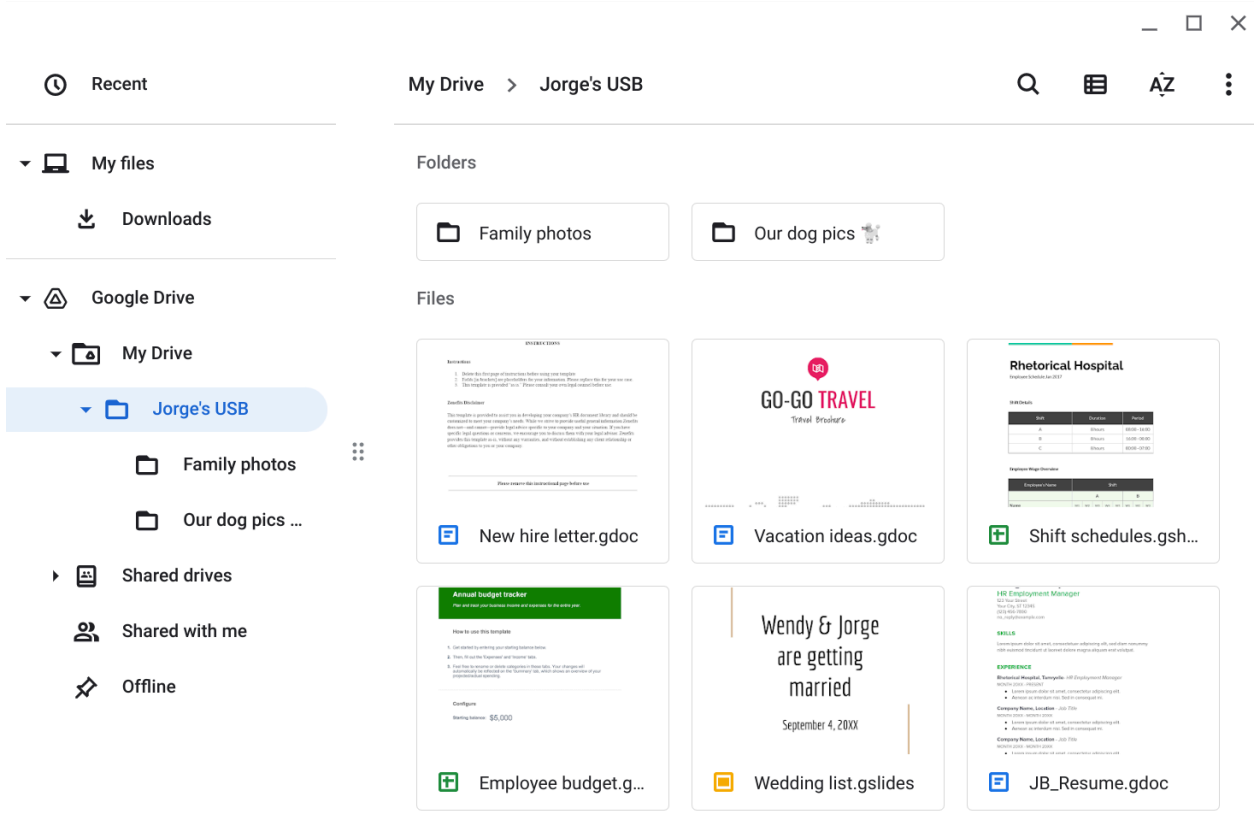
Scénario :

Vous faites partie de l'équipe de sécurité de l'Hôpital Rhétorique et vous arrivez au travail un matin. Sur le sol du parking, vous trouvez une clé USB avec le logo de l'hôpital imprimé dessus. Il n'y a personne d'autre aux alentours qui pourrait l'avoir laissé tomber, alors, par curiosité, vous décidez de la ramasser.

Vous rapportez la clé USB à votre bureau, où l'équipe dispose d'un logiciel de virtualisation installé sur un poste de travail. Le logiciel de virtualisation peut être utilisé précisément à cette fin, car c'est l'un des seuls moyens d'examiner en toute sécurité une clé USB inconnue. Le logiciel fonctionne en exécutant une instance simulée de l'ordinateur sur le même poste de travail. Cette simulation n'est pas connectée aux autres fichiers ni aux réseaux, de sorte que la clé USB ne peut pas affecter d'autres systèmes si elle contient un logiciel malveillant.

Contenus	La clé USB contient des données sensibles, notamment des informations personnelles sur le personnel de l'hôpital. On y trouve aussi des documents de travail comme les plannings des équipes et des informations budgétaires. Mélanger des fichiers personnels avec des fichiers professionnels sur un même support représente un risque de sécurité.
Attacker mindset	Ces données pourraient être utilisées pour nuire à Jorge, à d'autres employés ou à leurs proches. Elles pourraient aussi permettre un accès frauduleux aux activités de l'hôpital ou servir à faire chanter Jorge pour obtenir d'autres informations personnelles (numéros de carte, etc.).
Analyse des risques	Un malware caché sur une clé USB comme un cheval de Troie, un ransomware ou un keylogger, pourrait se propager, entraînant vol de données, chiffrement de fichiers ou compromission des systèmes. Les informations sensibles présentes sur ces dispositifs pourraient être exploitées pour des usurpations d'identité, fraude, chantage ou accès non autorisé aux systèmes de l'hôpital, causant des impacts graves sur les individus et l'organisation. Pour atténuer ce type de risque, il est essentiel de combiner des contrôles techniques, opérationnels et managériaux, comme l'analyse des supports externes dans des environnements isolés, la désactivation de l'exécution automatique des périphériques USB, la formation du personnel et la mise en place de politiques strictes de gestion des accès et des supports sensibles.

Ressources :


Recent
My Drive
Jorge's USB
My files
Downloads
Google Drive
My Drive
Jorge's USB
Family photos
Our dog pics ...
Shared drives
Shared with me
Offline
Folders
Family photos
Our dog pics
Files
New hire letter.gdoc
GO-GO TRAVEL
Travel Brochure
Vacation ideas.gdoc
Rhetorical Hospital
Shift schedules.gsh...
Annual budget tracker
Employee budget.g...
Wendy & Jorge are getting married
September 4, 20XX
Wedding list.gslides
JB_Resume.gdoc