Una nueva operación de ransomware como servicio (RaaS) llamada Micheael Kors, se ha convertido en el último malware de cifrado de archivos para atacar los sistemas Linux y VMware ESXi a partir de abril de 2023.

El desarrollo apunta a que los ciberdelincuentes ponen sus ojos cada vez más en el ESXi, dijo la firma de seguridad cibernética CrowdStrike en un informe.

> *«Esta tendencia es especialmente notable dado el hecho de que ESXi, por diseño, no es compatible con agentes de terceros o software AV»,* dijo la compañía.

> *«De hecho, VMware llega incluso a afirmar que no es necesario. Esto, combinado con la popularidad de ESXi como un sistema de administración y virtualización popular y generalizado, hace que el hipervisor sea un objetivo muy atractivo para los adversarios modernos».*

La selección de hipervisores VMware ESXi con ransomware para escalar tales compañías es una técnica conocida como jackpotting de hipervisor. A lo largo de los años, el enfoque ha sido adoptado por varios grupos de ransomware, incluyendo Royal.

Además, un análisis de Sentinel One la semana pasada, reveló que 10 familias de ransomware distintas, incluidas Conti y REvil, utilizaron el código fuente filtrado de Babuk en septiembre de 2021 para desarrollar casilleros para hipervisores VMware ESXi.

Otros equipos notables de ciberdelincuencia que han actualizado su arsenal para apuntar a ESXi son ALPHV (BlackCat), Black Basta, Defray, ESXiArgs, LockBit, Nevada, Play, Rook y Rorschach.

Parte de la razón por la que los hipervisores VMware ESXi se están convirtiendo en un objetivo atractivo es que el software se ejecuta directamente en un servidor físico, lo que

otorga a un atacante potencial la capacidad de ejecutar binarios ELF maliciosos y obtener acceso sin restricciones a los recursos subyacentes de la máquina.

Los atacantes que buscan violar los hipervisores ESXi pueden hacerlo usando credenciales comprometidas, y después obteniendo privilegios elevados y moviéndose lateralmente por medio de la red o escapando de los límites del entorno a través de vulnerabilidades para promover sus motivos.

VMware, en un artículo de la base de conocimientos actualizado por última vez en septiembre de 2020, dice que *«no se requiere software antivirus con vSphere Hypervisor y el uso de dicho software no es compatible».*

> *«Cada vez más actores de amenazas están reconociendo que la falta de herramientas de seguridad, la falta de una segmentación de red adecuada de las interfaces de ESXi y las vulnerabilidades [in-the-wild] para ESXi crean un entorno rico en objetivos»*, dijo CrowdStrike.

Los hackers de ransomware son de los únicos equipos que atacan la infraestructura virtual. En marzo de 2023, Mandiant, propiedad de Google, atribuyó a un grupo estatal chino el uso de puertas traseras novedosas denominadas VIRTUALPITA y VIRTUALPIE en ataques dirigidos a servidores VMware ESXi.

Para mitigar el impacto del jackpotting del hipervisor, se recomienda a las organizaciones que eviten el acceso directo a los hosts ESXi, habiliten la autenticación multifactor, realicen copias de seguridad de forma periódica de los volúmenes del almacén de datos ESXi, apliquen actualizaciones de seguridad y realicen revisiones de la postura de seguridad.

> *«Es probable que los atacantes sigan apuntando a la infraestructura de virtualización basada en VMware. Esto plantea una gran preocupación a medida que más organizaciones siguen transfiriendo cargas de trabajo e infraestructura a*

> *entornos de nube, todo por medio de entornos VMware Hypervisor»,* dijo CrowdStrike.