Investigadores de ciberseguridad han identificado una versión más avanzada del ransomware Qilin, que presenta un mayor nivel de sofisticación y nuevas tácticas para evitar ser detectado.

Esta nueva variante está siendo monitorizada por la firma de ciberseguridad Halcyon bajo el nombre Qilin.B.

> *«Es destacable que Qilin.B ahora implemente el cifrado AES-256-CTR en sistemas con soporte para AESNI, aunque sigue utilizando Chacha20 en aquellos que no lo tienen»,* explicó el equipo de investigación de Halcyon en un informe.
>
> *«Además, el cifrado de claves se protege mediante RSA-4096 con relleno OAEP, lo que hace imposible descifrar los archivos sin la clave privada del atacante o sin los valores de semilla capturados».*

Qilin, también conocido como Agenda, fue identificado por primera vez por la comunidad de ciberseguridad en julio/agosto de 2022. Las primeras versiones estaban desarrolladas en Golang, pero luego migraron a Rust.

Un informe de Group-IB, publicado en mayo de 2023, reveló que el esquema de ransomware como servicio (RaaS) permite a sus afiliados quedarse con entre el 80% y el 85% de los pagos de rescate, después de infiltrarse en el grupo y contactar con un reclutador de Qilin.

En los ataques más recientes vinculados a esta operación, se robaron credenciales almacenadas en navegadores Google Chrome de un pequeño número de dispositivos comprometidos, lo que marca un cambio en comparación con los típicos ataques de doble extorsión.

Las muestras de Qilin.B analizadas por Halcyon indican que esta versión se basa en iteraciones previas, añadiendo capacidades de cifrado más avanzadas y mejores tácticas

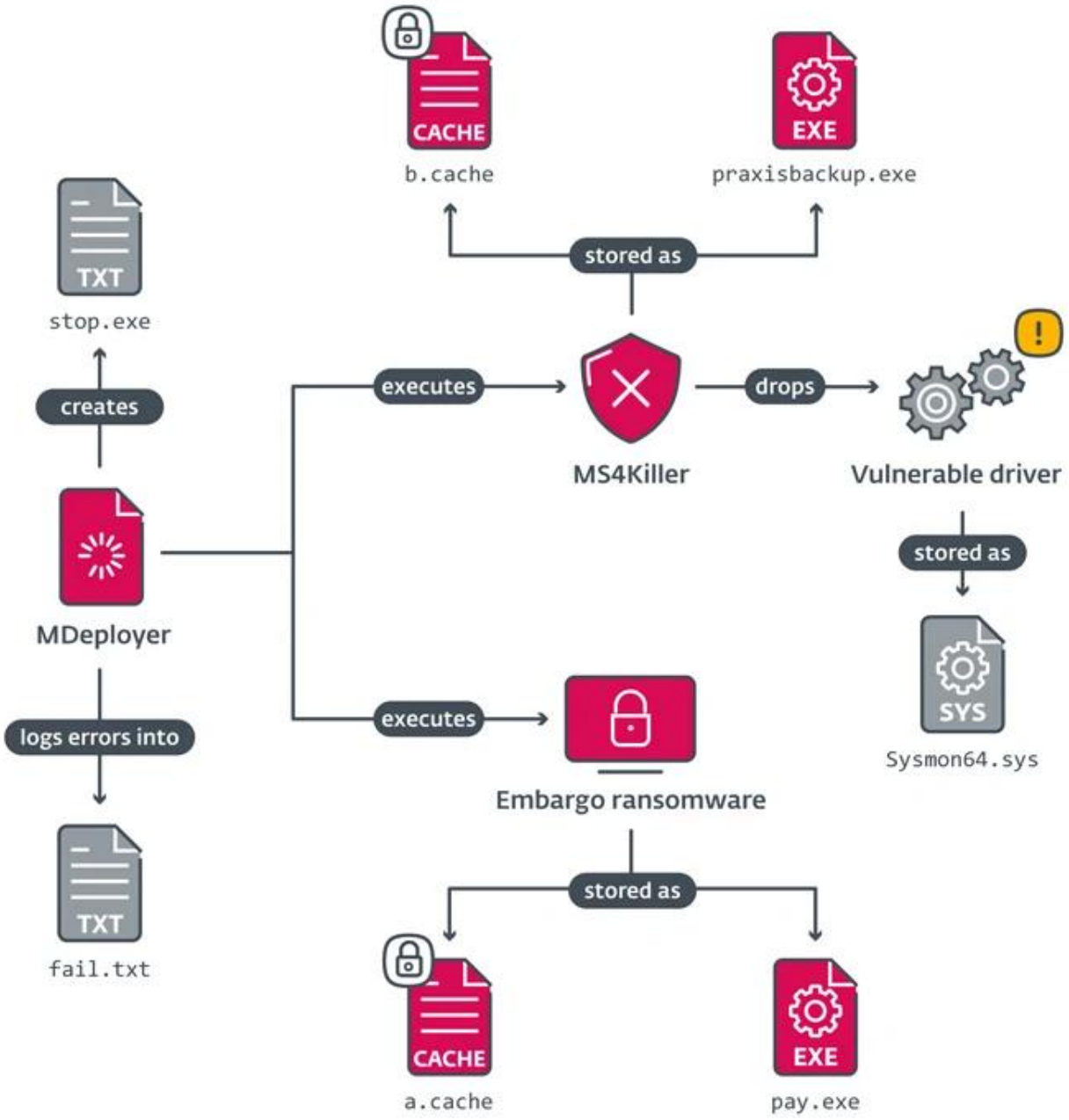
operativas.

