aDvens

Security for the greater good

Renseignement sur les menaces
Bulletin du mois de septembre

2024-10-03 | **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 d'intérêts, en complément de celles déjà publiées.

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

- trois modèles psychologiques/cyberpsychologiques pour comprendre la vulnérabilité des utilisateurs face à l'hameçonnage;
- une analyse d'une campagne d'escroqueire (*scam*) ciblant le secteur de la vente au détail.

2. Vulnérabilités

2.1. CVE-2024-40711

Le chercheur en sécurité Florian Hauser de *CODE WHITE Gmbh* a découvert une vulnérabilité critique (CVE-2024-40711) affectant Veeam Backup & Replication. Cette faille a été corrigée par l'éditeur dans son bulletin de septembre 2024.

Une déserialisation non sécurisée dans Veeam Backup & Replication permet à un attaquant, en envoyant une charge utile spécifiquement forgée, d'exécuter du code arbitraire.

Selon *Censys*, 2.833 serveurs Veeam Backup & Replication seraient exposés sur Internet, concentrés en Allemagne et en France. Ces serveurs ne sont pas nécessairement vulnérables.

2.1.1. Type de vulnérabilité

- CWE-502 : Deserialization of Untrusted Data

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

- Veeam Backup & Replication versions 12.x antérieures à 12.1.2.172 (incluse)

2.1.5. Recommandations

- Mettre à jour Veeam Backup & Replication vers la version 12.2 (build 12.2.0.334) ou ultérieure.
- Des informations complémentaires sont disponibles dans le [bulletin] de Veeam.

2.1.6. Preuve de concept

Une preuve de concept est disponible en sources ouvertes.

2.2. CVE-2024-40766

Le 22 août 2024, SonicWall a publié un bulletin de sécurité concernant une vulnérabilité critique affectant les pare-feux Sonicwall. L'éditeur a ajouté dans son bulletin le 6 septembre 2024, que la vulnérabilité impacte également SSLVPN.

Un défaut de contrôle d'accès dans SonicOS et SSLVPN permet à un attaquant de contourner la politique de sécurité et d'avoir accès à des ressources restreintes. Dans certaines conditions spécifiques, l'attaquant peut provoquer un déni de service.

La vulnérabilité est exploitée.
Elle a été ajoutée le 09 septembre 2024 au catalogue des vulnérabilités exploitées du CISA (KEV).

2.2.1. Type de vulnérabilité

- CWE-284: Improper Access Control

2.2.2. Risque

- Contournement de la politique de sécurité
- Atteinte à la confidentialité des données
- Déni de service

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

- SOHO (Gen 5) versions antérieures à 5.9.2.14-12o
- Pare-feux Gen6 versions antérieures à 6.5.4.14-109n, 6.5.4.15.116n : SOHOW, TZ 300, TZ 300W, TZ 400, TZ 400W, TZ 500, TZ 500W, TZ 600, NSA 2650, NSA 3600, NSA 3650, NSA 4600, NSA 4650, NSA 5600, NSA 5650, NSA 6600, NSA 6650, SM 9200, SM 9250, SM 9400, SM 9450, SM 9600, SM 9650, TZ 300P, TZ 600P, SOHO 250, SOHO 250W, TZ 350, TZ 350W
- Pare-feux Gen7 versions antérieures à 7.0.1-5035 : TZ270, TZ270W, TZ370, TZ370W, TZ470, TZ470W, TZ570, TZ570W, TZ570P, TZ670, NSa 2700, NSa 3700,NSa 4700, NSa 5700, NSa 6700, NSsp 10700, NSsp 11700, NSsp 13700

2.2.5. Recommandations

- Mettre à jour les produits SOHO (Gen 5) vers la version 5.9.2.14-12o ou ultérieure.
- Mettre à jour les pare-feux Gen6 vers la version 6.5.4.14-109n, 6.5.4.15.116n, ou ultérieure.
- Mettre à jour les pare-feux Gen7 vers la version 7.0.1-5035 ou ultérieure.
- L'éditeur recommande de mettre à jour les mots de passe des utilisateurs de SSLVPN et d'activer l'authentification à plusieurs facteurs.
- Des informations complémentaires sont disponibles dans le bulletin de SonicWall.

2.2.6. Preuve de concept

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

2.3. CVE-2024-6670

Le chercheur en sécurité Sina Kheirkhah de *Zero Day Initiative* a découvert une vulnérabilité critique (CVE-2024-6670) affectant WhatsUp Gold de Progress. Cette faille a été corrigée par l'éditeur dans son bulletin d'août 2024.

Une vulnérabilité de type injection SQL permet à un attaquant non authentifié d'obtenir le mot de passe chiffré de ce dernier. Selon l'éditeur Progress, cette faille existe lorsque le système ne possède qu'un seul utilisateur.

La vulnérabilité est exploitée.
Elle a été ajoutée le 16 septembre 2024 au catalogue des vulnérabilités exploitées du CISA (KEV).

2.3.1. Type de vulnérabilité

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

2.3.2. Risque

- Contournement de la politique de sécurité

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

- WhatsUp Gold versions antérieures à 2024.0.0

2.3.5. Recommandations

- Mettre à jour WhatsUp Gold vers la version 2024.0.0 ou ultérieure.
- Des informations complémentaires sont disponibles dans le bulletin de Progress.

2.3.6. Preuve de concept

Une preuve de concept est disponible en sources ouvertes.

