15/09/2023 **Alerta de Seguridad Digital**

Contexto incidente de seguridad digital infraestructura IFX Networks

Contexto de la Amenaza - Ransomware

El Ransomware que recientemente afectó a IFX, está relacionado con una de las posibles causas de un actor de la amenaza denominado **MarioLocker, el cual ha roto marca en la generación de incidentes**[1], más de 459 de ellos, hablan de la efectividad que ha tenido en diferentes organizaciones a nivel global.

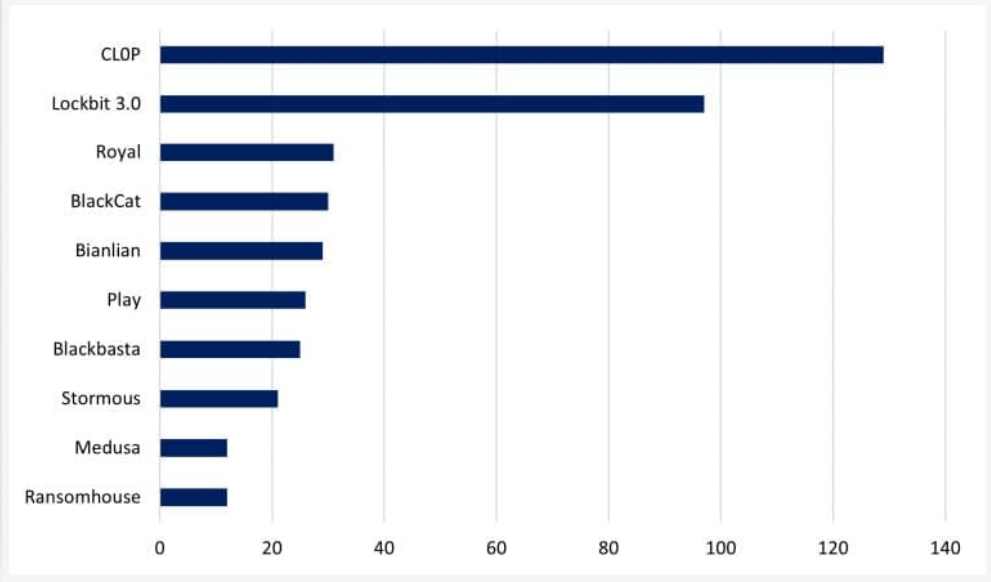

Ilustración 1 - Recuperada de https://www.bleepingcomputer.com/news/security/march-2023-broke-ransomware-attack-records-with-459-incidents/ y adaptada para el análisis del actor de la amenaza – NCC Group

[1] https://www.bleepingcomputer.com/news/security/march-2023-broke-ransomware-attack-records-with-459-incidents/

El COLCERT por medio de su análisis de (CTI) Cyber Treath Intelligence ha detectado diferentes artefactos que se asocian entre sí para poder validar que por medio de diferentes vulnerabilidades que pueden ser aprovechadas por terceros o que pueden relacionarse frente a dispositivos y activos que se encuentren compartiendo atributos de infraestructura con recursos en la nube, así lo manifiesta Microsoft[2] en este caso la propagación de la amenaza puede afectar los servicios que se comparten por medio de algunos sistemas de información y/o aplicaciones orientadas a la conexión remota de herramientas (entornos virtualizados) como ocurrió en mayo de 2023 frente a la explotación de diferentes acciones como las 10 familias de ransomware que fueron identificadas[3] que utilizan esta función, por ende no es ajeno a este tipo de técnicas utilizadas recientemente.

En la referenciación de la amenaza no existe una vinculación directa con un actor en particular, sin embargo, el agente que desarrolla y despliega el tipo de ransomware documentado hasta el momento se fundamenta en unos vectores particulares que tienen relación con publicaciones de posibles datos sobre *Abbeyfield y SAC Finance*, organizaciones, la primera de carácter humanitario y la segunda a servicios financieros localizadas en el Reino Unido y Estados Unidos respectivamente. En atención a los últimos acontecimientos relacionados con ADATA[4], el data breach más reciente ocasionado en 2021, ransomhouse negó esta acción, pero varias de las notas involucradas lo direccionaban a *"White Rabbit"* una de las firmas establecidas por este popular grupo cibercriminal que fue anunciado por @malwahunterTeam[5] desde agosto de 2022.

