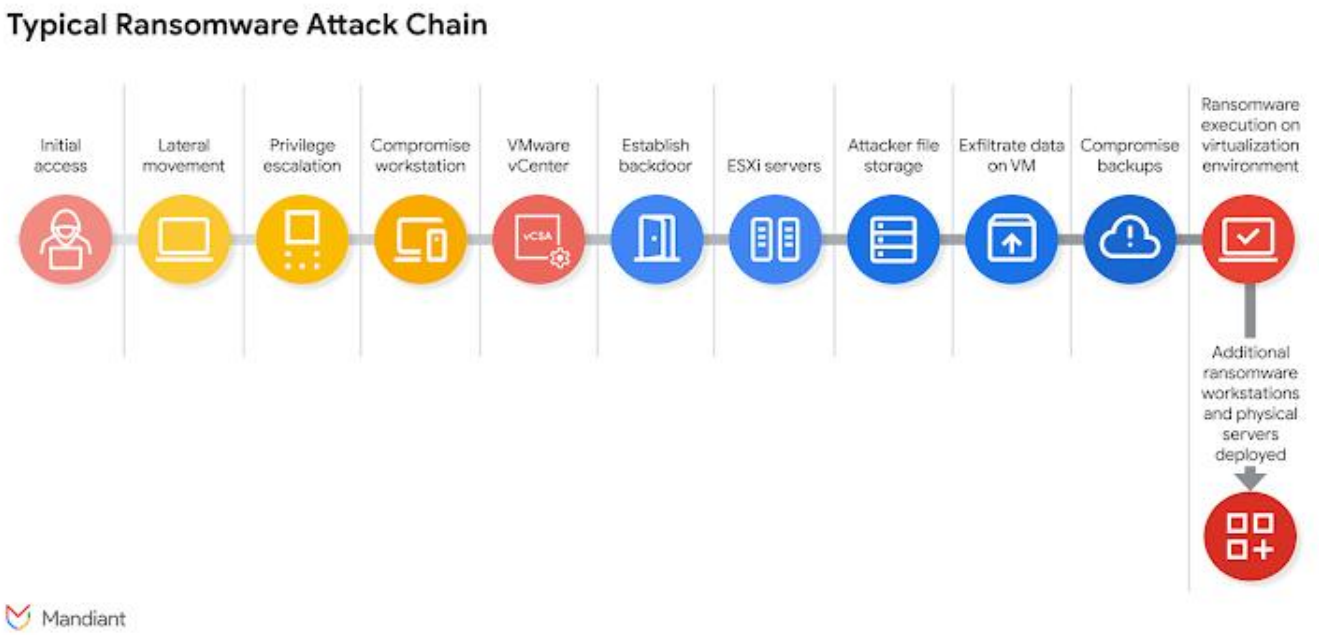
El notorio grupo de ciberdelincuentes conocido como Scattered Spider está dirigiendo ataques contra hipervisores VMware ESXi, enfocándose en los sectores de comercio minorista, aerolíneas y transporte en América del Norte.

"Las tácticas principales del grupo se han mantenido constantes y no dependen de la explotación de vulnerabilidades en software. En su lugar, utilizan un método probado basado en llamadas telefónicas al servicio de asistencia técnica de TI", indicó el equipo de Mandiant de Google en un análisis detallado.

"Los actores son agresivos, ingeniosos y muestran una gran habilidad para emplear la ingeniería social con el fin de evadir incluso programas de seguridad maduros. Sus ataques no son aleatorios, sino campañas planificadas y dirigidas a los sistemas y datos más críticos de una organización."

También identificados como 0ktapus, Muddled Libra, Octo Tempest y UNC3944, estos actores de amenaza tienen un historial de ataques sofisticados mediante ingeniería social para obtener acceso inicial a los entornos de sus víctimas. Posteriormente, adoptan un enfoque de *"vivir de la tierra"* (*living-off-the-land*, LotL), manipulando sistemas administrativos confiables y aprovechando el control del Active Directory para acceder al entorno de VMware vSphere.