3. Psychologie / Cyberpsychologie : Trois modèles pour comprendre la vulnérabilité des utilisateurs face à l'hameçonnage

3.1. Avant-propos

Cet article se compose de deux parties distinctes. La première partie examine en détail trois modèles majeurs utilisés par les chercheurs pour comprendre la vulnérabilité des utilisateurs face aux tentatives de phishing. Le premier modèle abordé est la **Théorie des opportunités et des activités routinières** (1979), suivi du modèle de **Traitement Heuristique Systématique de l'information** (1980), et enfin du **Suspicion, Cognition, and Automaticity Model** (2018).

La seconde partie introduit un nouveau concept, la **Surface d'Attaque Psychologique** (SAP), qui s'inspire directement de ces trois cadres théoriques.

Aide vocabulaire

Ci-dessous, quelques définitions pour faciliter la lecture.

- **Cognitif**
  Qui concerne l'acquisition des connaissances (LeRobert, 2024).

- **Heursitique**
  Utilisation de raccourcis mentaux pour formuler de manière rapide des jugements ou des prises de décisions (Cuofano, 2024).

- **Systématique**
  Évaluation analytique, rationnelle et approfondie du contenu informationnel (Cuofano, 2024).

- **Cyberpsychologie**
  Étude des phénomènes mentaux appliquée au cyberespace, soit le monde virtuel, artificiel et recréé. La réalité virtuelle et la télépsychothérapie sont deux exemples concrets de la cyberpsychologie (Bouchard, 2016).

- **Cyberespace**
  Espace de communication créé par l'interconnexion mondiale des ordinateurs (Internet) et par les données qui y sont traitées ; espace, milieu dans lequel naviguent les internautes (LeRobert, 2024).

- **Postmodernité**
  Désigne les bouleversements structurels des modes de vie et d'organisation sociale propres au XXe siècle (Yousfi, 2013).

- **Stimulus**
  Cause externe ou interne capable de provoquer la réaction d'un système excitable, d'un organisme vivant (LeRobert, 2024).

3.2. Section 1 : Les modèles

Cette première section est consacrée aux modèles.

3.2.1. Modèle 1 : Théorie des opportunités et des activités routinières

- Domaine : Criminologie
- Scientifiques : Marcus Felson et Lawrence E. Cohen
- Nom : Routine Activity Theory
- Sigle : RAT
- Année : 1979

Explication

Développée par Marcus Felson et Lawrence E. Cohen en 1979, la théorie des opportunités et des activités routinières (" *Routine Activity Theory* ") suggère que la probabilité du crime augmente selon la convergence de trois composantes: un criminel motivé, une cible appropriée et une protection peu efficace ou peu présente.

Cette convergence des trois composantes dans l'espace et le temps serait favorisée par la postmodernité, qui caractérise l'état actuel de la civilisation occidentale. Marquée par l'émergence d'une économie florissante après la Seconde Guerre mondiale, cette période a entrainé de profonds bouleversements sociaux, notamment dans les domaines de l'urbanisation et des transports. Toutefois, cette ère de développement s'est également accompagnée d'une augmentation significative de la criminalité. Selon Felson et Cohen, cette hausse résulte des nouvelles opportunités offertes par la prospérité économique. Par exemple :

- La féminisation du travail a créé une double opportunité pour les criminels : cibler à la fois les femmes et les domiciles souvent laissés vides et non protégés.
- L'essor de l'automobile a également engendré de nouvelles occasions criminelles, non seulement en facilitant le vol des véhicules, mais en offrant aux délinquants une mobilité rapide et libre.

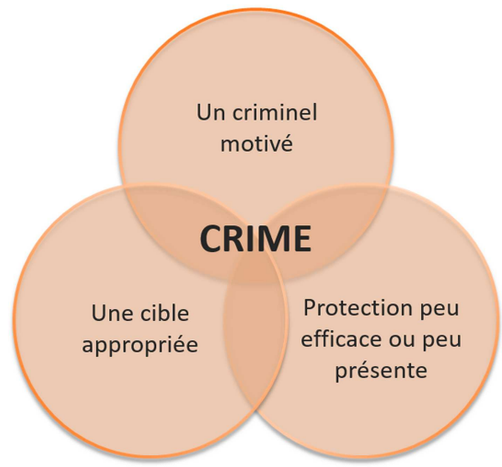


Figure 1. La théorie des opportunités et des activités routinières.

En résumé, Felson et Cohen ont proposé l'idée que le niveau de criminalité est étroitement lié à l'organisation structurelle de la société.

Éléments clés de la Théorie

- Selon la théorie, la mise en place d'une protection adéquate permet de prévenir les actes criminels et de sécuriser les cibles potentielles.
- L'interaction entre la motivation, les opportunités et la disponibilité de cibles vulnérables accroit la probabilité de commettre un crime.
- Bien que les transformations sociétales puissent améliorer la qualité de vie moderne, elles peuvent également créer des conditions favorables à l'augmentation de la criminalité.

Contexte cyber

Depuis son élaboration, la théorie des opportunités et des activités routinières a été largement appliquée à l'étude de diverses formes de criminalité, notamment le cybercrime. Comme d'autres transformations sociétales, l'essor de l'informatique et du cyberespace a créé de nouvelles opportunités pour les cybercriminels.

Figure 2. Cyberespace : le cinquième champ de bataille (après la terre, la mer, le ciel et l'espace).