Entre sus características, utiliza AES-256-CTR o Chacha20 para el cifrado, además de implementar medidas para dificultar el análisis y la detección, como detener servicios relacionados con herramientas de seguridad, limpiar continuamente los registros de eventos de Windows y eliminarse a sí mismo.

También tiene funciones para finalizar procesos asociados con servicios de respaldo y virtualización, como Veeam, SQL y SAP, así como eliminar copias de seguridad en sombra, lo que complica las tareas de recuperación.

> *«La combinación de mecanismos de cifrado mejorados, tácticas de evasión de defensa eficaces y la interrupción constante de los sistemas de respaldo hace que Qilin.B sea una variante de ransomware especialmente peligrosa»,* dijo Halcyon.

La evolución constante de las tácticas empleadas por los grupos de ransomware pone de manifiesto la persistencia de esta amenaza.



Un ejemplo de ello es el descubrimiento de un nuevo conjunto de herramientas basadas en Rust, que se ha utilizado para distribuir el nuevo ransomware Embargo. Antes de ejecutarse, desactiva las soluciones de detección y respuesta en los dispositivos afectados utilizando la

técnica *«Llevar tu propio controlador vulnerable»* (BYOVD).

Tanto el eliminador de EDR, llamado MS4Killer por ESET debido a su similitud con la herramienta de código abierto s4killer, como el ransomware, son ejecutados mediante un cargador malicioso conocido como MDeployer.

> *«MDeployer es el cargador malicioso principal que Embargo intenta desplegar en las máquinas de la red comprometida, facilitando el resto del ataque, que termina en la ejecución del ransomware y el cifrado de archivos. Se espera que MS4Killer se ejecute indefinidamente»*, explicaron los investigadores Jan Holman y Tomáš Zvara.
>
> *«Tanto MDeployer como MS4Killer están desarrollados en Rust. Esto también se aplica a la carga útil del ransomware, lo que sugiere que Rust es el lenguaje preferido por los desarrolladores del grupo».*

Según datos proporcionados por Microsoft, 389 instituciones de salud en los Estados Unidos han sido víctimas de ataques de ransomware en este año fiscal, lo que ha provocado pérdidas de hasta $900,000 diarios debido al tiempo de inactividad. Algunos de los grupos de ransomware conocidos por atacar hospitales incluyen Lace Tempest, Sangria Tempest, Cadenza Tempest y Vanilla Tempest.

> *«De las 99 organizaciones de salud que reconocieron haber pagado el rescate y revelaron la suma pagada, el pago mediano fue de $1.5 millones, mientras que el promedio alcanzó los $4.4 millones»,* indicó la empresa tecnológica.