

Tp 8 Guillaume Sanchez

	N° Technique	Explications
Prospecter	T1083	WannaCry recherche des fichiers utilisateur par extension avant de les chiffrer, incluant des documents Office, PDF, images, audio, vidéo, code source, archives, et certificats.
Pénétrer	T1210	WannaCry exploite une vulnérabilité SMBv1 (EternalBlue) pour accéder à des systèmes distants et se propager.
Pérenniser	T1222.001	WannaCry modifie les permissions de fichiers pour les rendre cachés et accorde un contrôle total à tous les utilisateurs.
Propager	T1570	Après avoir exploité SMB, WannaCry tente de se copier sur d'autres ordinateurs du réseau.
Paralyser	T1490	Le logiciel supprime les fonctionnalités de récupération du système en utilisant des outils comme vssadmin, wbadmin, bcdedit et wmic.