Parmi les nombreuses techniques malveillantes, l'hameçonnage est particulièrement prisé par les cybercriminels. Ces derniers s'efforcent de concevoir des courriels ou SMS frauduleux visant à exploiter les vulnérabilités psychologiques des utilisateurs (piraterie psychologique ou ingénierie sociale) afin d'obtenir un consentement manipulé. Une protection insuffisante ou inefficace ne permettrait pas de prévenir ces attaques ni de protéger les cibles vulnérables.

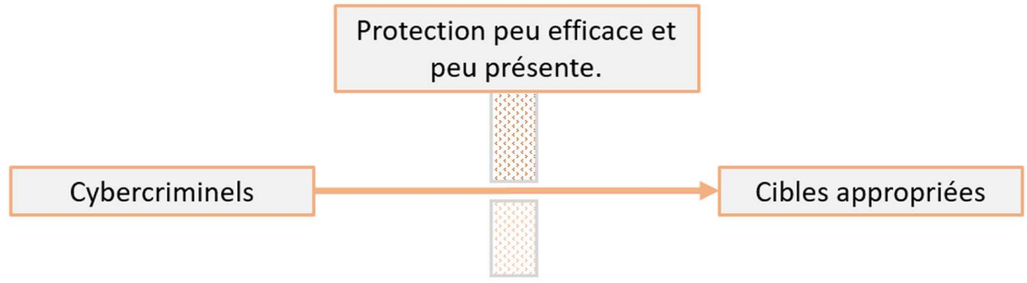


Figure 3. Une protection inefficace ne permettrait pas de contrer le crime.

Selon la théorie, une protection adéquate permettrait de contrer le crime et de protéger les cibles appropriées.

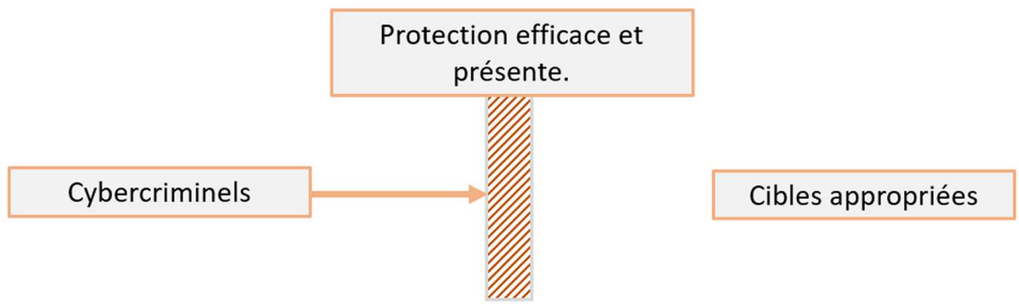


Figure 4. Une protection idoine permettrait de contrer le crime.

VIVA dans le contexte cyber

La théorie des opportunités et des activités routinières précise que la "cible appropriée" est définie par quatre attributs, regroupés sous l'acronyme **VIVA**. Ce sont ces attributs qui déterminent si une cible est jugée propice par le criminel. Voici les quatre attributs :

ATTRIBUTS	EXPLICATIONS (Miró, 2014)
V - Valeur	Il s'agit de la valeur de la cible selon le criminel.
I - Inertie	Les obstacles physiques de la cible : poids, taille, force, forme…
V - Visibilité	La visibilité du criminel sur la cible.
A - Accessibilité	L'accessibilité du criminel a l'environnement où la cube est située.

D'après les travaux de Liliana Ribeiro, Inês Sousa Guedes et Carla Sofia Cardoso (Which factors predict susceptibility to phishing? An empirical study), le modèle **VIVA** peut être interprété comme suit dans le contexte d'hameçonnage :

ATTRIBUTS	EXPLICATIONS
V - Valeur	Cette composante concerne des motivations telles que le gain financier. Par conséquent, les personnes ayant des revenus plus élevés peuvent courir un plus grand risque de recevoir des courriels d'hameçonnage (Graham & Triplett, 2017).
I - Inertie	Celle-ci s'applique aux personnes ou aux objets, ce qui, dans le contexte du cyberespace, pourrait être illustré lorsqu'une pièce jointe est téléchargée avec un virus (Leukfeldt & Yar, 2016).
V - Visibilité	Dans le contexte du cyberespace, la « visibilité » pourrait être facilitée en raison de l'absence de barrières physiques sur Internet, ce qui pourrait à son tour attirer des criminels plus motivés (Yar, 2005).
A - Accessibilité	L'accessibilité aux cibles appropriées en mettant en œuvre diverses mesures de sécurité, telles que l'utilisation de mots de passe forts.

Conclusion

Dans le contexte de la cybersécurité, la théorie des opportunités et des activités routinières souligne l'importance essentielle d'une protection adaptée pour prévenir le cybercrime. En bloquant la convergence des trois éléments clés – un cybercriminel motivé, une cible vulnérable et une protection insuffisante ou absente – il est possible de réduire considérablement la susceptibilité des utilisateurs face aux attaques d'hameçonnage.

3.2.2. Modèle 2 : Traitement Heuristique Systématique de l'information

- Domaines : Psychologie cognitive et Psychologie sociale
- Scientifique : Shelly Chaiken
- Nom : The Heuristic-Systemic model of information processing
- Sigle : THS
- Année : 1980

Explication

Le modèle de Traitement Heuristique Systématique de l'information (" *The Heuristic-Systemic model of information processing* ") a été élaboré en 1980 par la psychologue Shelly Chaiken afin de décrire la manière dont les individus reçoivent et traitent les messages persuasifs.

Selon le modèle, l'être humain traite les messages de deux façons : de manière systématique et heuristique .

