Se ha observado que se está explotando una vulnerabilidad ya parcheada en VMware Workspace ONE Access para entregar mineros de criptomonedas y ransomware en las máquinas afectadas.

> *«El atacante tiene la intención de usar los recursos de la víctima tanto como sea posible, no solo para instalar RAR1Ransom para la extorsión, sino también para difundir GuardMiner para recolectar criptomonedas»,* dijo Cara Lin, investigadora de Fortinet FortiGuard Labs.

La vulnerabilidad, rastreada como CVE-2022-22954 (puntuación CVSS: 9.8), se refiere a una falla de ejecución remota de código que se deriva de un caso de inyección de plantilla del lado del servidor. Aunque el proveedor de servicios de virtualización abordó la deficiencia en abril de 2022, desde entonces ha estado bajo explotación activa en la naturaleza.

Fortinet dijo que observó en agosto de 2022 ataques que buscan armar la falla para implementar la botnet Mirai en dispositivos Linux, así como RAR1Ransom y GuardMiner, una variante del minero XMRig Monero.

La muestra de Mirai se recupera de un servidor remoto y está dieñada para lanzar ataques de denegación de servicio (DoS) y de fuerza bruta dirigidos a dispositivos IoT conocidos mediante el uso de una lista de credenciales predeterminadas.

La distribución de RAR1Ransom y GuardMiner, por otro lado, se logra mediante un PowerShell o un script de shell dependiendo del sistema operativo. RAR1Ransom también se destaca por aprovechar la utilidad legítima WinRAR para bloquear archivos mediante contraseña.

Además, GuardMiner viene con capacidades para propagarse a otros hosts al aprovechar las

vulnerabilidades de una serie de fallas de ejecución remota de código en otro software, incluyendo los de Apache Struts, Atlassian Confluence y Spring Cloud Gateway.

Los hallazgos son otro recordatorio de que las campañas de malware siguen explotando activamente las vulnerabilidades reveladas recientemente para ingresar a los sistemas sin parches, por lo que es esencial que los usuarios den prioridad a la instalación de actualizaciones de seguridad.