Nro. Alerta:	AL-2024-016	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	24-jul-2024	**Funcionamiento interno del ransomware Qilin**	Pág.: **1** of **10**

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Tipo de incidente: Ransomware
Nivel de riesgo: Alto

II. ALERTA

El grupo de ransomware Qilin de origen ruso, también conocido como "Agenda" es un ransomware que opera bajo el modelo Ransomware como Servicio (RaaS)[1], permitiendo que sus afiliados realicen ataques utilizando su infraestructura basada en lenguaje Rust. Este ransomware se ha convertido en una amenaza importante desde su descubrimiento en agosto de 2022 ya que emplea técnicas de doble extorsión; exige pago por la clave de descifrado y otro pago por no publicar la información robada.

Un grupo de investigadores se infiltró y analizó el funcionamiento interno de Qilin, revelando información sobre sus objetivos y técnicas sofisticadas que emplean.

Figura 1: *logotipo del ransomware Qilin (Agenda)*

III. INTRODUCCIÓN

El Ransomware "Agenda" (también conocido como Qilin y Water Galura) se detectó por primera vez en agosto de 2022. Su primer ransomware basado en Golang se utilizó en

[1] RaaS es un modelo de negocio de la ciberdelincuencia en el que los desarrolladores de ransomware venden su malware a otros hacker.

contra de empresas dedicadas a la atención médica, manufactura y educación, desde Canadá hasta Colombia e Indonesia.

A finales de 2022, los propietarios de Agenda reescribieron su malware en Rust, un lenguaje de programación útil para los autores de malware que buscan difundir el ransomware en todos los sistemas operativos (Windows, Linux, VMware vCenter y ESXi); gracias a sus cualidades de evasión, personalización y difícil descifrado.
Muchos ataques de Qilin se personalizan para cada víctima para maximizar su impacto. Para hacer esto, los actores de amenazas pueden aprovechar tácticas como cambiar las extensiones de los nombres de los archivos cifrados y finalizar procesos y servicios específicos.

Una vez obtenido los datos, el grupo anuncia sus actividades en la red oscura y cuenta con un DLS[2] patentado que contiene identificaciones únicas de empresas y detalles filtrados de cuentas.

Con la variante Rust, Agenda pudo comprometer a empresas de varios países de sectores críticos como finanzas, derecho, construcción y más. Los investigadores de Group-IB entre julio de 2022 y mayo de 2023, publicaron información sobre 12 víctimas en su sitio de filtración de filtración de datos dedicado (DLS). Estas víctimas abarcan varios países, incluidos Australia, Brasil, Canadá, Colombia, Francia, Países Bajos, Serbia, el Reino Unido, Japón y Estados Unidos.

Desde diciembre de 2023, estos ciberdelincuentes también han estado desarrollando uno de los cifradores de Linux más avanzados y personalizables vistos hasta la fecha, diseñado específicamente para apuntar a las máquinas virtuales VMware ESXi preferidas por las organizaciones empresariales para sus necesidades de recursos livianos.

IV. FUNCIONAMIENTO INTERNO DE QILIN

Los investigadores del Group-IB Threat Intelligence pudieron infiltrarse en la operación Qilin en marzo de 2024 y lo que encontraron fue que ransomware Qilin:

[2] Dedicated Leak Sites (DLS) o sitio de filtración de datos: es un sitio web donde ciberdelincuente publican datos recuperados ilícitamente de empresas que se niegan a pagar el rescate producto de un ataque con ransomware. Estos sitios pueden contener información confidencial, como credenciales de inicio de sesión, propiedad intelectual, datos personales y financieros, etc., que ponen a una organización en riesgo.

- Es una ventanilla única para que los aspirantes a ciberdelincuentes pudieran obtener ransomware avanzado y personalizable;
- Una estructura de pago definida; y,
- Servicios de cifrado para soportar doble operaciones de extorsión (es decir, exigir dinero para descifrar los datos, así como una tarifa adicional por no revelar los datos en un sitio de filtración de Wark Web).

Los ataques de ransomware respaldados por operadores de Qilin generalmente comienzan con un correo electrónico de phishing, para infiltrarse en las redes de una empresa y extraer datos mientras se desplaza por los sistemas de la víctima.

