Investigadores en ciberseguridad han revelado información sobre una variante de Linux de un ransomware relativamente reciente llamado Helldown, lo que indica que los atacantes están ampliando sus objetivos.

> *«Helldown utiliza ransomware para Windows basado en el código de LockBit 3.0. Dado el desarrollo reciente de ransomware enfocado en ESX, parece que este grupo podría estar adaptando sus operaciones actuales para atacar infraestructuras virtualizadas a través de VMware»*, explicó Sekoia en un informe.

Helldown fue mencionado públicamente por primera vez por Halcyon a mediados de agosto de 2024, describiéndolo como un *«grupo de ransomware altamente agresivo»* que compromete redes al explotar vulnerabilidades de seguridad. Entre los sectores afectados por este grupo criminal se encuentran servicios de TI, telecomunicaciones, manufactura y salud.

Al igual que otros grupos de ransomware, Helldown emplea sitios de filtración de datos para coaccionar a las víctimas, amenazando con publicar información robada si no se paga un rescate, una estrategia conocida como doble extorsión. Se estima que este ransomware ha atacado al menos a 31 organizaciones en un periodo de tres meses.

Truesec, en un análisis reciente, describió las cadenas de ataque de Helldown, que incluyen el uso de firewalls Zyxel expuestos a internet como punto de entrada inicial. Posteriormente, realizan acciones como establecer persistencia, robar credenciales, mapear redes, evadir defensas y moverse lateralmente antes de desplegar el ransomware.

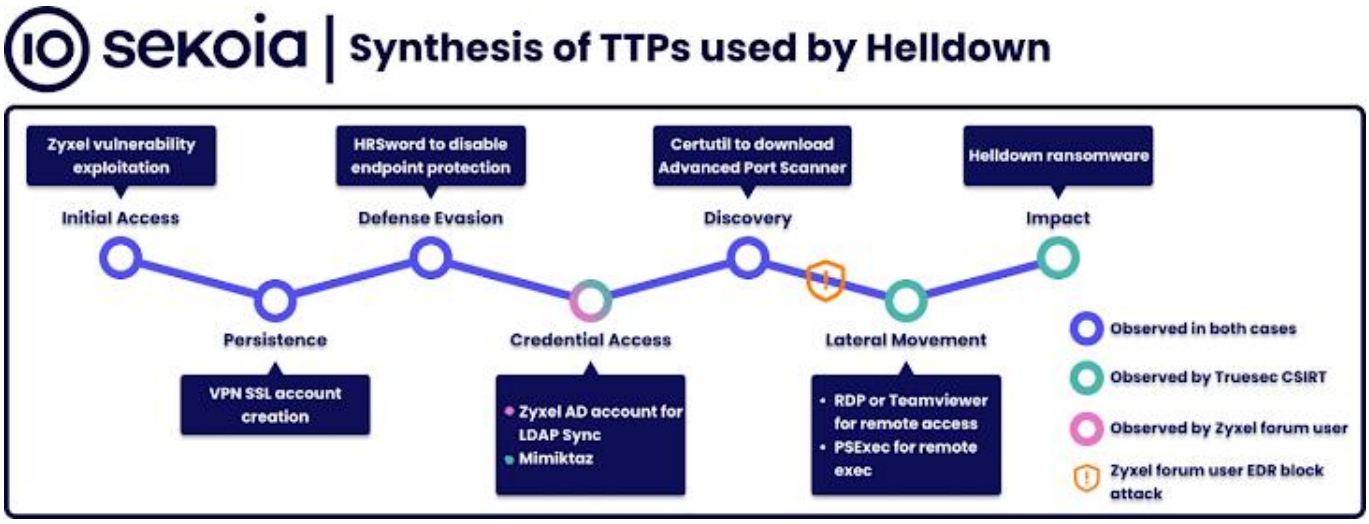
Según el análisis de Sekoia, los atacantes están explotando vulnerabilidades conocidas y desconocidas en los dispositivos Zyxel para ingresar a las redes, utilizando este acceso para obtener credenciales y configurar túneles VPN SSL con usuarios temporales.