Un suceso también reciente que involucra a "RansomHouse" tiene que ver con el cifrado de los datos de AMD[6] (Advanced Micro Devices) el cual tiene una relación con algunos eventos relacionados con FIN8[7], la APT (Advanced Persistent Treath) relacionada con

---

[2] Guía para el entendimiento para la distribución de Malware y sus familias como el Ransomware: Malware distributor Storm-0324 facilitates ransomware access

[3] https://www.sentinelone.com/labs/hypervisor-ransomware-multiple-threat-actor-groups-hop-on-leaked-babuk-code-to-build-esxi-lockers/

[4] https://www.bleepingcomputer.com/news/security/adata-denies-ransomhouse-cyberattack-says-leaked-data-from-2021-breach/

[5] https://twitter.com/malwrhunterteam/status/1560327142621208577/

[6] https://www.theregister.com/2022/06/28/amd-ransomhouse-data-extortion/ y https://www.theregister.com/2020/03/26/amd_code_shutdown/

[7] https://www.hivepro.com/fin8-hacker-group-using-new-white-rabbit-ransomware-against-u-s-banks/

algunas actividades orientadas hacia la ejecución de ciertas características propias del Grupo Cibercriminal, obteniendo de esta forma de actuar la suficiente experiencia para poder atacar objetivos sensibles como los financieros y utilizando técnicas de evasión en objetivos y generalmente utiliza una nota denominada "scrypt.txt"[8] para después ejecutar su rutina y desactivar los servicios de antivirus, también como técnica evasiva puede saltarse varios unidades de uso compartido para evitar colapsar el sistema.

En agosto de 2021 fue detectado el uso de un famoso troyano llamado "Sardonic" [9] en el análisis de la amenaza y descrita por *Bitdefender*, ese mismo había sido usado en la APT- FIN8[10] utilizando algunas técnicas descritas en la siguiente imagen:

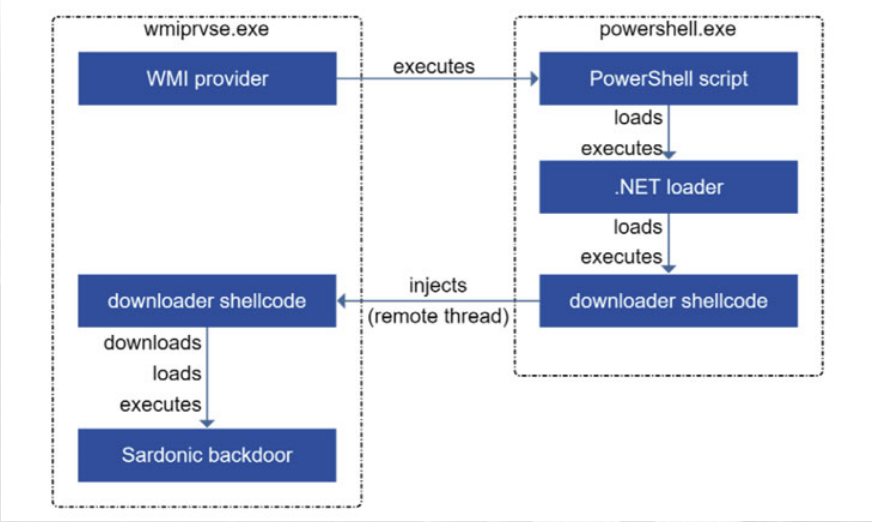

Ilustración 2 - adaptada de https://thehackernews.com/2021/08/researchers-uncover-fin8s-new-backdoor.html, relacionada con la forma de inyección de procesos, una técnica ampliamente utilizada por FIN8.

Por otra parte, la utilización de diversas maneras de poder aprovechar las vulnerabilidades relacionadas con ESXi y la popular guía que publicó CISA[11] en febrero de este año ha permitido establecer que las probabilidades que los vectores que realice

[8] https://pastebin.com/waLqSHCh - Nota de Rescate
[9] https://thehackernews.com/2022/01/fin8-hackers-spotted-using-new-white.html
[10] https://thehackernews.com/2021/08/researchers-uncover-fin8s-new-backdoor.html
[11] https://www.cisa.gov/sites/default/files/2023-02/aa23-039a-esxiargs-ransomware-virtual-machine-recovery-guidance.pdf

este actor se encuentren relacionados con las diferentes técnicas utilizadas en el top 5[12] destacado para este tipo de ciberataques. El cálculo realizado por el grupo de especialistas del COLCERT orientado mediante el Framework NISTIR 8374 y NIST SPECIAL PUBLICATION 1800-26[13] ha determinado el uso de las técnicas a saber:

- T1486: Data Encrypted for Impact
- T1490: Inhibit System Recovery
- T1027: Obfuscated Files or Information
- T1047: Windows Management Instrumentation
- T1036: Masquerading
- T1059: Command and Scripting Interpreter
- T1562: Impair Defenses
- T1112: Modify Registry
- T1204: User Execution
- T1055: Process Injection

[12] https://top-attack-techniques.mitre-engenuity.org/
[13] NIST SPECIAL PUBLICATION 1800-26 - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-26.pdf

En relación con estas actividades relacionadas con el actor de la amenaza el grupo de CTI realiza el siguiente análisis:

Ilustración 3 - Proximidad e impacto – COLCERT : Ciberataques relacionados: SAC FInance, Clinice Barcelona, Keralty y IFX Networks.

