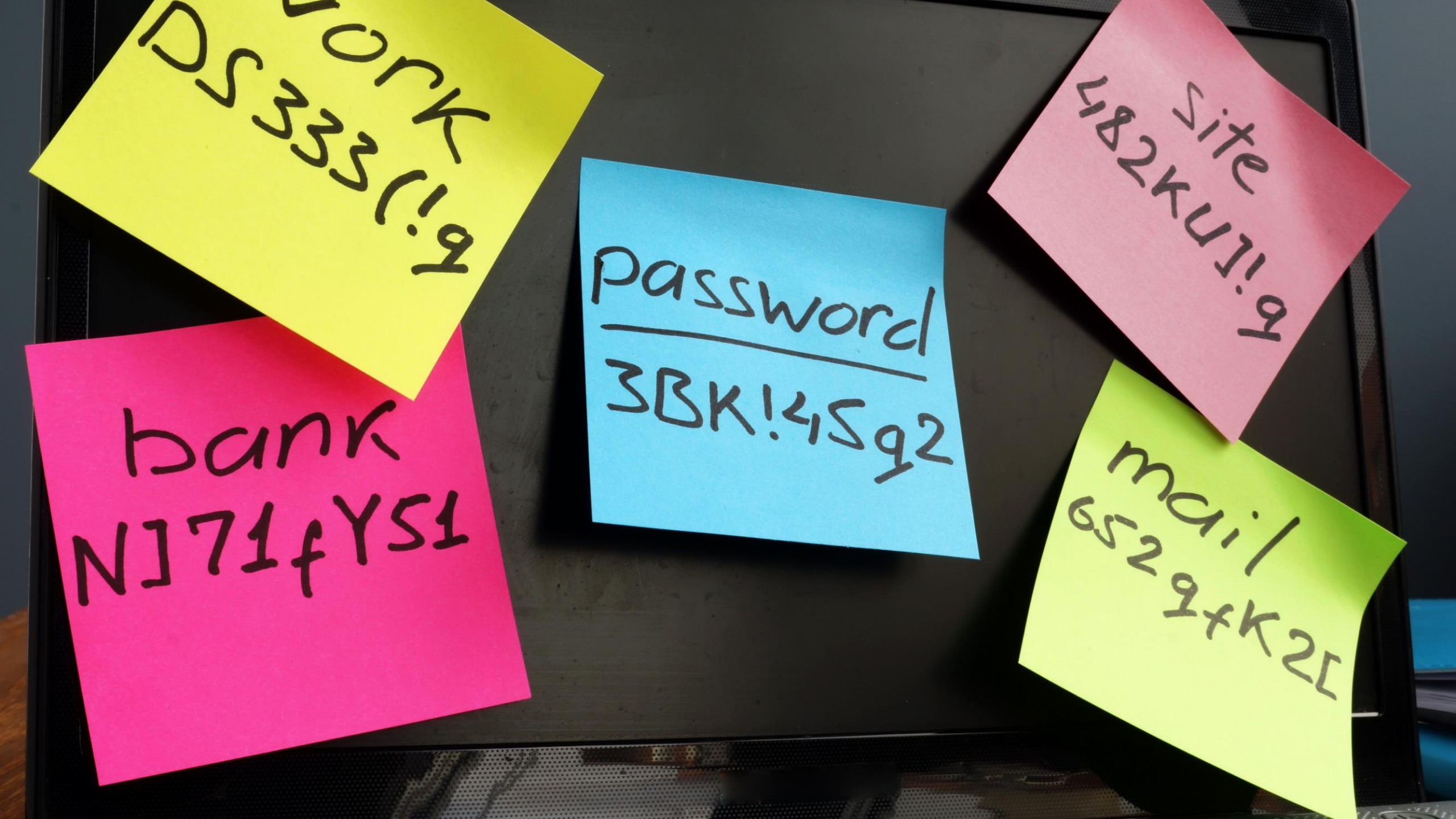

work
DS33(!9
site
482KU1!9
password
3BK!4Sq2
bank
N]71fY51
mail
652q+K2[

“ Plus de **80 %** des violations liées au piratage impliquent la force brute ou des informations d'identification perdues et volées ”

Verizon’s Data Breach Investigations Report

Mots de passe = la premiere ligne de défense

- Les utilisateurs et leurs informations d'identification constituent votre première ligne de défense contre les cyberattaques
- Le mot de passe ne va pas disparaître de sitôt
- Les pirates multiplient ce à quoi ils ont accès une fois à l'intérieur du réseau
- L'accès peut être obtenu en quelques secondes
- Un seul mot de passe compromis peut être la cause d'une violation