- **Systématique** : Ce mode de traitement repose sur une analyse approfondie et détaillée de l'information. L'individu évalue la pertinence des arguments en examinant le contenu et la fiabilité des sources. Ce processus demande des capacités cognitives élevées, ce qui entraine une forte consommation de ressources mentales. Les jugements issus du traitement systématique sont généralement bien adaptés au contenu sémantique du message (Bhattacharjee, 2017; Chen et al., 1999).

- **Heuristique** : Ce traitement s'appuie sur des règles de décision simplifiées pour évaluer rapidement le message. Il repose sur des structures de connaissances que l'individu a déjà apprises et mémorisées. Les trois facteurs clés du traitement heuristique sont la disponibilité (connaissances mémorisées), l'accessibilité (connaissances activées) et l'applicabilité (pertinence des connaissances par rapport aux objectifs de l'individu). Ce mode permet d'économiser des ressources cognitives, car il demande moins d'effort mental. Les publicités exploitent souvent ce type de traitement chez les individus (Bhattacharjee, 2017; Tanner, 2005).

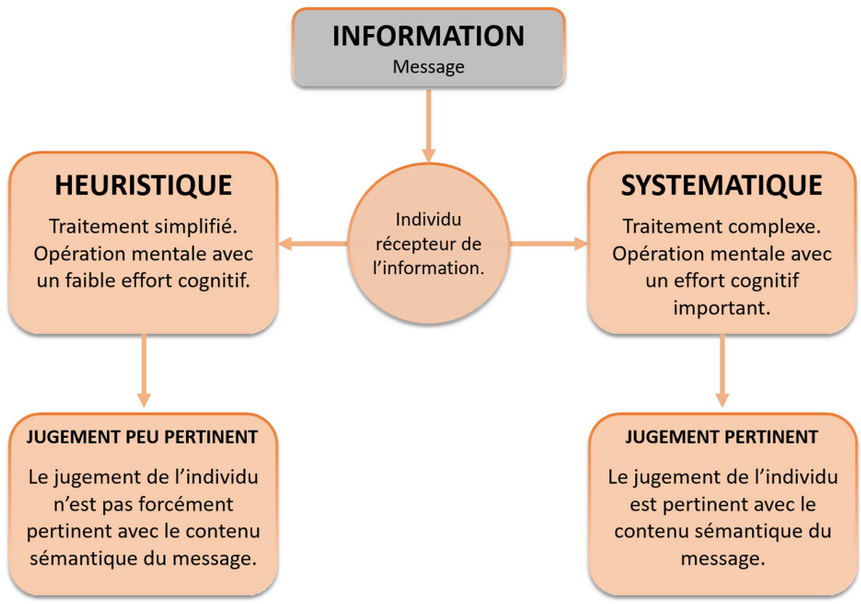


Figure 5. Deux processus de traitements de l'information.

Éléments clés de la Théorie

- Les recherches scientifiques montrent que bien que les individus soient capables de recourir aux deux types de traitement, le traitement heuristique tend à prédominer sur le traitement systématique (Vishwanath et al., 2011).
- Le traitement systématique exige un effort cognitif plus important que le traitement heuristique (Suri & Monroe, 2003).
- Les individus peuvent soit effectuer l'un des deux processus de manière indépendante, soit les combiner et les utiliser simultanément (Bhattacharjee, 2017).
- Contrairement aux attitudes issues par un traitement systématique, celles développées ou modifiées par le biais du processus heuristique tendent à être moins stable, moins résistantes aux contrarguments et moins prédictives des comportements futurs des individus(Bhattacharjee, 2017).

Contexte cyber

L'explication proposée par le modèle de Traitement Heuristique Systématique de l'information ne se limite pas au monde physique. En effet, ce modèle s'applique également au cyberespace où des milliards d'individus interagissent. Il permet ainsi de mieux comprendre les individus reçoivent et traitent les messages persuasifs dans le cyberespace.

Les travaux supplémentaires réalisés par Shelly Chaiken, publiés en 1987 dans *Social Influence The Ontario Symposium, Volume 5* soulignent l'importance de divers facteurs susceptibles d'influencer l'individu à privilégier le traitement heuristique. Parmi ces facteurs figurent l'autorité (directeur, CEO, manager…), la pression temporelle et/ou sociale, ainsi que les capacités personnelles.

Ces travaux font écho avec les nombreuses recherches portant sur l'exploitation des biais cognitifs lors de l'ingénierie sociale. Selon le type de fraude, les attaquants peuvent concevoir des courriels d'hameçonnage visant à exploiter certains biais cognitifs. Cette vulnérabilité psychologique est particulièrement émergente lors du traitement heuristique.