La versión de Helldown para Windows lleva a cabo varios pasos antes de cifrar los archivos, como eliminar copias de seguridad del sistema y detener procesos de bases de datos y

aplicaciones de Microsoft Office. Finalmente, elimina su propio binario para ocultar evidencias, deja una nota de rescate y apaga el dispositivo.

En contraste, la variante de Linux, según la empresa francesa, no tiene mecanismos de ofuscación o anti-depuración, y utiliza una funcionalidad más simple para buscar y cifrar archivos. Sin embargo, antes de hacerlo, identifica y apaga todas las máquinas virtuales activas.

> *«El análisis estático y dinámico no encontró comunicación con la red ni claves públicas o compartidas. Esto es llamativo, ya que plantea dudas sobre cómo los atacantes proporcionarían una herramienta para descifrar los archivos»,* destacó el informe.



> *«Apagar máquinas virtuales antes del cifrado permite al ransomware escribir en los archivos de imagen. No obstante, aunque esta funcionalidad está presente en el código, no se activa durante los ataques observados. Estos hallazgos sugieren que este ransomware no es especialmente sofisticado y podría estar en etapas de desarrollo».*

Las muestras de Helldown para Windows muestran similitudes con DarkRace, un ransomware que apareció en mayo de 2023 utilizando código de LockBit 3.0 y que luego se renombró como DoNex. En julio de 2024, Avast lanzó un descifrador para DoNex.

> *«Ambos son variantes de LockBit 3.0. Dado el historial de DarkRace y DoNex en cambiar de nombre, y las similitudes significativas con Helldown, no se puede descartar que Helldown sea otro rebranding. Sin embargo, esta relación no puede confirmarse completamente en este momento»,* señaló Sekoia.

Por otro lado, Cisco Talos ha identificado otra familia de ransomware emergente llamada Interlock, que se ha dirigido a sectores de salud, tecnología y gobierno en los EE. UU., y a la manufactura en Europa. Este ransomware tiene la capacidad de cifrar sistemas operativos Windows y Linux.

Las cadenas de ataque que distribuyen Interlock utilizan un archivo falso de actualización del navegador Google Chrome alojado en un sitio web legítimo pero comprometido. Cuando se ejecuta, instala un troyano de acceso remoto (RAT) que permite a los atacantes extraer datos sensibles y ejecutar comandos de PowerShell para desplegar herramientas diseñadas para robar credenciales y realizar reconocimientos.

> *«En su blog, Interlock afirma atacar la infraestructura de organizaciones explotando vulnerabilidades no corregidas y asegura que sus acciones están motivadas, en parte, por responsabilizar a las empresas por sus malas prácticas de ciberseguridad, además de buscar un beneficio económico»,* indicaron los investigadores de Talos.

Se cree que Interlock podría estar vinculado a los operadores o desarrolladores de Rhysida, según el informe, debido a las similitudes en las tácticas, herramientas y el comportamiento del ransomware.

> *«La posible relación de Interlock con Rhysida encaja con las tendencias más amplias en el panorama de amenazas. Hemos observado cómo los grupos de ransomware diversifican sus capacidades para realizar operaciones más avanzadas y trabajan de manera más colaborativa entre distintos grupos»,* explicó el informe.

Además de Helldown e Interlock, ha surgido otro nuevo actor en el ecosistema de ransomware llamado SafePay, que asegura haber atacado a 22 organizaciones hasta la fecha. Según Huntress, SafePay también está basado en LockBit 3.0, lo que sugiere que la filtración del código fuente de LockBit ha generado múltiples variantes.

En dos incidentes analizados por Huntress, *«los atacantes utilizaron credenciales válidas para acceder a los sistemas de las víctimas a través de portales VPN. No se observaron acciones como habilitación de RDP, creación de cuentas de usuario o establecimiento de mecanismos de persistencia»*, concluyeron los investigadores.