SPECOPS
AN OUTPOST24 COMPANY

Attaque de mot de passe / Matrice des menaces

Tactiques de prévention	Attaque de force brute	Attaque par dictionaire	Pulvérisation de mot de passe	Bourrage d'informations d'identification	Phishing	Attaque d'enregistreur de frappe (Keylogger Attack)	Ingénierie sociale	Réinitialisation du mot de passe	Noter sur un papier	Réutilisation du mot de passe
Verrouillage du compte	X			X						
Formation de sensibilisation					X	X	X	X	X	X
Blocage des modèles incrémentiels / communs	X	X	X	X						X
Blocage des périphériques USB inconnus						X				
Protection par mot de passe compromis / dictionnaire personnalisé	X	X	X	X						X
Configuration des bannières email					X					
Configuration du serveur de messagerie					X					
Protection contre les URL malveillantes						X				
MFA	X	X	X	X	X	X	X	X		
Longueur du mot de passe / phrases de passe > 20 caractères	X	X	X						X	X
Gestionnaires de mots de passe						X			X	X
Réinitialisation de mots de passe en libre-service avec MFA								X		
Protection à jour contre les logiciels malveillants						X				
Vérification / MFA auprès du helpdesk								X		

Nouvelles recommandations de la CNIL – 17/10/2022

CNIL.

COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

SPECOPS
AN OUTPOST24 COMPANY

Liste de mots interdits / mots de passe connus

Ministère des Solidarités et de la Santé

AGENCE DU NUMÉRIQUE EN SANTÉ

CERT Santé

ACCUEIL | ACTUALITÉS | ESPACE DOCUMENTAIRE | AIDE AU SIGNALEMENT | LIENS UTILES | CYBER-SURVEILLANCE | CONTACT | SE CONNECTER

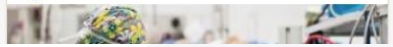
Alertes

vulnérabilité critique exploitée dans des produits Fortinet
CVE-2022-40684 **[Score CVSS v3.1: 9.8]**
Une faille de contournement d'authentification sur l'interface d'administration des produits FortiGate, FortiProxy et FortiSwitchManager permet à un attaquant d'exécuter du code HTTP/HTTPS avec les privilèges les plus élevés. Cette vulnérabilité est actuellement exploitée.

Alertes

Cyberveille

Cyberveille santé



LE PROJET RICHELIEU, UNE LISTE DES MOTS DE PASSE FRANÇAIS LES PLUS COURANTS À DESTINATION DES ÉQUIPES SÉCURITÉ

Le projet Richelieu est un nouveau projet diffusé sur la plateforme GitHub et regroupant une liste des 20 000 mots de passe français les plus utilisés. Le projet sur GitHub est maintenu par Maxime Alay-Eddine et Paul Barbaste, deux développeurs d'outils en cybersécurité. Richelieu est distribué sous licence CC BY 4.0, ce qui signifie que le contenu de sa base peut être réutilisé, sous réserve d'en mentionner l'origine et d'en redistribuer toute modification ou adaptation sous la même licence.

L'objectif du projet est de fournir aux responsables en sécurité et "pen-testeurs" français un dictionnaire ouvert avec les mots de passe les plus communs, afin qu'ils soient en mesure d'évaluer leurs vulnérabilités avec un jeu de données représentatifs (par exemple en effectuant des attaques par dictionnaire ou par force brute sur leur propre système d'information).

Cette base a été construite à partir de la diffusion massive d'identifiants de connexion survenues ces dernières années. Elles ont donné lieu à un filtrage pour ne conserver que les mots de passe liés aux adresses e-mail dont le nom de domaine est en ".fr". Les développeurs précisent au demeurant que seuls les 20 000 premiers mots de passe les plus courants ont été conservés, cela afin d'éviter la diffusion de véritables combinaisons identifiantes.

Parmi les 20 000 mots de passe diffusés, on note par ailleurs certaines caractéristiques récurrentes :

https://github.com/tarraschk/richelieu/blame/master/french_passwords_top20000.txt

Abandon de l'expiration des mots de passe

De plus en plus d'études démontrent que forcer l'utilisateur à changer son mot de passe à une fréquence régulière n'est pas une mesure réellement efficace. Les stratégies utilisées par les utilisateurs pour s'adapter aux politiques d'expiration de mots de passe sont généralement prévisibles et abaissent le niveau de sécurité effectif. En effet, ***la majorité des participants utilise une version légèrement modifiée de leur mot de passe précédent****, par exemple en ajoutant un chiffre à la fin. Les bénéfices en termes de sécurité sont ainsi mineurs et largement contrebalancés par l'expérience utilisateur négative.*