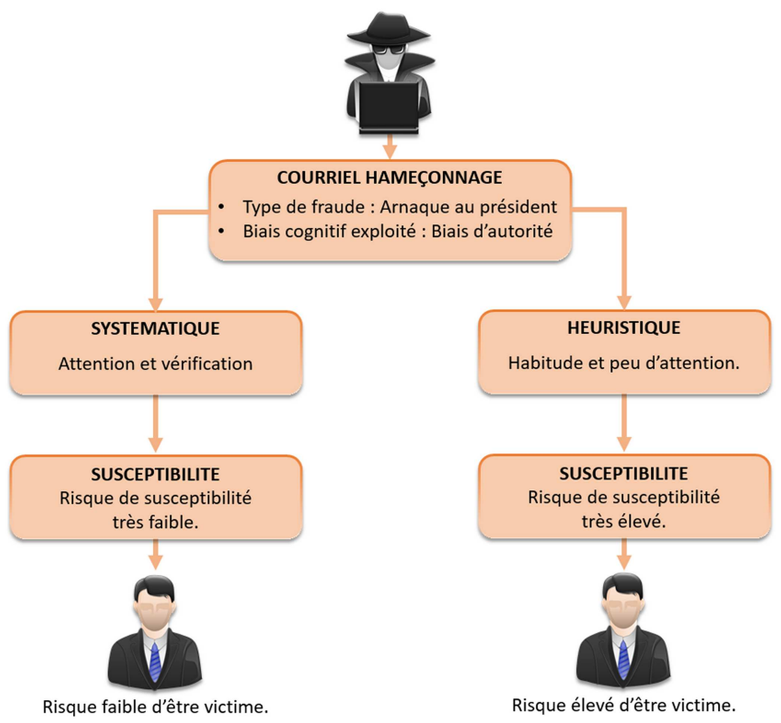


Figure 6. Comprendre la susceptibilité des utilisateurs à l'hameçonnage avec le modèle THS.

Conclusion

Sur la base du modèle de Traitement Heuristique Systématique, la susceptibilité des utilisateurs à l'hameçonnage peut être atténuée en favorisant un traitement systématique de l'information. En adoptant un comportement rationnel et analytique, les utilisateurs sont mieux armés pour contrer l'apparition de vulnérabilité psychologique tels que les habitudes et les biais cognitifs. Ce traitement approfondi permet de réduire l'influence des facteurs qui exploitent les décisions rapides et intuitives, souvent ciblées par les techniques d'ingénierie sociale.

3.2.3. Modèle 3 : Suspicion, cognition, and automaticity model

- Domaine : Communication
- Scientifiques : Arun Vishwanath, Brynne Harrison et Yu Jie Ng
- Nom : Suspicion, cognition, and automaticity model
- Sigle : SCAM
- Année : 2018

Explication

En 2018, Vishwanath et ses collègues présentent leurs travaux sur le modèle SCAM (*Suspicion, cognition, and automaticity model*) qui s'appuie sur les recherches antérieures, notamment le modèle THS (*Traitement Heuristique Systématique*), pour expliquer la susceptibilité des individus à l'hameçonnage (Vishwanath et al., 2018).

L'élément central de ce modèle est la méfiance (*Suspicion*) considérée comme le principal prédicteur interne de la vulnérabilité individuelle à l'hameçonnage. La méfiance est définie définie comme le degré d'incertitude qu'un individu ressent lors d'une interaction avec un stimulus particulier (Lyons et al., 2011).

Ce niveau de méfiance peut être influencé par le type de traitement de l'information que l'utilisateur privilégie. Un traitement fortement heuristique réduit la méfiance face aux courriels d'hameçonnage, car il repose sur des raccourcis mentaux et une évaluation rapide. En revanche, un traitement systématique, qui implique une analyse plus approfondie, entraine une augmentation de la méfiance et, par conséquent, une meilleure protection contre ces tentatives de fraude.

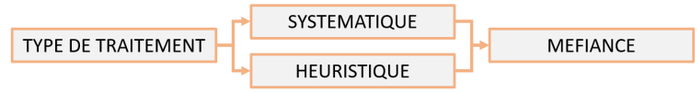


Figure 7. La méfiance est influencée par le type de traitement.

Le modèle SCAM suggère qu'un facteur clé détermine le type de traitement de l'information privilégié par l'utilisateur : les **convictions au cyberrisque** (*Cyber-risk beliefs*). Ces convictions, ou croyances représentent les cognitions les plus fréquemment mobilisées par les individus lorsqu'ils évaluent des situations en ligne présentant des risques (Griffin et al., 2002).

Les **convictions au cyberrisque** renvoient aux perceptions que les utilisateurs se forment des dangers liés à leurs comportements en ligne. Ces croyances jouent un double rôle : elles influencent non seulement le type de traitement de l'information choisi (heuristique ou systématique), mais elles impactent également directement le niveau de méfiance ressenti face à des stimuli potentiellement frauduleux, comme les courriels d'hameçonnage (Vishwanath et al., 2018). Une perception élevée du cyberrisque peut ainsi encourager un traitement plus systématique et une méfiance accrue.

Figure 8. Les convictions aux cyberrisques influence le type de traitement et la méfiance.

Par ailleurs, le modèle suggère aussi que l'incapacité à l'individu à autoréguler son comportement influence ses habitudes. Ainsi, un utilisateur qui maintient ses habitudes est amené à ne pas élever sa méfiance vis-à-vis des courriels d'hameçonnage.

Figure 9. L'habitude influence la méfiance.

Éléments clés de la Théorie

- La méfiance est identifiée comme le principal facteur interne influençant la vulnérabilité d'un utilisateur face à l'hameçonnage.
- Un recours accru au traitement heuristique réduit la méfiance à l'égard des courriels frauduleux.
- Selon le modèle, une forte perception des cyberrisques incite l'utilisateur à adopter un traitement de l'information plus systématique.
- En privilégiant un traitement systématique, l'utilisateur diminue sa susceptibilité aux tentatives d'hameçonnage.
- Les croyances en matière de cyberrisque ("Cyber-risk beliefs") influencent le mode de traitement de l'information.

- L'incapacité à autoréguler son comportement conduit à perpétuer des habitudes qui diminuent la vigilance face à l'hameçonnage.