En la ilustración 3 se identifican tres factores esenciales que tienen una relación de línea de tiempo de cada uno de los ciberataques relacionados, y se valida la proximidad de estos para poder identificar la autoría de ***"RansomHouse"*** como amenaza como se observa en la imagen, de la misma manera se realiza una validación del impacto causado sobre el volumen de la información reportado para poder definir aquellos aspectos de interés dentro del análisis.

¿Cómo ocurre un incidente de ransomware y cómo prevenirlos?

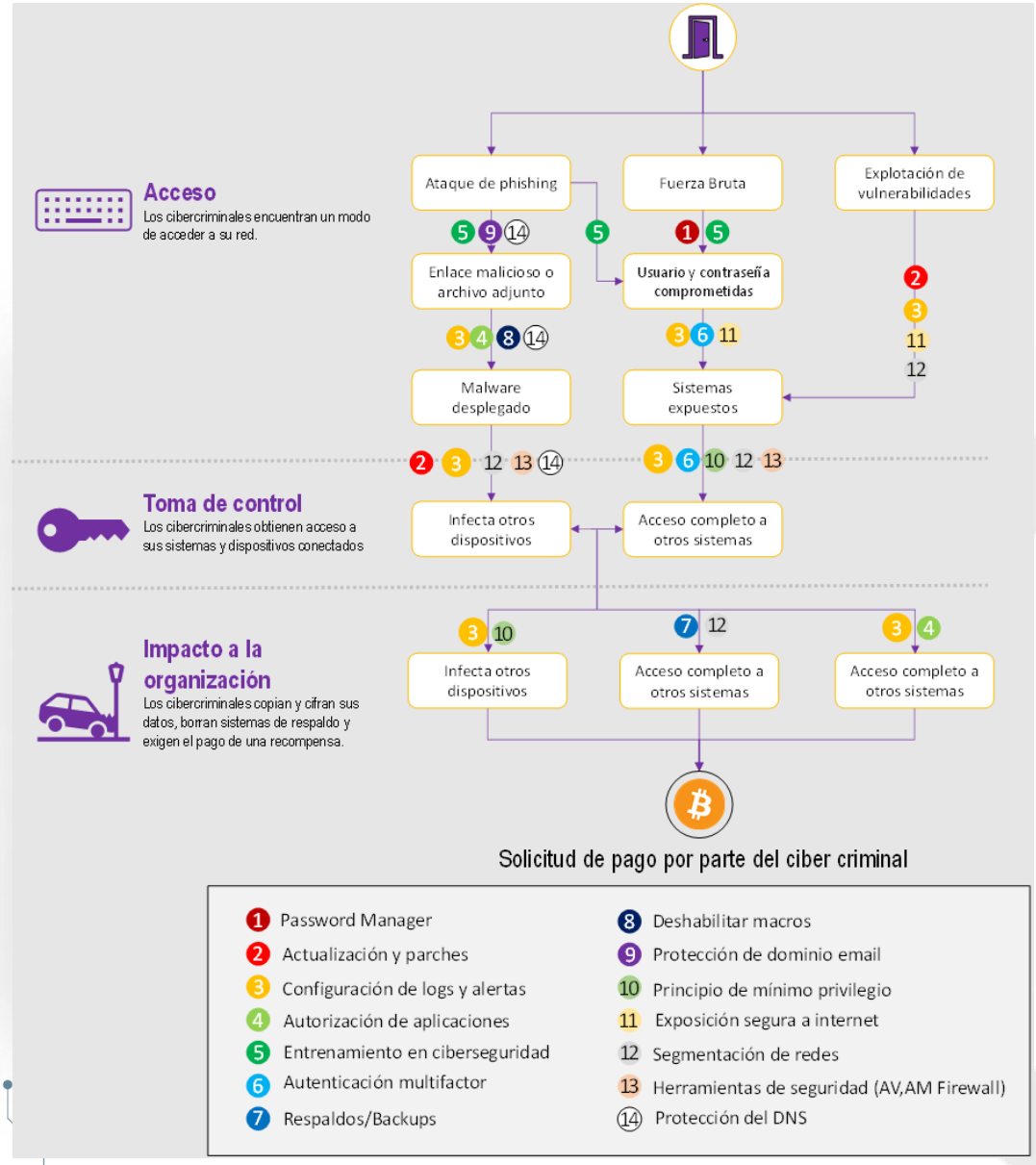

Ilustración 4 - Mecanismo de operación de un Ransomware. Fuente: Adaptado de Canadian Centre for Cyber Security

¿Cómo puede preparar su organización?

