Uber data breach

El 15 de septiembre de 2022 la compañía Uber sufrió una brecha de seguridad donde un atacante alcanzó privilegios de administrador; sospechándose que pudo acceder a información reservada, incluyendo el código fuente de sus aplicaciones. Aunque no es pública toda la información relativa al incidente, en el siguiente diagrama podemos ver la secuencia seguida por el asaltante usando las tácticas/técnicas de la matriz MITRE con la información conocida:

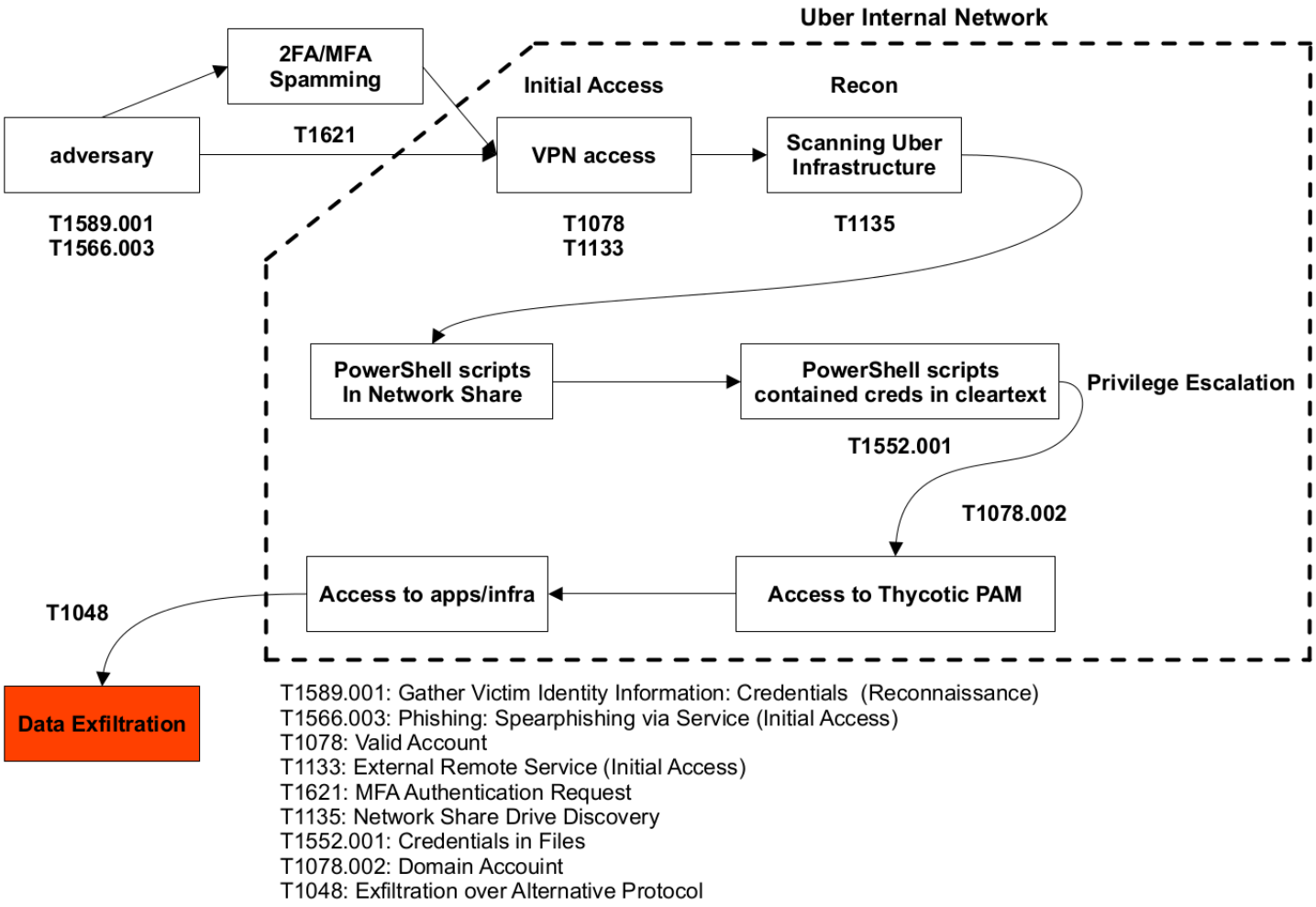

Fig. Uber data breach (2022)

La secuencia se puede resumir en los siguientes pasos:

1. Descubrimiento de credenciales de la víctima (T1589.001: Gather Victim Identity Information: Credentials - Reconnaissance)
   - el atacante compró las credenciales de un usuario en la *dark web*
   - o con *phishing* le convenció para acceder a un sitio web falso de Uber de forma que descubrió sus credenciales.
2. Un primer intento de acceso a la red de Uber mediante VPN falló porque la cuenta está protegida mediante MFA.
3. El atacante simulando ser un miembro del equipo de seguridad de Uber y a través de mensajes al

whatsapp del empleado T1566.003: Phishing: Spearphishing via Service, lanzó un ataque de fatiga (introdujo muchas veces las credenciales correctas en el sitio real de Uber lo que provocó una avalancha de mensajes de confirmación hasta que el empleado, confuso o cansado, aceptó la conexión) logrando saltarse el sistema de autenticación de varios factores (2FA/MFA).

4. Al permitir la VPN de Uber conexiones simultáneas desde cualquier parte del mundo, el atacante consigue acceder por VPN a la red interna de Uber (T1133: External Remote Service - Initial Access).
5. Una vez dentro de la infraestructura realizó un reconocimiento en busca información (TA0007: Discovery) y localizó unos *scripts* en *powershell* en una carpeta compartida en la red.
6. Estos *scripts powershell* tenían dentro credenciales de administrador para automatizar el acceso a algunos servicios de red.
7. Esas nuevas credenciales le permiten el acceso a información/aplicaciones como usuario administrador (Thycotic, VMWare vSphere, SentinelOne, AWS, Slack, GSuite, ...).
8. Aunque no se ha revelado si se produjo una exfiltración de información, el atacante publicó un mensaje en Slack para informar a los trabajadores de Uber de la intrusión y quejarse del bajo salario que se le paga a los conductores.