Contexte cyber

Ci-dessous, une infographie alternative du modèle SCAM :

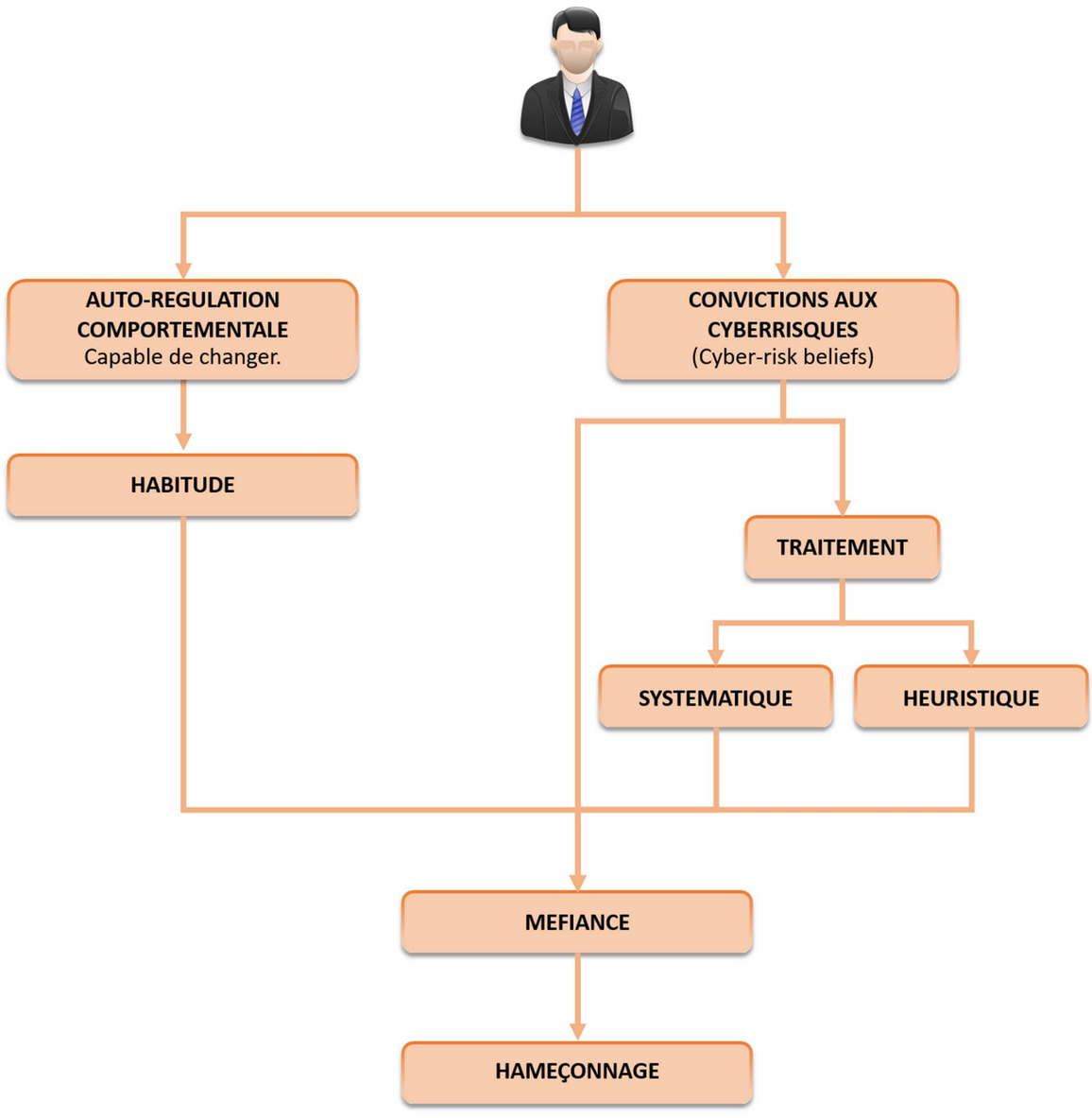


Figure 10. Infographie alternative.

Conclusion

Le développant des connaissances et des convictions relatives aux cyberrisques permettent d'influencer le type de traitement de l'information opéré par l'individu. Ainsi, de fortes convictions contribuent au traitement systématique qui résulte en une méfiance augmentée vis-à-vis de l'hameçonnage.

De plus, en étant capable d'autoréguler son comportement afin d'éviter les habitudes, il devient possible de réduire le risque de susceptibilité à l'hameçonnage.

3.2.4. Synthèse

Ci-dessous, un récapitulatif non exhaustif des solutions proposées par les trois modèles explicatifs.

MODÈLES EXPLICATIFS	SOLUTION
1 - RAT	Éviter la convergence des trois composantes dans l'espace et le temps (criminel potentiel, cible appropriée, protection peu efficace et peu présente) en favorisant une protection efficace et présente.
2 - THS	Favoriser un processus traitement systématique de l'information.
3 - SCAM	Développer des convictions vis-à-vis des cyberrisques (Cyber-risk beliefs) afin de favoriser un traitement systématique qui augmente la méfiance à l'hameçonnage. Une méfiance augmentée diminue le risque de susceptibilité. De plus, la capacité d'autorégulation pour éviter les habitudes permet aussi de contribuer à réduire le risque de susceptibilité.

