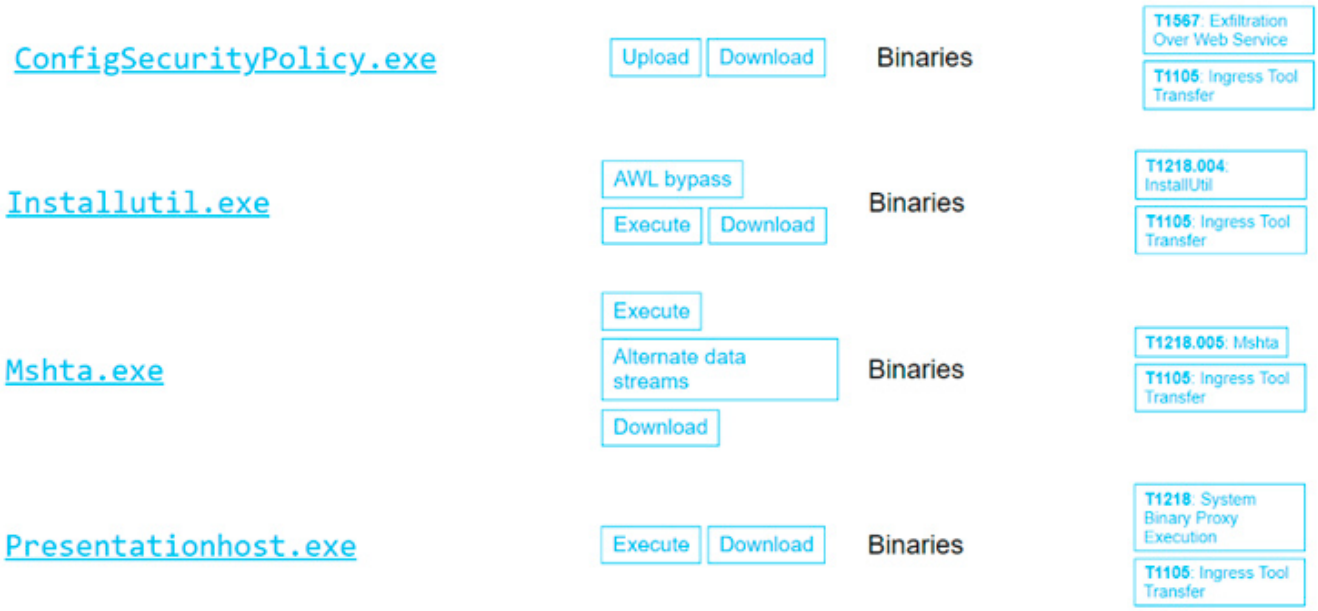
Expertos en ciberseguridad han encontrado un conjunto de 11 binarios y guiones de «*living-off-the-land*» (LOLBAS) que podrían ser aprovechados de manera maliciosa por actores de amenazas para llevar a cabo actividades posteriores a la explotación.

> *«LOLBAS es un método de ataque que emplea binarios y guiones que ya forman parte del sistema con propósitos maliciosos. Esto dificulta que los equipos de seguridad distingan entre actividades legítimas y maliciosas, dado que todas son realizadas por utilidades de sistema confiables»,* afirmó Nir Chako, investigador de seguridad de Pentera.

En este sentido, la empresa de ciberseguridad israelí informó que ha descubierto nueve descargadores LOLBAS y tres ejecutores que podrían permitir a los adversarios descargar y ejecutar *«malware más sólido»* en hosts infectados.

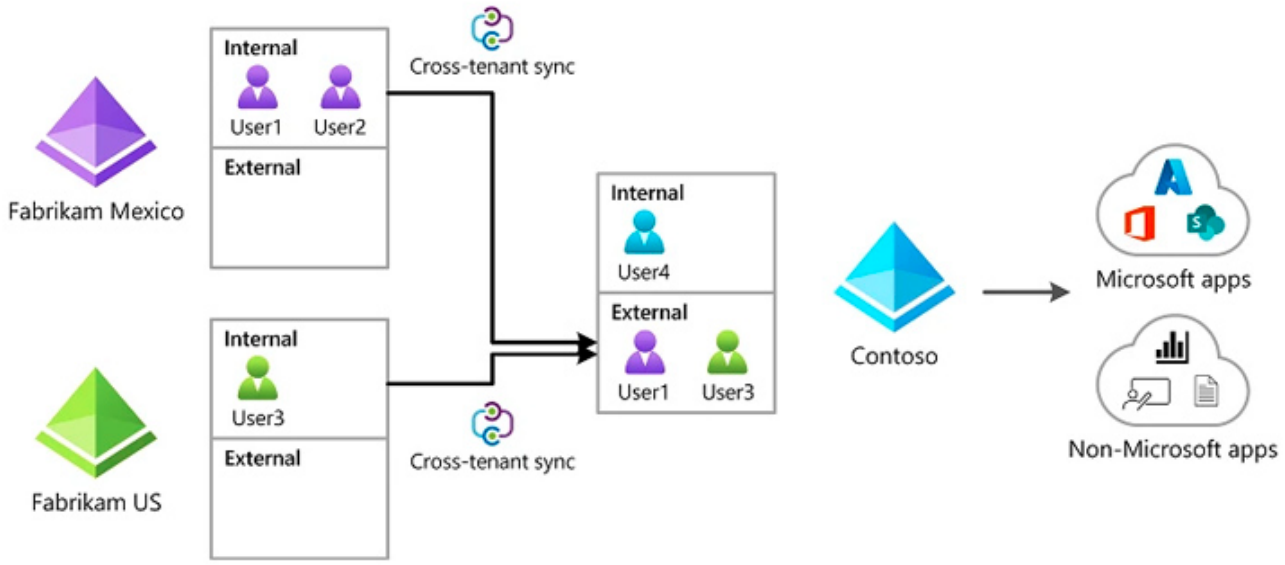
Estos incluyen: MsoHtmEd.exe, Mspub.exe, ProtocolHandler.exe, ConfigSecurityPolicy.exe, InstallUtil.exe, Mshta.exe, Presentationhost.exe, Outlook.exe, MSAccess.exe, scp.exe y sftp.exe.

> *«En una secuencia de ataque completa, un hacker empleará un descargador LOLBAS para obtener un malware más potente. Luego, intentarán ejecutarlo de manera sigilosa. Los ejecutores LOLBAS permiten a los atacantes ejecutar sus herramientas maliciosas como parte de un árbol de procesos que parece legítimo en el sistema»,* explicó Chako.



Sin embargo, Pentera resaltó que los atacantes también podrían recurrir a otros ejecutables de software aparte de los relacionados con Microsoft para lograr objetivos similares.

Estos hallazgos coinciden con la revelación de Vectra de un nuevo posible vector de ataque que aprovecha la característica de sincronización entre inquilinos (CTS, por sus siglas en inglés) de Microsoft Entra ID (anteriormente Azure Active Directory) para facilitar el movimiento lateral hacia otros inquilinos, partiendo de la suposición de que ya se ha comprometido una identidad privilegiada en el entorno en la nube.



> *«Un atacante que opera en un entorno comprometido puede explotar una configuración de CTS existente en un inquilino para moverse lateralmente de un inquilino a otro conectado. Un atacante que opera en un inquilino comprometido puede implementar una configuración de Acceso entre Inquilinos Falso para mantener un acceso persistente»,* señaló la empresa.