Augmenter l'entropie du mot de passe

*Ce principe (de l'entropie) nous permet de définir un **niveau minimal générique de 80 bits** pour un mot de passe sans mesure complémentaire, et de laisser à chacun le loisir de définir sa politique de mot de passe.*

Exemples	MDPs
Exemple 1	01258976545495
Exemple 2	V@cances1!
Exemple 3	arbre stylo lapin

Précisions concernant les règles de mots de passe

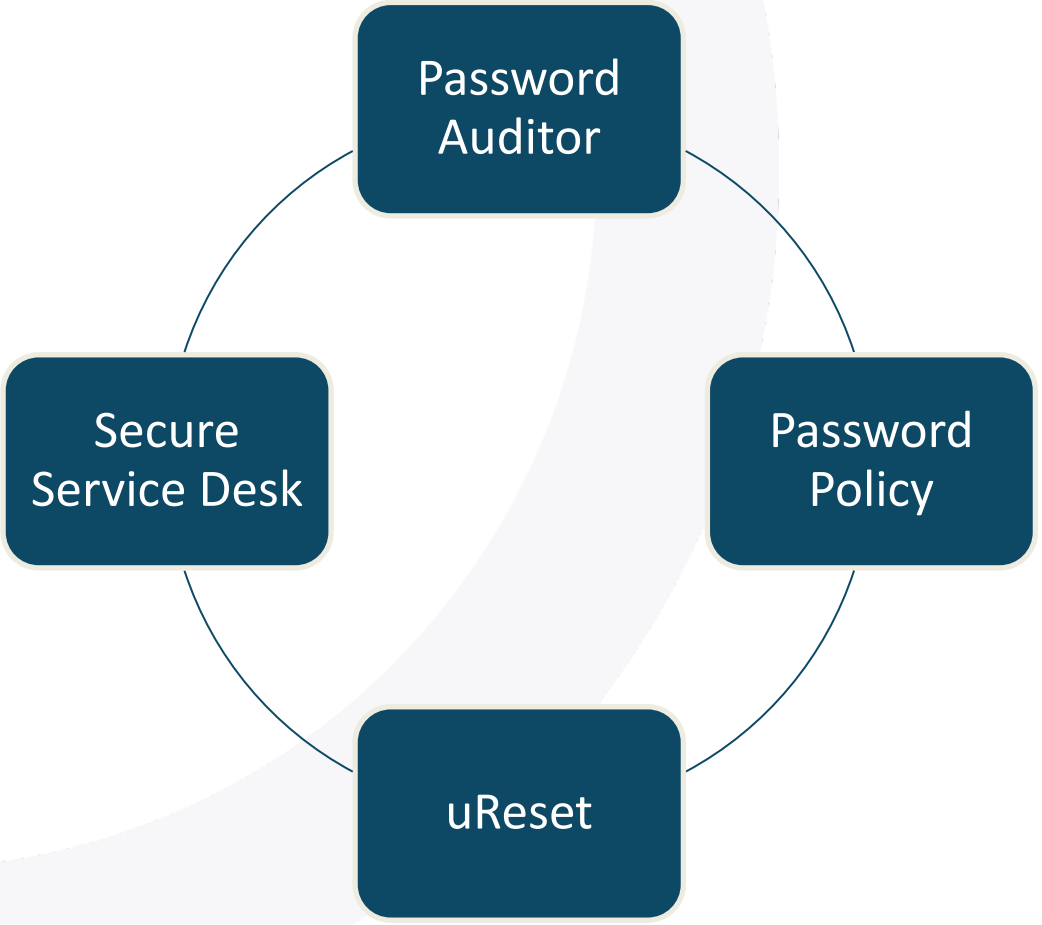
Expérience utilisateur

Savez-vous ce que les GPOs de Microsoft ne prennent pas en compte ?

- Les paramètres visant à éliminer les modèles prévisibles
- Interdire les caractères identiques consécutifs
- Types de caractères communs au début et à la fin
- Utilisation de la substitution de caractères communs (leetspeak)
- Dictionnaire de mots interdits
- Notification par e-mail de l'expiration du mot de passe
- Application de plus que 3 types de caractères
- ...

SPECOPS
AN OUTPOST24 COMPANY

SPECOPS
AN OUTPOST24 COMPANY



Expertise autour de la sécurité autour des mots de passe AD

Un leader européen de la cybersécurité

Outpost24

SPECOPS
AN OUTPOST24 COMPANY

Blueliv.
AN OUTPOST24 COMPANY

Julien Berteraut
Regional Sales Manager
Specops Software France
julien.berteraut@specopssoft.com