3.3. Section 2 : Imagination et concept

3.3.1. Description

Dans le contexte informatique, le concept de "surface d'attaque" ou "surface d'exposition" fait référence à l'ensemble des points vulnérables par lesquels un attaquant pourrait potentiellement s'introduire dans un système ou un réseau. En s'inspirant de cette notion, une seconde surface peut être envisagée et adapter au domaine psychologique : **la Surface d'Attaque Psychologique** (SAP). Cette dernière est perçue comme complémentaire, en ce qu'elle représente l'ensemble des vulnérabilités mentales et comportementales que les cybercriminels peuvent exploiter pour manipuler ou tromper les individus.

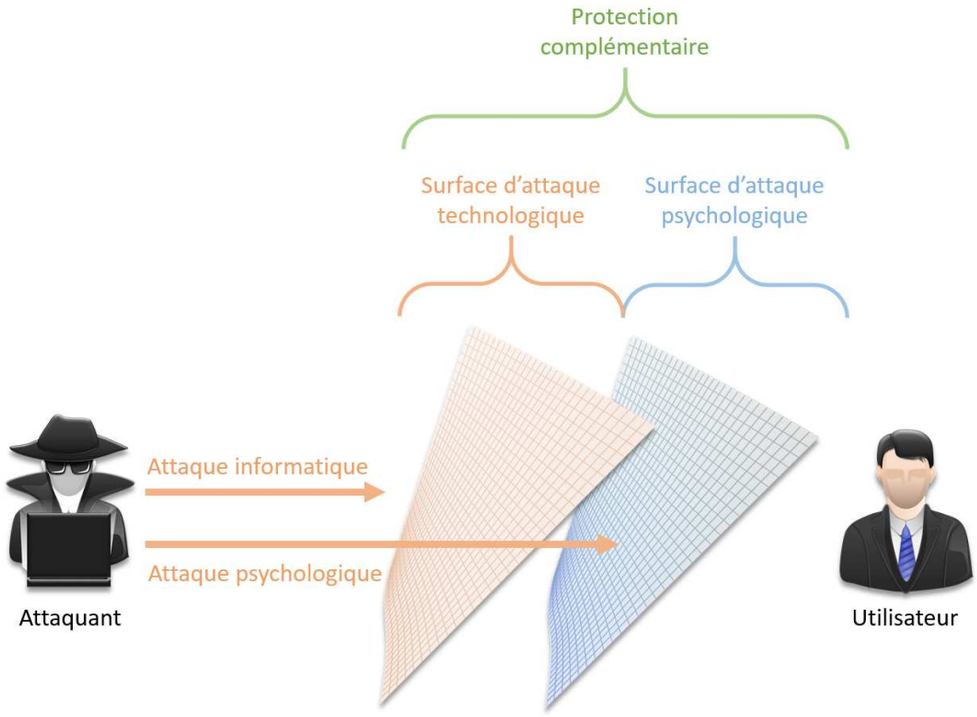


Figure 11. SAP : une protection complémentaire.

3.3.2. objectif

L'objectif est de rendre le SAP plus **robuste** et de **minimiser** sa surface d'attaque.

3.3.3. Comprendre le SAP : ses points de vulnérabilités

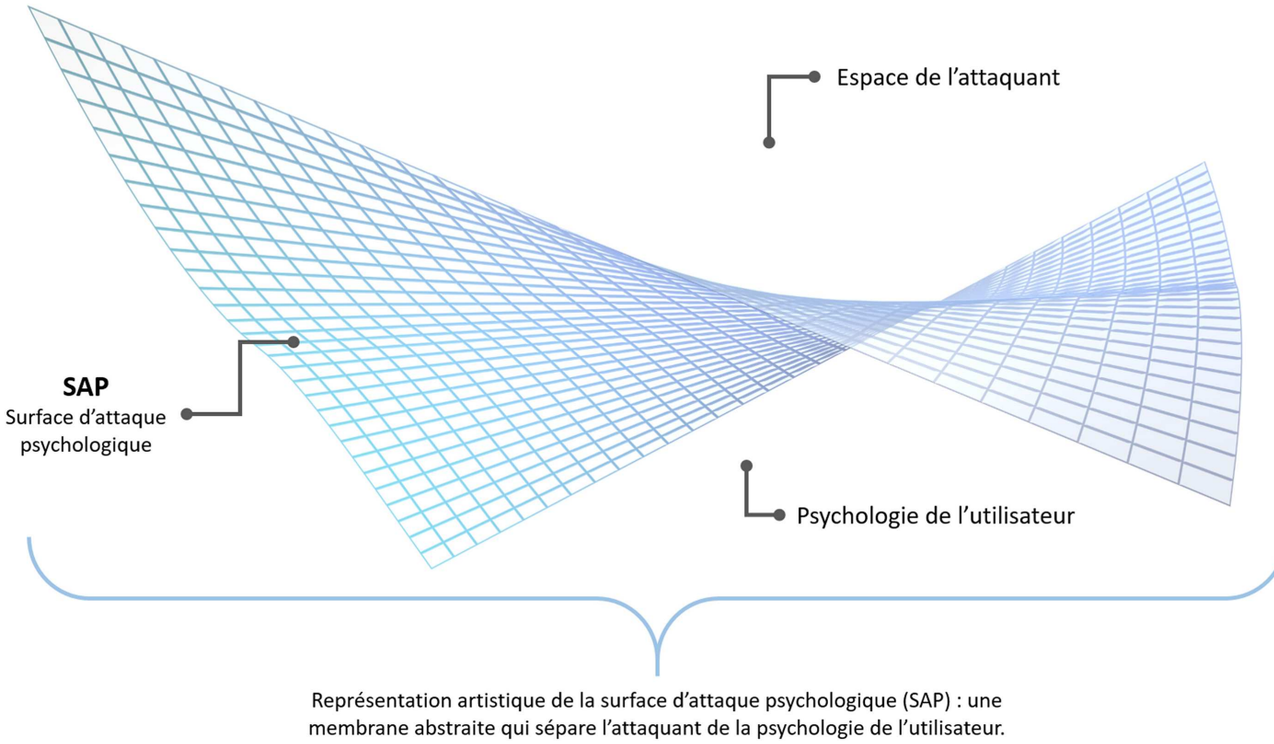


Figure 12. SAP.

