego desactivar las políticas de seguridad del firewall de borde.



Muestra de registros Anti-Virus.

## Síntomas

Lista de los sistemas afectados por el ataque.

|  |  |  |  |
| --- | --- | --- | --- |
| **Dsipositivo** | **Función** | **Serveridad** | **Impacto en opración** |
| ESXI-MS | Servidor principal | Critica | Acceso denegado, no acceso a otros servidores. |
| SIGA-VM | Sistema de acreditaciones | Critica | Las acreditaciones no pueden ser procesadas. |
| ACQUA-VM | Sistema de administración | Critica | Facturación, Recibos etc.. |
| FS-VM | Sistema de archivos general | Media | Información general, carreras, contratos. |
| AD-V | Sistema de autenticación y gestión de usuarios. | Critica | Gestión de cuentas, contraseñas, accesos y permisos. |
| BKP-SVR | Servidor repositorio de copias de seguridad | Critica | Información y accesos cifrados. |
| Firewall | Sistema de control de red | Critica | Se desactivaron las barreas de seguridad de la red. |

## Resolución

Acciones Inmediatas

Debido a que todos los sistemas estaban comprometidos se tomaron los siguientes pasos:

1. Aislamiento de red para todos los servidores afectados.
2. Montado de servidor físico alternativo.
3. Descifrado de toda información comprometida y análisis de amenazas de la información recuperada.
4. Migración de base de datos recuperadas.
5. Reinstalación de todos los sistemas principales de servidores en versiones actualizadas y licenciadas (versiones 2019), configuración de dependencias para otros sistemas.
6. Creación de un nuevo dominio de Windows Server y migración de dispositivos de usuarios al nuevo entorno.
7. Revisión y configuración de firewall.
8. Segmentación de red para datos de servidores.
9. Reconfiguración de copias de seguridad.

Acciones posteriores

Luego de recuperar la operatividad en todos los Servidores procedimos a realizar las siguientes acciones preventivas:

1. Reposición del servidor físico. Debido a la antigüedad y características del servidor donde alojábamos virtualmente todos los servidores con tecnología ESXI de VmWare, procedimos a adquirir un nuevo servidor que nos permita tener las ultimas actualización de sistema y seguridad del entorno de virtualización.
2. Revisión y actualización de sistema Antivirus en todos los dispositivos de usuarios.
3. Inicio de recambio y licenciamiento en dispositivos de usuarios obsoletos por antigüedad.
4. Aumento de políticas de restricción de red y aplicaciones.
5. Implementación de un tercer método de backup utilizando el servicio en la nube de Microsoft Azure.

## Cambios de Hardware

SERVIDOR FISICO

Antes del ataque:

Servidor clon con procesador i7 4470 (4ta generación), 4TB, 32 Gb Ram DDR3 1333Mhz.

Actual:

Servidor Lenovo Thinksystem SR530 con procesador Intel Xeon 3204 Bronze, 8TB, 32 Gb Ram TruDDR4 2933Mhz.

DISPOSITIVOS DE USUARIOS (Notebook y Pc escritorio)

Iniciamos un cambio progresivo en el cual renovaremos y licenciaremos todos los dispositivos de usuarios que no cumplan los requisitos mínimos de seguridad y actualizaciones.

Quedan comprendidos todos aquellos dispositivos que por antigüedad o características de Hardware no puedan operar bajo Windows 10 o posterior.

Recomendamos como estándar mínimo los siguientes requisitos:

* Procesador Intel i5 (10 Generación) o equivalente
* 8gb Ram DDR4
* Disco SSD 240Gb
* Windows 10 Pro

## Hallazgos

Mediante la descarga de software malicioso (troyano) a un equipo de un usuario, un atacante pudo infiltrarse en los servidores, que luego robo una clave de administrador para comprometer la red completa.

El software malicioso pudo ejecutarse por una vulnerabilidad sin resolver debido a que el equipo no estaba licenciado para descarga actualizaciones de seguridad importantes.

El atacante utiliza un ransomware (egregor) para cifrar toda la información de todos los servidores.

Egregor es un Ransomware-as-a-Service (**RaaS**) que implementa técnicas de anti-análisis, como la ofuscación de código y cifrados de carga útil. En una de sus etapas de ejecución la carga útil sólo se puede descifrar si se proporciona la clave correcta en la línea de comando del proceso. Egregor puede recibir parámetros adicionales a través de la línea de comandos. También, a los archivos encriptados agrega una cadena o caracteres aleatorios como la nueva extensión, por ejemplo, a un archivo llamado «**imagen.jpg**» lo cambia por «**imagen.jpg.ACTC**«.

Utiliza un esquema de cifrado de archivos híbrido basado en el cifrado de flujo ChaCha y el cifrado asimétrico RSA. La clave pública maestra RSA-2048 de los delincuentes está incrustada en el cuerpo del troyano. Para cada archivo de datos que procesa Egregor, genera una nueva clave ChaCha de 256 bits y un nonce de 64 bits, cifra el contenido del archivo por ChaCha, luego los cifra usando la clave pública RSA de la sesión y los guarda junto con alguna información auxiliar al final del archivo cifrado. De igual forma, crea el archivo de texto de rescate «**RECOVER-FILES.txt**» en todas las carpetas que contienen archivos encriptados.

## Acciones para realizar

* Se recomienda cambio de firewall.
* Licenciar equipos de usuarios o servidores que no tengan licencia.
* Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.
* Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.
* Generar una regla personalizada para bloqueos de IOC’s en perfiles entrantes perimetrales.
* Aumentar la protección en el protocolo RDP, deshabilitando los servicios RDP y demás servicios si no son utilizados, para reducir su exposición a las vulnerabilidades. Si no es posible cerrarlos, limite las direcciones de origen que pueden acceder a los puertos.
* Bloquear bidireccionalmente el puerto TCP 3389 o hacerlo accesible sólo a través de una VPN privada. Además, prestar atención sobre el tráfico sospechoso que tengan conexiones a los puertos 135TCP/UDP y 445TCP/UDP.
* El software y sistema operativo instalados debe actualizarse con herramientas y/o funciones implementadas proporcionadas por sus desarrolladores oficiales. No se deben utilizar otras herramientas de activación y/o actualización de terceros ni para activar o actualizar ningún software instalado.
* Escanear regularmente los equipos en busca de amenazas con un antivirus o un paquete anti-spyware de buena reputación y considerar aumentar los niveles de protección en los equipos que cumplan las funciones de AntiSpam, WebFilter y Antivirus o su vez, mantener actualizado el software antivirus en todos los sistemas.