PREPARACIÓN - Antes del Ataque

¿Cómo puede proteger su información - Aspectos generales?

1. **Políticas de Seguridad de la Información**
   Defina sus políticas de gestión de la seguridad de la información, procurando responder al contexto de su organización, objetivos de negocio, misión y enfoque de su análisis de riesgos de seguridad de la información.

2. **Plan de Continuidad del Negocio.**
   Desarrolle y busque la aprobación del plan de continuidad del negocio, para definir las aplicaciones de misión crítica que deben ser respaldadas en sitio alterno para la recuperación y restablecimiento de las operaciones según el tiempo tolerable necesario para que los sistemas críticos vuelvan a estar operativos (RTO) y la cantidad máxima aceptable de pérdida de datos entre la última copia de seguridad y la fecha en que ocurre del incidente (RPO)**.**

3. **Copia de seguridad de los datos de aplicaciones y servicios críticos.**
   Implemente y operacionalice procedimientos de respaldos o copias de seguridad/backups. Tenga en cuenta que estas copias de seguridad deben ser generadas y almacenadas en segmentos aislados para evitar ser alcanzado por el ransomware.

4. **Principio del mínimo privilegio- Zero Trust**
   Administre y supervise las cuentas de usuario y el acceso aplicando el principio de mínimos privilegios.

5. **Deshabilitar macros**
   Asegúrese de deshabilitar las macros como predeterminadas, para reducir el riesgo que el ransomware se propague a través de los archivos adjuntos de Microsoft Office.

6. **Configuración de herramientas de seguridad**
   Procure instalar firewall de red y de aplicaciones -WAF, sistema Endpoint Detection Response EDR, para obtener visibilidad en la red.

7. **Uso de VPN (Red Privada Virtual)**
   La configuración de una VPN establece un túnel cifrado de comunicación entre el equipo que sale a internet e Internet, estableciendo una conexión segura, garantizando protección frente a amenazas externas.

8. **Desactivación de unidades externas**
   Desactive las opciones Autorun y Autoplay en las unidades externas (CD, USB, etc.), de igual forma minimice el uso de conexión de dispositivos externos por parte de los colabores en los computadores de la organización.

9. **Configuración de correo corporativo con filtros antispam**
   El filtro antispam mantiene la bandeja de entrada libre de spam y phishing, se puede realizar a correos comerciales.

10. **Plan de auditoría de logs del sistema**
    Implemente plan de auditoría de logs permanente, de las actividades de gestión del Directorio Activo, como cambios de contraseñas, eliminación de usuario, creación y/o modificación de cuentas de usuario, etc.

11. **Programación de pruebas de vulnerabilidad**
    Las pruebas de vulnerabilidades aplicadas regularmente permiten revisar y estimar las debilidades de seguridad en la infraestructura de un sistema de información.

12. **Limitar el uso de escritorio remoto (RDP)**
    Los actores de amenazas generalmente acceden una red a través de servicios remotos desprotegidos.

DURANTE – Línea de Infección y Propagación

- **Lista de comprobación de respuesta al ransomware**

La Agencia de Seguridad de Ciberseguridad e Infraestructura (CISA) y el COLCERT recomienda responder al ransomware utilizando la siguiente lista de verificación proporcionada en una Guía conjunta de #StopRansomware de CISA, FBI, NSA y Multi-State Information Sharing and Analysis Center (MS-ISAC), actualizada en mayo de 2023.

Esta información lo guiará a través del proceso de respuesta desde la detección hasta la contención y la erradicación. Asegúrese de avanzar a través de los primeros tres pasos en secuencia.

- **Detección y análisis - Durante la infección**

Consulte las prácticas recomendadas y las referencias a continuación para ayudar a administrar el *riesgo* que plantea el ransomware y respaldar la respuesta coordinada y eficiente de su organización a un incidente de ransomware. Aplicar estas prácticas en la mayor medida posible en función de la disponibilidad de recursos de la organización.