Después de obtener las credenciales de administrador para los servidores y recopilar todos los datos confidenciales, los atacantes implementan las cargas útiles del ransomware para cifrar todos los dispositivos conectados a la red.
Luego aprovechan los datos robados y los archivos cifrados para llevar a cabo ataques de doble extorsión, presionando a las empresas objetivo para que cumplan con sus demandas.

ANÁLISIS DEL PANEL DE ADMINISTRACIÓN DE QILIN

Los especialistas de Group-IB observaron que Qilin opera bajo el modelo RaaS y proporciona a sus afiliados un panel administrativo para gestionar los ataques de manera más efectiva. Este panel se divide en las siguientes secciones:

- **Sección 1 Objetivos:** Contiene información sobre las empresas atacadas tales como: el monto del rescate, período de espera para el pago del rescate, zona horaria de la empresa, información sobre los ingresos de la empresa del sitio web Zoominfo, anuncio, descripción de la empresa atacada, etc.

  Además, esta sección permite a los afiliados crear muestras de ransomware Qilin con varias configuraciones como el contenido de la nota de rescate, los directorios y extensiones que se omitirán, los procesos que serán eliminados, los servicios que serán suspendidos, credenciales de inicio de sesión de cuentas hosts excluidos del modo seguro, modo de cifrado, extensiones que se cifrarán, lista de máquinas virtuales (VM) que no serán eliminadas/apagadas, etc.

- **Sección 2 Blogs:** En esta sección, los afiliados también pueden crear y editar publicaciones de blog que contengan información sobre las empresas atacadas que no han pagado el rescate.

- **Sección 3 Stuffers**: Permite a los intrusos crear cuentas para los miembros de su equipo ingresando sus apodos, credenciales de inicio de sesión y contraseñas. Además, pueden controlar si los miembros de su equipo pueden presenciar todos sus ataques, crear muestras de ransomware u obtener acceso a los chats con las víctimas.

- **Sección 4 Noticias:** Los operadores de ransomware Qilin publican actualizaciones relacionadas con su asociación de ransomware.

- **Sección 5 Pagos:** El bloque de Pagos contiene información sobre el saldo de las billeteras de los afiliados, las transacciones y las tarifas del grupo de ransomware. En esta sección, los afiliados pueden retirar el dinero del rescate.

- **Sección 6 Preguntas frecuentes:** Los afiliados también tienen acceso a soporte y documentación en la sección de preguntas frecuentes, que detalla el tipo de infecciones, cómo utilizar el malware, información adicional sobre los objetivos y más.

Algunas de las organizaciones que han sido víctimas del ransomware Qilin incluyen:

- The Big Issue, un periódico del Reino Unido, del cual se filtraron 550 GB de datos confidenciales de empleados.
- Yanfeng, un gigante mundial de piezas de automóviles.
- Servicios judiciales en Australia.
- Synnovis, una empresa que brinda servicios de patología a hospitales del NHS en Londres, lo que provocó la cancelación de cirugías planificadas

RANSOMWARE AGENDA(QILIN) EN ENTORNOS VIRTUALES

Por otro lado, investigadores de la empresa Trend Micro han observado, que el grupo de ransomware Agenda utiliza herramientas de administración y monitoreo remoto (RMM)[3], así como Cobalt Strike[4] para la implementación del binario de ransomware para sistemas operativos de virtualización, al mismo tiempo que utiliza diferentes controladores SYS[5] vulnerables para la evasión de defensa.

