El actor de amenazas conocido como Muddled Libra ha sido observado atacando de manera activa aplicaciones de software como servicio (SaaS) y entornos proveedores de servicios en la nube (CSP) con el objetivo de extraer datos confidenciales.

> *«Las empresas suelen almacenar una diversidad de datos en aplicaciones SaaS y utilizan servicios de CSP»,* señaló Palo Alto Networks Unit 42 en un informe emitido la semana pasada.
>
> *«Estos actores de amenazas han comenzado a intentar aprovechar parte de estos datos para facilitar la progresión de sus ataques y para utilizarlos en intentos de extorsión al tratar de obtener beneficios de su trabajo».*

Muddled Libra, también conocido como Starfraud, UNC3944, Scatter Swine y Scattered Spider, es un grupo de cibercriminales notorio que ha hecho uso de técnicas sofisticadas de ingeniería social para obtener acceso inicial a redes objetivo.

> *«Los actores de amenazas de Scattered Spider han logrado históricamente evadir la detección en redes objetivo mediante el uso de técnicas de camuflaje y aplicaciones aprobadas para navegar por las redes de las víctimas, además de modificar frecuentemente sus procedimientos tácticos y técnicos»*, declaró el gobierno de Estados Unidos en un aviso emitido a finales del año pasado.

Estos atacantes también tienen un historial de monetización del acceso a las redes de las víctimas de diversas maneras, incluyendo la extorsión facilitada por ransomware y el robo de datos.

Unit 42 previamente informó que el apodo «Muddled Libra» proviene de la *«confusa y compleja red de amenazas»* asociada con el kit de phishing 0ktapus, el cual ha sido utilizado

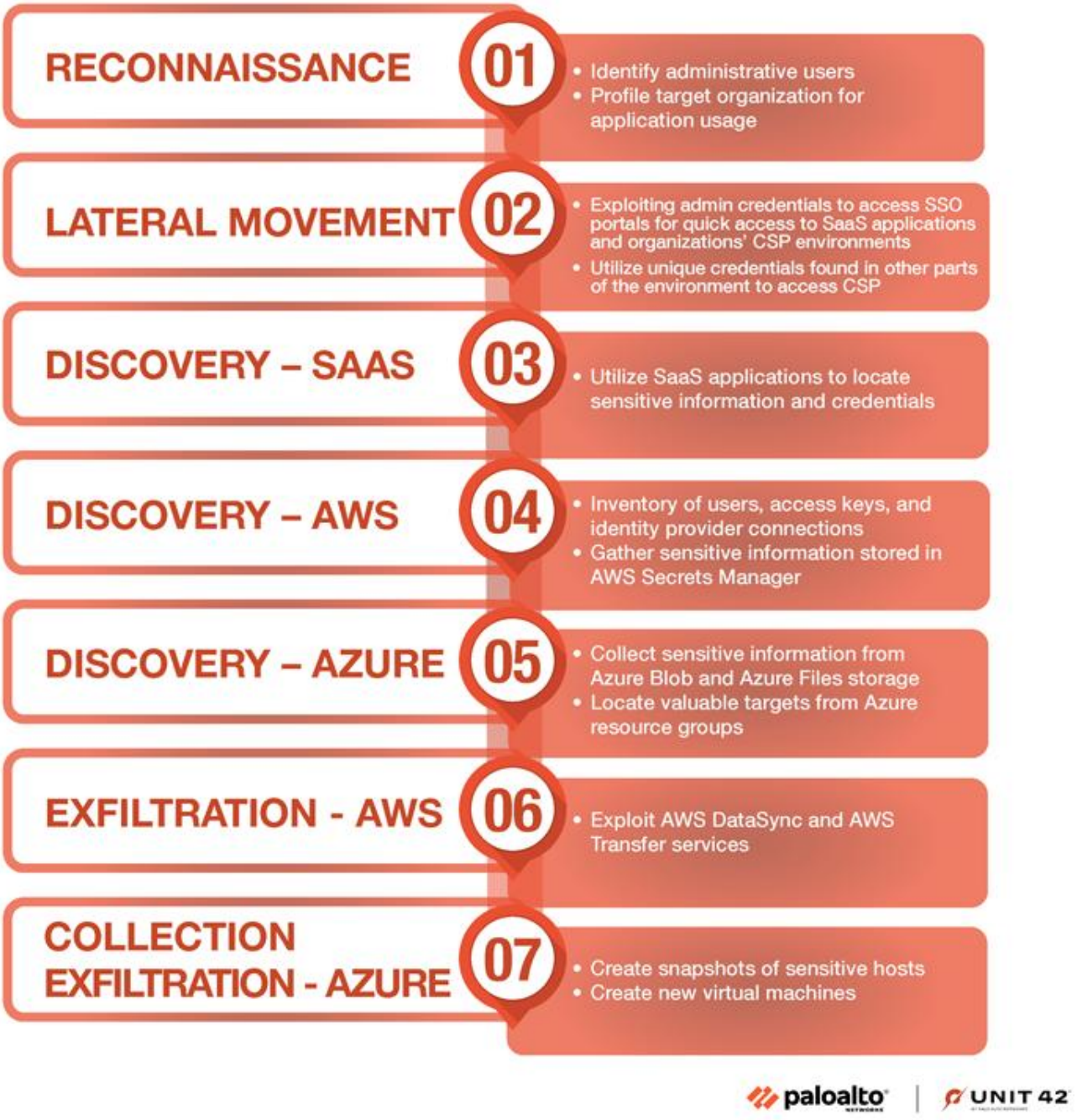
por otros actores de amenazas para llevar a cabo ataques de suplantación de identidad.