Google señaló que esta técnica, que permite la exfiltración de datos y el despliegue de ransomware directamente desde el hipervisor, es *"altamente efectiva"*, ya que evita las herramientas de seguridad y deja escasos rastros del compromiso.



La cadena de ataque se desarrolla en cinco fases distintas:

1. Compromiso inicial, reconocimiento y escalamiento de privilegios, permitiendo a los atacantes recopilar información relacionada con documentación de TI, manuales de soporte, organigramas y administradores de vSphere. También identifican credenciales almacenadas en gestores como HashiCorp Vault u otras soluciones de gestión de acceso privilegiado (PAM). Los atacantes suelen hacer llamadas adicionales al soporte técnico de la empresa, haciéndose pasar por administradores de alto nivel para solicitar el restablecimiento de contraseñas.
2. Acceso al entorno virtual mediante el uso de credenciales obtenidas de Active Directory para ingresar al VMware vCenter Server Appliance (vCSA). Luego ejecutan *teleport*, una herramienta que crea un shell inverso persistente y cifrado que evita las reglas del firewall.
3. Habilitación de conexiones SSH en los hosts ESXi, restablecimiento de contraseñas root, y ejecución de un ataque llamado *"disk-swap"* para extraer la base de datos NTDS.dit de Active Directory. Este ataque consiste en apagar una máquina virtual del

controlador de dominio (DC), desacoplar su disco virtual y conectarlo a otra VM no monitoreada bajo su control. Una vez copiado el archivo, el proceso se revierte y el DC se vuelve a encender.
4. Sabotaje del entorno de respaldo, eliminando tareas de copia de seguridad, instantáneas y repositorios para dificultar la recuperación.
5. Despliegue de ransomware, utilizando el acceso SSH a los hosts ESXi para transferir su binario personalizado mediante SCP o SFTP.

"El manual de operaciones de UNC3944 exige un cambio fundamental en la estrategia defensiva, pasando de la caza de amenazas basada en EDR a una defensa proactiva centrada en la infraestructura", señaló Google. *"Esta amenaza se diferencia del ransomware tradicional en entornos Windows en dos aspectos: velocidad y sigilo."*