- Determine qué sistemas se vieron afectados y aíslelos inmediatamente.
- Si varios sistemas o subredes aparecen afectados, desconecte la red en el nivel del conmutador. Puede que no sea factible desconectar sistemas individuales durante un incidente.
- Priorice el aislamiento de sistemas críticos que son esenciales para las operaciones diarias.
- Si no es posible desconectar la red temporalmente, localice el cable de red (por ejemplo, ethernet) y desconecte los dispositivos afectados de la red o elimínelos de Wi-Fi para contener la infección.
- Para los recursos en la nube, tome una instantánea de los volúmenes para obtener una copia puntual para revisarla más tarde para la investigación forense.
- Después de un *compromiso inicial,* los actores pueden monitorear la actividad o las comunicaciones de su organización para comprender si se han detectado sus acciones. Aísle los sistemas de manera coordinada y utilice métodos de comunicación como llamadas telefónicas, para evitar avisar a los *actores* de que han sido descubiertos y que se están llevando a cabo acciones de mitigación. No hacerlo podría hacer que los actores se muevan lateralmente para preservar su acceso o implementar ransomware ampliamente antes de que las redes se desconecten.
- Apague los dispositivos si no puede desconectarlos de la red para evitar una mayor propagación de la infección de ransomware. *Nota: Este paso evitará que su organización mantenga artefactos de infección de ransomware y evidencia potencial almacenada en la memoria volátil. Debe llevarse a cabo solo si no es posible apagar*

temporalmente la red o desconectar los hosts afectados de la red utilizando otros medios.

- Triage de los sistemas afectados para la restauración y recuperación.
- Identifique y priorice los sistemas críticos para la restauración en una red limpia y confirme la naturaleza de los datos alojados en los sistemas afectados.
- Priorice la restauración y la recuperación en función de una lista de activos críticos predefinida que incluya sistemas de información críticos para la salud y la seguridad, generación de ingresos u otros servicios críticos, así como sistemas de los que dependen.
- Realice un seguimiento de los sistemas y dispositivos que no se perciben afectados para que puedan ser des priorizados para la restauración y recuperación. Esto permite a su organización volver al negocio de una manera más eficiente.
- Examinar los sistemas de detección o prevención organizacionales existentes (por ejemplo, antivirus, EDR, IDS, Sistema de Prevención de Intrusiones) y los registros. Esta actividad puede resaltar la evidencia de sistemas adicionales o malware involucrados en etapas anteriores del ataque.
- Busque evidencia de malware precursor "gotero", como Bumblebee, Dridex, Emotet, QakBot o Anchor. Un evento de ransomware puede ser evidencia de un compromiso de red anterior no resuelto.
- Los operadores de estas variantes avanzadas de malware a menudo venden acceso a una red. Los actores maliciosos a veces usan este acceso para filtrar datos y luego amenazan con divulgar los datos públicamente antes de rescatar la red para extorsionar aún más a la víctima y presionarla para que pague.
- Los actores maliciosos a menudo dejan caer variantes de ransomware para ocultar la actividad posterior al compromiso. Se debe tener cuidado para identificar dicho malware "Dropper" antes de reconstruir a partir de copias de seguridad para evitar compromisos continuos.
- Consulte con su equipo para desarrollar y documentar una comprensión inicial de lo que ha ocurrido basada en el análisis inicial.

Actividades de Ciberinteligencia (CTI)

Para entornos empresariales, compruebe lo siguiente:

- Cuentas de "Directorio Activo" recién creadas o cuentas con privilegios escalados y actividad reciente relacionada con cuentas privilegiadas como administradores de dominio.
- Inicios de sesión anómalos de dispositivos VPN u otros inicios de sesión sospechosos.
- Modificaciones de punto de conexión que pueden afectar a las copias de seguridad, instantáneas, registro en diario de disco o configuraciones de arranque. Busque el uso anómalo de las herramientas integradas de Windows como bcdedit.exe, fsutil.exe (deletejournal), vssadmin.exe, wbadmin.exe y wmic.exe (shadowcopy o shadowstorage). El mal uso de estas herramientas es una técnica común de ransomware para no permitir la recuperación del sistema.

Posibles hallazgos - Signos de *Cobalt Strike:*

- Es un paquete de software de pruebas de penetración comercial. Los actores malintencionados a menudo nombran los procesos de Cobalt Strike Windows con los mismos nombres que los procesos legítimos de Windows para ofuscar su presencia y complicar las investigaciones.
- Señales de cualquier uso inesperado del software de monitoreo y administración remotos (RMM o RDP) (incluidos los ejecutables que no están instalados). El software RMM es comúnmente utilizado por actores maliciosos para mantener la persistencia.
- Cualquier ejecución inesperada de PowerShell o uso de la suite PsTools.
- Signos de enumeración de credenciales AD y/o LSASS que se están volcando (por ejemplo, Mimikatz o NTDSutil.exe).
- Señales de comunicaciones inesperadas de punto final a punto final (incluidos los servidores).