Un aspecto crucial de la evolución táctica del actor de amenazas es el uso de técnicas de reconocimiento para identificar usuarios administrativos a los cuales atacar haciéndose pasar por personal de ayuda mediante llamadas telefónicas para obtener sus contraseñas.

La fase de reconocimiento también abarca a Muddled Libra, el cual lleva a cabo una investigación exhaustiva para encontrar información sobre las aplicaciones y proveedores de servicios en la nube utilizados por las organizaciones objetivo.

> *«Los ataques de suplantación de identidad cruzada de Okta que ocurrieron desde finales de julio hasta principios de agosto de 2023, en los cuales Muddled Libra eludió las restricciones de IAM, demuestran cómo este grupo explota Okta para acceder a aplicaciones SaaS y a los diversos entornos de CSP de una organización»,* explicó la investigadora de seguridad Margaret Zimmermann.

La información obtenida en esta etapa sirve como un punto de partida para realizar movimientos laterales, aprovechando las credenciales de administrador para acceder a portales de inicio de sesión único (SSO) y obtener acceso rápido a aplicaciones SaaS e infraestructura en la nube.



En el caso de que la autenticación única (SSO) no esté incorporada en el CSP de un objetivo, Muddled Libra lleva a cabo amplias actividades de búsqueda para descubrir las credenciales

del CSP, posiblemente almacenadas en lugares no seguros, para alcanzar sus metas.

Los datos almacenados en las aplicaciones SaaS también son utilizados para obtener detalles sobre el entorno infectado, capturando tantas credenciales como sea posible para ampliar el alcance de la brecha mediante la escalada de privilegios y el movimiento lateral.

> *«Una parte considerable de las campañas de Muddled Libra implica recolectar inteligencia y datos. Los atacantes luego emplean esta información para generar nuevos métodos de movimiento lateral dentro de un entorno. Las organizaciones almacenan una variedad de datos dentro de sus propios entornos CSP, lo que convierte a estos lugares centralizados en un objetivo principal para Muddled Libra»,* expresó Zimmermann.

Estas acciones están dirigidas específicamente a Amazon Web Services (AWS) y Microsoft Azure, atacando servicios como AWS IAM, Amazon Simple Storage Service (S3), AWS Secrets Manager, claves de acceso a cuentas de almacenamiento de Azure, Azure Blob Storage y Azure Files para extraer datos pertinentes.

La extracción de datos hacia una entidad externa se logra mediante el abuso de los servicios y características legítimas del CSP. Esto incluye herramientas como AWS DataSync, AWS Transfer y una técnica denominada «snapshot«, esta última de las cuales permite mover datos fuera de un entorno de Azure al alojar los datos robados en una máquina virtual.

El cambio táctico de Muddled Libra implica que las organizaciones aseguren sus portales de identidad con sólidas protecciones de autenticación secundaria, como tokens de hardware o biometría.

> *«Al expandir sus tácticas para incluir aplicaciones SaaS y entornos en la nube, la evolución de la metodología de Muddled Libra muestra la complejidad de los ciberataques en el paisaje de amenazas moderno. El uso de entornos en la nube*

> *para recolectar grandes cantidades de información y exfiltrarla rápidamente presenta nuevos desafíos para los defensores»,* concluyó Zimmermann.