La Corporación MITRE ha informado que el ciberataque que apuntó a la empresa sin fines de lucro a finales de diciembre de 2023, explotando vulnerabilidades de día cero en Ivanti Connect Secure (ICS), implicó al atacante creando máquinas virtuales (VM) maliciosas dentro de su entorno VMware.

> *«El atacante creó sus propias VM maliciosas dentro del entorno VMware, utilizando el acceso comprometido al servidor vCenter,»* explicaron los investigadores de MITRE *Lex Crumpton y Charles Clancy*.
>
> *«Ellos escribieron y desplegaron un shell web JSP (BEEFLUSH) en el servidor Tomcat del servidor vCenter para ejecutar una herramienta de túnel basada en Python, facilitando conexiones SSH entre las VM creadas por el atacante y la infraestructura del hipervisor ESXi.»*

El propósito de esta acción es evitar la detección al ocultar sus actividades maliciosas de las interfaces de gestión centralizadas como vCenter y mantener un acceso persistente mientras minimizan el riesgo de ser descubiertos.

Los detalles del ataque surgieron el mes pasado cuando MITRE reveló que el actor de amenazas con vínculos en China, rastreado por Mandiant, propiedad de Google, bajo el nombre UNC5221, violó su Entorno de Experimentación en Red, Investigación y Virtualización (NERVE) explotando dos vulnerabilidades de ICS, CVE-2023-46805 y CVE-2024-21887.

Después de evadir la autenticación multifactor y obtener un punto de entrada inicial, el atacante se movió lateralmente a través de la red y utilizó una cuenta de administrador comprometida para tomar el control de la infraestructura VMware, desplegando diversas puertas traseras y shells web para mantener el acceso y robar credenciales.

Esto incluyó una puerta trasera basada en Golang llamada BRICKSTORM que estaba presente dentro de las VM maliciosas y dos shells web denominados BEEFLUSH y BUSHWALK,

permitiendo a UNC5221 ejecutar comandos arbitrarios y comunicarse con servidores de comando y control.

> *«El atacante también utilizó una cuenta predeterminada de VMware, VPXUSER, para realizar siete llamadas API que enumeraron una lista de unidades montadas y desmontadas,»* explicó MITRE.
>
> *«Las VM maliciosas operan fuera de los procesos de gestión estándar y no siguen las políticas de seguridad establecidas, lo que las hace difíciles de detectar y gestionar solo a través de la interfaz gráfica. Se necesitan herramientas o técnicas especiales para identificar y mitigar eficazmente los riesgos asociados con las VM maliciosas.»*

Una medida efectiva contra los esfuerzos sigilosos de los actores de amenazas para evitar la detección y mantener el acceso es habilitar el arranque seguro, lo que previene modificaciones no autorizadas al verificar la integridad del proceso de arranque.

La empresa también mencionó que está poniendo a disposición dos scripts de PowerShell llamados Invoke-HiddenVMQuery y VirtualGHOST para ayudar a identificar y mitigar posibles amenazas dentro del entorno VMware.

> *«A medida que los atacantes continúan evolucionando sus tácticas y técnicas, es crucial que las organizaciones se mantengan vigilantes y adaptativas en la defensa contra amenazas cibernéticas,»* concluyó MITRE.