- Posibles señales de exfiltración de datos de la red. Las herramientas comunes para la exfiltración de datos incluyen Rclone
- Rsync, varios servicios de almacenamiento de archivos basados en la web (también utilizados por actores de amenazas para implantar malware/herramientas en la red afectada) y FTP/SFTP.
- Servicios recién creados, tareas programadas inesperadas, software inesperado instalado, etc.

Para entornos de nube:

- Habilite herramientas para detectar y evitar modificaciones en IAM, seguridad de red y recursos de protección de datos.
- Utilice la automatización para detectar problemas comunes (por ejemplo, deshabilitar funciones, introducir nuevas reglas de firewall) y tomar medidas automatizadas tan pronto como ocurran. Por ejemplo, si se crea una nueva regla de firewall que permite el tráfico abierto (0.0.0.0/0), se puede realizar una acción automatizada para deshabilitar o eliminar esta regla y enviar notificaciones al usuario que la creó, así como al equipo de seguridad para que la conozca. Esto ayudará a evitar la fatiga de alerta y permitirá que el personal de seguridad se centre en cuestiones críticas.

Informes y notificaciones:

Nota: Consulte la sección Información de contacto al final de esta guía para obtener detalles sobre cómo informar y notificar sobre incidentes de ransomware.

- Siga los requisitos de notificación descritos en su plan de comunicaciones y respuesta a incidentes cibernéticos para involucrar a los equipos internos y externos y a las partes interesadas con una comprensión de lo que pueden proporcionar para ayudarlo a mitigar, responder y recuperarse del incidente.
- Comparta la información que tiene a su disposición para recibir asistencia oportuna y relevante. Mantenga informados a la gerencia y a los líderes superiores a través

de actualizaciones periódicas a medida que se desarrolla la situación. Las partes interesadas relevantes pueden incluir su departamento de TI, proveedores de servicios de seguridad administrados.

- De acuerdo a lo que corresponda, puede realizar coordinaciones con el personal de comunicaciones e información pública para garantizar que la información precisa se comparta internamente con su organización y externamente con el público.
- Si el incidente resultó en una violación de datos, siga los requisitos de notificación como se describe en sus planes de comunicación y respuesta a incidentes cibernéticos.

Contención y erradicación:

Si no parece posible ninguna acción de *mitigación inicial*:

- Tome una imagen forense del sistema y una captura de memoria de una muestra de dispositivos afectados (por ejemplo, estaciones de trabajo, servidores, servidores virtuales y servidores en la nube). Recopile cualquier registro relevante, así como muestras de cualquier binario de malware *"precursor"* y observables asociados o indicadores de compromiso (por ejemplo, direcciones IP sospechosas de comando y control, entradas de registro sospechosas u otros archivos relevantes detectados).
- Conserve la evidencia que es de naturaleza altamente volátil, o limitada en retención, para evitar la pérdida o la manipulación (por ejemplo, memoria del sistema, registros de seguridad de Windows, datos en búferes de registro de firewall).
- Consulte en la comunidad de ciberseguridad la cual incluye al COLCERT incluso si las acciones de mitigación son posibles, con respecto a los posibles descifradores disponibles, ya que los investigadores de seguridad pueden haber descubierto fallas de cifrado para algunas variantes de ransomware y liberado descifrado u otros tipos de herramientas.

Para continuar con los pasos para contener y mitigar el incidente:

- Oriéntese bajo una guía confiable (por ejemplo, publicada por fuentes como el gobierno de EE. UU., MS-ISAC o un proveedor de seguridad acreditado) para la variante de ransomware en particular y siga los pasos recomendados adicionales para identificar y contener los sistemas o redes que se confirma que están afectados.
- Deshabilitar la ejecución de binarios de ransomware conocidos; Esto minimizará el daño y el impacto en sus sistemas. Elimine otros archivos y valores del Registro asociados conocidos.
- Identifique los sistemas y las cuentas involucradas en la violación inicial. Esto puede incluir cuentas de correo electrónico.
- En función de los detalles de incumplimiento o compromiso determinados anteriormente, contener sistemas asociados que puedan usarse para un acceso no autorizado adicional o continuo. Las infracciones a menudo implican la exfiltración masiva de credenciales. Proteger las redes y otras fuentes de información del acceso continuo no autorizado basado en credenciales puede incluir:
- Deshabilite las redes privadas virtuales (VPN), los servidores de acceso remoto, los recursos de inicio de sesión único y los activos basados en la nube u otros activos públicos.
- Si una estación de trabajo infectada cifra los datos del lado del servidor, siga los pasos de identificación rápida del cifrado de datos del lado del servidor.
- Revise las listas Administración de equipos > sesiones y Abrir archivos en los servidores asociados para determinar el usuario o el sistema que accede a esos archivos.
- Revise las propiedades de archivo de archivos cifrados o notas de rescate para identificar usuarios específicos que pueden estar asociados con la propiedad del archivo.
- Revise el registro de eventos TerminalServices-RemoteConnectionManager para comprobar si las conexiones de red RDP se han realizado correctamente.
- Revise el registro de seguridad de Windows, los registros de eventos SMB y los registros relacionados que pueden identificar eventos significativos de autenticación o acceso.
- Ejecute software de captura de paquetes, como Wireshark, en el servidor afectado con un filtro para identificar las direcciones IP involucradas en la escritura activa o

el cambio de nombre de los archivos (por ejemplo, smb2.filename contiene cryptxxx).