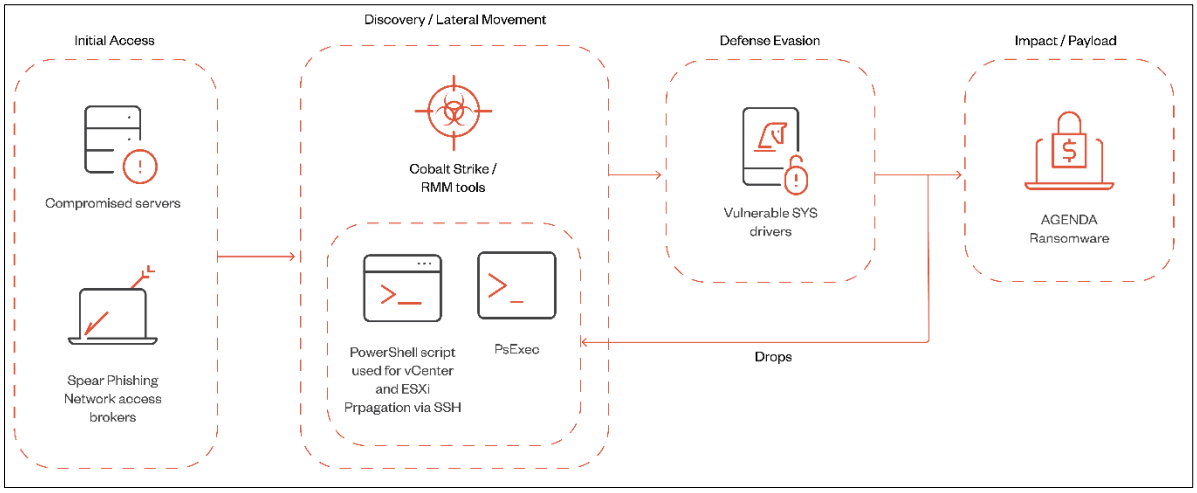

Figura 1: Cadena de infección del ransomware Agenda

[3] Remote Monitoring and Management (RMM) es un software de monitorización remota es una aplicación para supervisar y automatizar la infraestructura de TI. La plataforma permite a los usuarios detectar y configurar nuevos dispositivos e instalar actualizaciones sin estar en las instalaciones.

[4] Cobalt Strike es una herramienta de seguridad legítima que permite a los equipos de seguridad emular la actividad de los ciberdelincuentes dentro de una red, pero también es un recurso cada vez más utilizado por los ciberdelincuentes como carga útil de acceso inicial para desviar datos, hacer movimientos laterales y ejecutar cargas útiles de malware adicionales.

[5] Los controladores SYS vulnerables son un problema de seguridad importante en Windows, hasta 34 controladores únicos y vulnerables de Windows Driver Model (WDM) y Windows Driver Frameworks (WDF) podrían ser explotados por atacantes sin privilegios para obtener el control total de los dispositivos y ejecutar código arbitrario. Algunos de los nombres de estos controladores vulnerables incluyen AODDriver.sys, ComputerZ.sys, dellbios.sys, GEDevDrv.sys, GtcKmdfBs.sys, IoAccess.sys, kerneld.amd64, ngiodriver.sys, nvoclock.sys, PDFWKRNL.sys (CVE-2023-20598), RadHwMgr.sys, rtif.sys, rtport.sys, stdcdrv64.sys, y TdkLib64.sys (CVE-2023-35841).

El ejecutable del ransomware Agenda, también puede propagarse a través de las herramientas de comandos PsExec y SecureShell; para lo cual, utilizará un script de PowerShell personalizado integrado en el binario para propagarse a través de los servidores VMWare vCenter y ESXi.

Para ejecutarse, Agenda requiere que los usuarios ingresen sus credenciales en el vCenter o host ESXi de destino y especifiquen la ruta del binario de ESXi para propagarse. El script de PowerShell se ejecuta en memoria como un flujo de memoria en un proceso de PowerShell en ejecución, lo que hace que su ejecución no tenga archivos (ya que el script no estará presente en la máquina).

El script primero verifica si sus dependencias están instaladas, luego se conecta a los nombres de host especificados por el atacante y cambia la contraseña raíz para todos los hosts ESXi. La nueva contraseña será la requerida por Agenda para su ejecución. Esto evita efectivamente que las víctimas accedan al host comprometido incluso después de realizar el cifrado.

Una vez que SSH esté habilitado, se procederá a crear una sesión SSH que se utilizará para cargar el binario de ESXi. Después de la carga exitosa, ésta se ejecutará en el host de destino, comprometiendo efectivamente el sistema con una función para imprimir notas de rescate en impresoras conectadas.