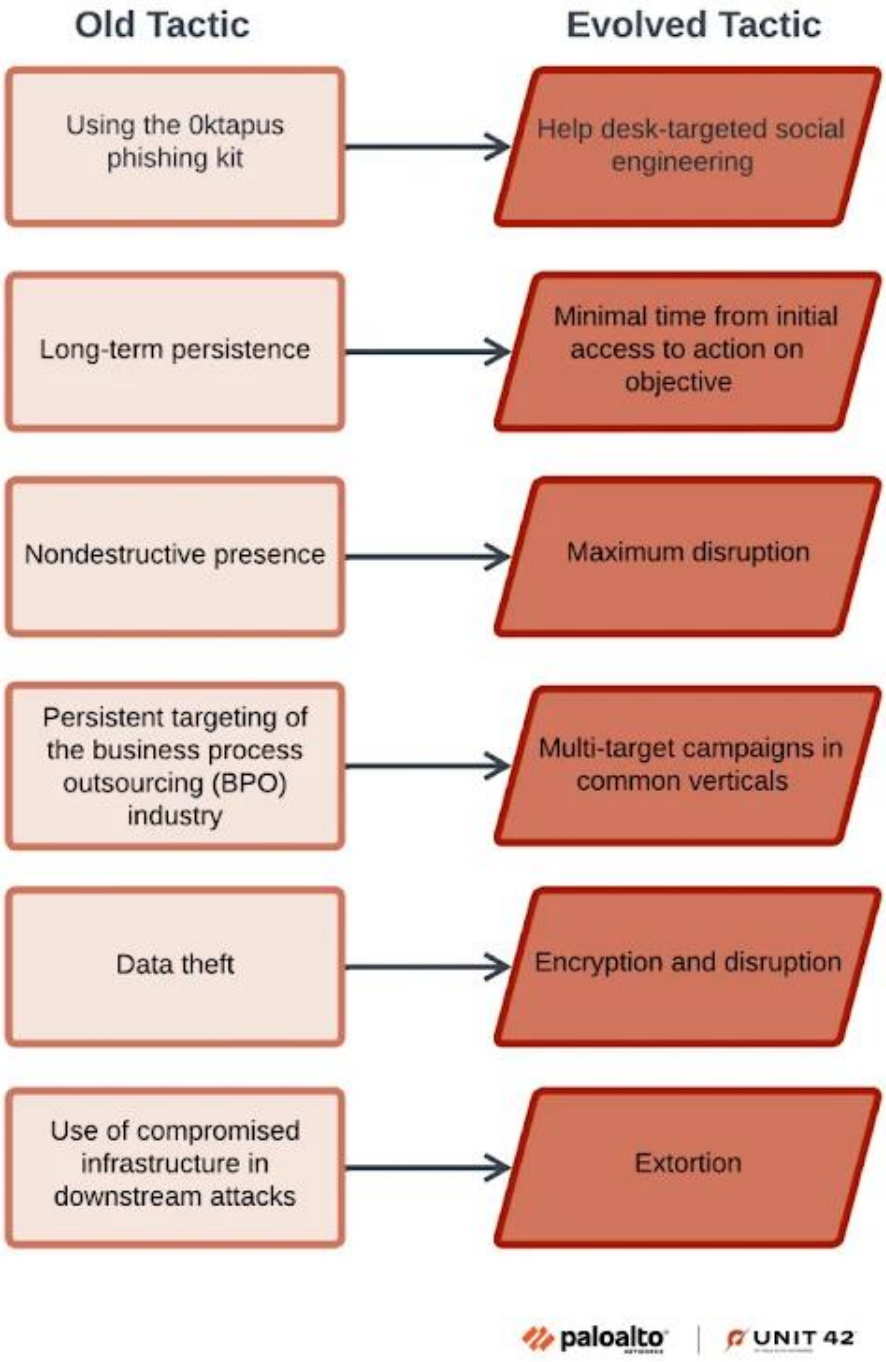
La empresa tecnológica también destacó la *"velocidad extrema"* del grupo, indicando que toda la secuencia, desde el acceso inicial hasta la exfiltración de datos y el despliegue final del ransomware, puede completarse en pocas horas.

De acuerdo con Unit 42 de Palo Alto Networks, los actores de Scattered Spider no solo han perfeccionado sus técnicas de ingeniería social, sino que también se han aliado con el grupo responsable del ransomware DragonForce (también conocido como *Slippery Scorpius*). En un caso, llegaron a exfiltrar más de 100 GB de datos en apenas dos días.

Para enfrentar estas amenazas, se recomienda implementar una estrategia de defensa en tres niveles:

- Activar el modo de bloqueo de vSphere, forzar el uso de *execInstalledOnly*, cifrar las máquinas virtuales, retirar VMs antiguas y reforzar el soporte técnico.
- Implementar autenticación multifactor resistente al *phishing*, aislar la infraestructura crítica de identidad y evitar bucles de autenticación.
- Centralizar y monitorear los registros clave, aislar las copias de seguridad del Active Directory en producción y asegurar que no sean accesibles para cuentas comprometidas.

Google también está instando a las organizaciones a rediseñar sus sistemas con un enfoque centrado en la seguridad, especialmente durante la transición desde VMware vSphere 7, cuya vida útil llegará a su fin en octubre de 2025.



"El ransomware dirigido a la infraestructura vSphere, que incluye tanto los hosts ESXi como el servidor vCenter, representa un riesgo excepcionalmente grave debido a su capacidad

para paralizar de inmediato y de forma generalizada toda la infraestructura," advirtió Google.

"No abordar de forma proactiva estos riesgos interconectados mediante la aplicación de las mitigaciones recomendadas dejará a las organizaciones vulnerables frente a ataques dirigidos, capaces de inutilizar rápidamente toda su infraestructura virtualizada, causando interrupciones operativas y pérdidas económicas."