- Realizar análisis extensos para identificar mecanismos de persistencia de afuera hacia adentro y de adentro hacia afuera.
- La persistencia de afuera hacia adentro puede incluir acceso autenticado a sistemas externos a través de cuentas no autorizadas, puertas traseras en sistemas perimetrales, explotación de vulnerabilidades externas, etc.
- La persistencia de adentro hacia afuera puede incluir implantes de malware en la red interna o una variedad de modificaciones de estilo de vida fuera de la tierra (por ejemplo, uso de herramientas comerciales de prueba de penetración como Cobalt Strike; uso de la suite PsTools, incluido PsExec, para instalar y controlar malware de forma remota y recopilar información sobre sistemas Windows o realizar administración remota de ellos; uso de scripts de PowerShell).

La identificación puede implicar la implementación de soluciones EDR, auditorías de cuentas locales y de dominio, examen de datos encontrados en sistemas de registro centralizados o análisis forense más profundo de sistemas específicos una vez que se ha mapeado el movimiento dentro del entorno.

- Reconstruya sistemas basados en la priorización de servicios críticos (por ejemplo, salud y seguridad o servicios generadores de ingresos), utilizando imágenes estándar preconfiguradas, si es posible. Use la infraestructura como plantillas de código para reconstruir los recursos de la nube[14].
- Emitir restablecimientos de contraseñas para todos los sistemas afectados y abordar cualquier vulnerabilidad asociada y brechas en seguridad o visibilidad una vez que el entorno se haya limpiado y reconstruido por completo, incluidas las cuentas afectadas asociadas y la eliminación o corrección de mecanismos de persistencia maliciosos. Esto puede incluir la aplicación de parches, la actualización de software y la toma de otras precauciones de seguridad que no se habían tomado anteriormente. Actualice las claves de cifrado administradas por el cliente según sea necesario.

[14] https://learn.microsoft.com/es-es/security/ransomware/protect-against-ransomware

- La autoridad de TI o de seguridad de TI designada declara el incidente de ransomware en función de criterios establecidos, que pueden incluir tomar los pasos anteriores o buscar ayuda externa.

Recuperación y actividad posterior al incidente:

- Vuelva a conectar los sistemas y restaure los datos de copias de seguridad cifradas sin conexión en función de una priorización de los servicios críticos.
- Tenga cuidado de no volver a infectar los sistemas limpios durante la recuperación. Por ejemplo, si se ha creado una nueva red de área local virtual (VLAN) con fines de recuperación, asegúrese de que solo se agreguen sistemas limpios.
- Documente las lecciones aprendidas del incidente y las actividades de respuesta asociadas para informar las actualizaciones y refinar las políticas, planes y procedimientos de la organización y guiar los ejercicios futuros de los mismos.
- Considere compartir las lecciones aprendidas y los indicadores relevantes de compromiso con el COLCERT para beneficiar a otros dentro de la comunidad y Ecosistema Digital Colombiano.

¿Cómo detectar el ransomware?

- Alertas de seguridad de plataformas antivirus y soluciones EDR
- Cambios en las extensiones de los archivos.
- Cambios en los nombres de los archivos.
- Tráfico de red anormal.
- Archivos cifrados e inaccesibles.
- Aparición de algún tipo de nota de rescate.

¿Recomendaciones de CISA[15], aplicables en la recolección de información a equipos afectados con ransomware, para ser aportado como primer respondiente en el incidente?

1. Determine qué sistemas se vieron afectados y aíslelos inmediatamente.
   Para los recursos en la nube, tome una instantánea de los volúmenes para obtener una copia exacta para revisarla más tarde en la investigación forense.

2. Apague los dispositivos, si no puede desconectarlos de la red para evitar una mayor propagación de la infección de ransomware.

   a. Nota: Este paso evitará que su organización mantenga artefactos de infección de ransomware y evidencia potencial almacenada en la memoria volátil. Debe llevarse a cabo solo si no es posible apagar temporalmente la red o desconectar los hosts afectados de la red utilizando otros medios

3. Triage de los sistemas afectados para restauración y recuperación.
   Identifique y priorice los sistemas críticos para la restauración en una red limpia y confirme la naturaleza de los datos alojados en los sistemas afectados.