V. VECTOR DE ATAQUE:

Se ha identificado que los ataques del grupo de Ransomware Qilin utilizan correos electrónicos de phishing con enlaces maliciosos para infiltrarse en las redes de las víctimas y extraer datos confidenciales. Tras obtener acceso, el grupo se desplaza lateralmente dentro de la infraestructura en busca de datos esenciales para cifrar.

Durante el proceso de cifrado, colocan una nota de rescate en cada directorio infectado, proporcionando instrucciones para adquirir la clave de descifrado. Los ciberdelincuentes también pueden intentar reiniciar sistemas y detener procesos para complicar la recuperación de datos por parte de la víctima.

VI. INDICADORES DE COMPROMISO:

A continuación los hashes de archivos maliciosos detectados:

MD5: 36d7912ff401c22e8cce925ba2d39d65
SHA-1: 5d88c0345937a375976187a72da0f88c632ef1d1
SHA-256: fd7cbadcfca84b38380cf57898d0de2adcdfb9c3d64d17f886e8c5903e416039

MD5: ee6a9116b3aa59833a9a051d1530c171
SHA-1: 79d63505eb23e607808e7867892a867670481d1d
SHA-256 : 76f860a0e238231c2ac262901ce447e83d840e16fca52018293c6cf611a6807e

MD5: 11d795baafa44b73766e850d13b8e254
SHA-1: be50782fd91e3ac926d5f4f964853324624f2495
SHA-256: 73b1fffd35d3a72775e0ac4c836e70efefa0930551a2f813843bdfb32df4579a

MD5: 14dec91fdcaab96f51382a43adb84016
SHA-1: a85d9d2a3913011cd282abc7d9711b2346c23899
SHA-256: 37546b811e369547c8bd631fa4399730d3bdaff635e744d83632b74f44f56cf6

MD5: 334fd98ab462edc1274fecdb89fb0791
SHA-1: e3496a341c96d77c0ef9bdeec333dd98e2215527
SHA-256:55e070a86b3ef2488d0e58f945f432aca494bfe65c9c4363d739649225efbbd1

MD5: 417ad60624345ef85e648038e18902ab
SHA-1: e18e6f975ef8fce97790fb8ae583caad1ec7d5b3
SHA-256: 555964b2fed3cced4c75a383dd4b3cf02776dae224f4848dcc03510b1de4dbf4

MD5: 6a93e618e467ed13f98819172e24fffa
SHA-1: d34550ebc2bee47c708c8e048eb78881468e6bca
SHA-256:e90bdaaf5f9ca900133b699f18e4062562148169b29cb4eb37a0577388c22527

ENLACES DE INTERÉS

- https://any.run/report/e90bdaaf5f9ca900133b699f18e4062562148169b29cb4eb37a0577388c22527/0bd5c06c-b1c3-4a1d-83f0-db5746476ef6
- https://any.run/report/f6e41d29ac9cf68bf48a280a1edf05e6dc0fccc5f6fe3709368fb567e3b5aa3e/8a7ec0a7-8de1-49bc-bfb2-5c65fdce0c4f
- https://any.run/report/ea2a632a6a786dceb4e65f00be143dbe4df07e5b58135c1f0c181999eedb5cce/bb06d0cb-8a16-4474-9be3-be49a86af699
- https://bazaar.abuse.ch/browse/signature/Qilin/ (cuidado al bajar las muestras)
- https://www.joesandbox.com/analysis/search?q=Qilin

VII. RECOMENDACIONES:

Ante un ataque de ransomware, es fundamental actuar con rapidez y seguir un conjunto de pasos específicos para minimizar el daño y aumentar las posibilidades de recuperación. Algunos pasos a seguir son:

1. **Aislar el Sistema o Red:** Si se detecta actividad de ransomware en una computadora o en la red, aislar inmediatamente el sistema afectado desconectándolo de la red informática. Esto ayudará a evitar que el ransomware se propague a otros sistemas. **Recuerde** no apagar el equipo para no perder información que se almacena temporalmente en la memoria volátil, necesaria para la investigación; la cual se borra cuando se reinicia o apaga el equipo.
2. **Confirmar el Ataque:** Asegurarse de que se trata de un ataque de ransomware. Los ataques de ransomware suelen mostrar una nota de rescate en la pantalla de la víctima. Tomar capturas de pantalla o fotografías de la pantalla para documentar la nota de rescate.
3. **No Pagar el Rescate:** No pagar el rescate exigido por los atacantes. No hay garantía de que se obtendrá la clave de descifrado después de realizar el pago, y pagar solo alienta a los ciberdelincuentes.
4. **Informar del Ataque:** Notificar de inmediato al equipo de seguridad de la organización o a las autoridades. Cuanto antes se informe, mejor será la respuesta y la posibilidad de rastrear a los atacantes.
5. **Restauración desde una Copia de Seguridad:** Si se cuenta con copias de seguridad actualizadas y seguras, utilizar estas copias para restaurar los datos y sistemas afectados. Asegurarse de que las copias de seguridad sean de confianza y no estén comprometidas.
6. **No Borrar Evidencia:** No apagar los equipos afectados, no borrar ningún archivo o evidencia del ataque, hasta que se haya evaluado completamente la situación y se haya informado a las autoridades. La evidencia es necesaria para iniciar la investigación.
7. **Contactar con la autoridad:** De ser víctima, contacte a las Autoridades competentes para denunciar el ciberdelito con base a la Normativa Legal Vigente.

8. **Recopilar Información:** Documentar todos los detalles del ataque, incluyendo la nota de rescate, la dirección de Bitcoin utilizada para el rescate (si está disponible), y cualquier información sobre cómo se propagó el ransomware.
9. **Escanear y Limpiar el Sistema:** Escanear el sistema afectado en busca de malware residual y limpia cualquier instancia del ransomware. Utilizar herramientas de seguridad confiables y actualizadas.
10. **Mejorar la Seguridad:** Identificar las vulnerabilidades o puntos débiles que permitieron que el ransomware infectara el sistema y tomar medidas para mejorar la seguridad, como parchear software, fortalecer contraseñas y educar a los usuarios sobre la seguridad cibernética.
11. **Mejorar el Plan de Respuesta a Incidentes:** Desarrollar y revisar un plan de respuesta a incidentes que incluya los pasos específicos a seguir en caso de futuros ataques de ransomware.
12. **Monitoreo Continuo:** Implementar un monitoreo de seguridad continuo para detectar actividades inusuales en la red y sistemas que podrían indicar un ataque en curso o intentos de infiltración futuros.
13. **Concienciación de Usuarios:** Educar a los usuarios sobre cómo identificar el ransomware y los peligros del phishing, ya que la mayoría de los ataques de ransomware comienzan con correos electrónicos maliciosos.
14. **Buscar información sobre el ransomware:** En el caso de que la organización se vea afectada por un ransomware, se puede visitar páginas especializadas en tratamiento de ese ransomware y en el mejor de los casos encontrar el descifrador (ej. www.nomoreransom.org).
15. **Establecer perfiles de usuarios** en equipos y sistemas en los cuales se otorgue derechos de administrador y acceso solo cuando sea necesario.
16. **Añadir varias capas extras de seguridad** con por ejemplo la autenticación multifactor (MFA) especialmente en los servicios críticos.
17. **Realizar periódicamente una evaluación de riesgos y análisis de brechas** para identificar y mitigar oportunamente posibles vulnerabilidades.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta; se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

https://www.infosecurity-magazine.com/news/qilin-ransomware-targets-critical/

https://www.darkreading.com/threat-intelligence/qilin-ransomware-operation-affiliate-turnkey-cyberattacks

https://www.darkreading.com/cloud-security/agenda-ransomware-vmware-esxi-servers

https://www.group-ib.com/blog/qilin-ransomware/

https://www.trendmicro.com/en_us/research/24/c/agenda-ransomware-propagates-to-vcenters-and-esxi-via-custom-pow.html

https://www.virustotal.com

https://devel.group/blog/ataque-de-ransomware-qilin-impacta-a-hospitales-en-londres/

https://www.group-ib.com/resources/knowledge-hub/dedicated-leak-sites/

https://www.incibe.es/empresas/guias/ransomware-guia-aproximacion-el-empresario