Se descubrió que los hackers están realizando implantes posteriores al compromiso nunca antes vistos en el software de virtualización de VMware, con el fin de tomar el control de los sistemas infectados y evadir la detección.

La división de inteligencia de amenazas Mandiant de Google, se refirió a esto como *«un ecosistema de malware novedoso»* que afecta a VMware ESXi, servidores Linux vCenter y máquinas virtuales de Windows, lo que permite a los atacantes mantener un acceso persistente al hipervisor y ejecutar comandos arbitrarios.

Los ataques de hyperjacking, según el proveedor de seguridad cibernética, implicaron el uso de paquetes de instalación de vSphere (VIB) maliciosos para infiltrar dos implantes, denominados VIRTUALPITA Y VIRTUALPIE, en los hipervisores ESXi.

> *«Es importante resaltar que esta no es una vulnerabilidad de ejecución remota de código externo; el atacante necesita privilegios de nivel de administrador para el hipervisor ESXi antes de que pueda implementar malware»,* dijeron los investigadores de Mandiant, Alexander Marvi, Jeremy Koppen, Tufail Ahmed y Jonathan Lepore en un informe en dos partes

No hay evidencia de que se haya explotado una vulnerabilidad de día cero para obtener acceso a los servidores ESXi. Dicho esto, el uso de VIB troyanizados, un formato de paquete de software utilizado para facilitar la distribución de software y la gestión de máquinas virtuales, apunta a un nuevo nivel de sofisticación.

> *«Este malware se diferencia en que permite permanecer tanto persistente como encubierto, lo que es consistente con los objetivos de los atacantes más grandes y los grupos APT que se dirigen a instituciones estratégicas con la intención de permanecer sin ser detectados durante algún tiempo»,* dijo VMware.

Mientras que VIRTUALPITA viene con capacidades para ejecutar comandos, así como para cargar y descargar archivos, VIRTUALPIE es una backdoor de Python con soporte para la ejecución de línea de comandos, transferencia de archivos y funciones de shell inverso.

También se descubrió una muestra de malware llamada VIRTUALGATE en máquinas virtuales invitadas de Windows, que es un programa de utilidad basado en C que ejecuta una carga útil integrada capaz de usar los sockets de la interfaz de comunicación de máquina virtual (VMCI) de VMware, para ejecutar comandos en una máquina virtual invitada desde un hipervisor anfitrión.

Mandiant también advirtió que las técnicas de la campaña para eludir los controles de seguridad tradicionales al explotar el software de virtualización representan una nueva superficie de ataque que probablemente sea detectada por otros grupos de hackers.

Los ataques se han atribuido a un grupo de amenazas emergentes sin categorizar, con nombre en código UNC3886, cuya motivación probablemente esté impulsada por el espionaje, considerando la naturaleza altamente específica de las intrusiones. Además, evaluó con baja confianza que UNC3886 tiene un nexo con China.