   Examinar los sistemas organizativos existentes de detección o prevención (por ejemplo, antivirus, EDR, IDS, sistema de prevención de intrusiones) y los registros. Si lo hace, puede resaltar la evidencia de sistemas adicionales o malware involucrados en etapas anteriores del ataque.

4. Iniciar actividades de caza de amenazas.

[15] Cybersecurity and Infrastructure Security Agency the United States - CISA

Toma una imagen del sistema y captura de memoria de una muestra de dispositivos afectados (por ejemplo, estaciones de trabajo, servidores, servidores virtuales y servidores en la nube).

Recopilar todos los registros relevantes, (Direcciones IP de comando y control inspeccionadas, entradas de registro sospechosas u otros archivos relevantes detectados).

5. Preservar la evidencia que es de naturaleza altamente volátil, o limitada en retención, para evitar la pérdida o manipulación (por ejemplo, memoria del sistema, Registros de seguridad de Windows, datos en búferes de registro de firewall).

6. Compartir las muestras con el equipo de informática forense, para realizar la respectiva investigación.

Otras recomendaciones:

- Ponga el equipo en cuarentena aísle el dispositivo inmediatamente: Desconecte los dispositivos afectados de todas las interfaces de red (ethernet, wifi, bluetooth, etc.).
- Dejar la computadora y servidores encendidos: Mantenga los dispositivos prendidos para aumentar la probabilidad de recuperación, no apagar los dispositivos para evitar la pérdida de memoria volátil y realizar la investigación forense.
- Identifique el tipo de ransomware: Utilice la información en la nota de rescate (por ejemplo, las URL listadas) y las extensiones de archivo que tienen los archivos cifrados, para identificar la cepa del ransomware e investigar ataques recurrentes.
- Realice una investigación: Para identificar vector de ataque, indicadores de compromiso – IoC y posibles mecanismos de propagación con el propósito de

realizar seguimiento al comportamiento del ransomware a las técnicas y tácticas empleadas por los ciberdelincuentes.

- Restablezca el dispositivo y borre todos los datos: Si no hay ninguna herramienta de descifrado disponible en línea para su cepa de ransomware, limpie de forma segura su dispositivo y vuelva a instalar el sistema operativo, instale nuevamente la solución de antivirus y de ser posible realice una imagen forense a equipos afectados como evidencia digital.

- Restaure desde su copia de seguridad: Analice sus archivos de copia de seguridad y asegúrese de que estén libres del ransomware o cualquier otro malware

Fuentes consultadas:

- Guía para el entendimiento para la distribución de Malware y sus familias como el Ransomware: Malware distributor Storm-0324 facilitates ransomware access
- https://www.sentinelone.com/labs/hypervisor-ransomware-multiple-threat-actor-groups-hop-on-leaked-babuk-code-to-build-esxi-lockers/
- https://www.bleepingcomputer.com/news/security/adata-denies-ransomhouse-cyberattack-says-leaked-data-from-2021-breach/
- https://twitter.com/malwrhunterteam/status/1560327142621208577/
- https://www.theregister.com/2022/06/28/amd-ransomhouse-data-extortion/ y https://www.theregister.com/2020/03/26/amd_code_shutdown/
- https://www.hivepro.com/fin8-hacker-group-using-new-white-rabbit-ransomware-against-u-s-banks/
- https://pastebin.com/waLqSHCh - Nota de Rescate
- https://thehackernews.com/2022/01/fin8-hackers-spotted-using-new-white.html
- https://thehackernews.com/2021/08/researchers-uncover-fin8s-new-backdoor.html
- https://www.bleepingcomputer.com/news/security/march-2023-broke-ransomware-attack-records-with-459-incidents/
- https://www.cisa.gov/sites/default/files/2023-02/aa23-039a-esxiargs-ransomware-virtual-machine-recovery-guidance.pdf
- https://top-attack-techniques.mitre-engenuity.org/

- NIST SPECIAL PUBLICATION 1800-26 - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-26.pdf
- https://www.cisa.gov/stopransomware/ive-been-hit-ransomware
- https://www.cisa.gov/sites/default/files/2023-06/stopransomware_guide_finales.pdf

CANALES DE ATENCIÓN

Si tiene alguna consulta técnica, puede comunicarse con CSIRT Presidencia al teléfono (601) 5629300 ext. 3309, correo electrónico csirt@presidencia.gov.co, con copia a los correos segdig-gtd@presidencia.gov.co; contacto@colcert.gov.co.