La surface d'attaque psychologique rassemble les points vulnérables suivants (non exhaustif) qui peuvent être exploités par l'attaquant lors des phases d'ingénierie sociale :

- **Habitude**
  La manière usuelle d'agir.

- **Biais cognitifs**
  Schéma de pensée faussement logique.

- **Faiblesse à l'autorégulation**
  Difficulté à changer le comportement.

- **Stress**
  Situation de tension nerveuse excessive qui peut empêcher de rationaliser.

- **Inexperience**
  L'utilisateur n'a pas été exposé à de véritables exemples de cyberattaques (inoculation psychologique).

- **État émotionnel**
  De fortes émotions peuvent perturber le raisonnement.

- **Convictions aux cyberrisques**
  Une absence de convictions aux cyberrisques (" *Cyber-risk beliefs* ") peut favoriser un traitement heurisitique.

- **Heuristique**
  Utilisation de raccourcis mentaux pour formuler de manière rapide des jugements ou des prises de décisions.

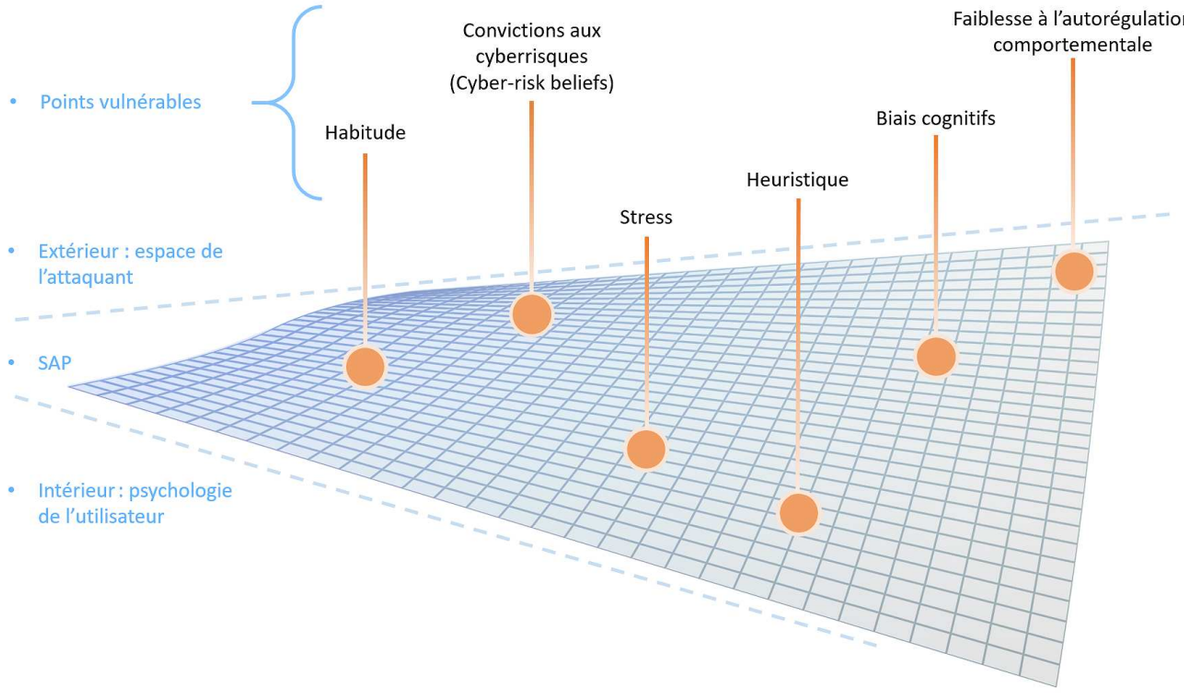


Figure 13. SAP.

3.3.4. Préparation et prévention psychologique

Une réduction optimale de la surface d'attaque psychologique reposerait essentiellement sur la **psychoprophylaxie** de ses utilisateurs.

La psychoprophylaxie est la préparation psychologique visant à prévenir les réactions indésirables pouvant contrarier le bon fonctionnement de l'organisme (Larousse, 2024). Appliquée dans le contexte cyber celle-ci peut être reformulée de la manière suivante : **psychoprophylaxie cyberpsychologique** ou **cyberpsychoprophylaxie.**

Le cadre théorique de la cyberpsychoprophylaxie peut être structuré en 5 échelons de perfectionnement ayant pour objectif ultime l'aguerrissement. Ces 5 échelons, résumés par l'acronyme **SAISA** sont les suivants : la **Sensibilisation / initiation**, l' **Apprentissage**, l' **Inoculation psychologique**, la **Simulation** et enfin l' **Aguerrissement**.

Figure 14. La cyberpsychoprophylaxie.

Cette préparation psychologique nécessiterait un management cohérent du SAP.

3.3.5. Management envisagé du SAP

Le management du SAP pourrait être réalisé en six étapes :

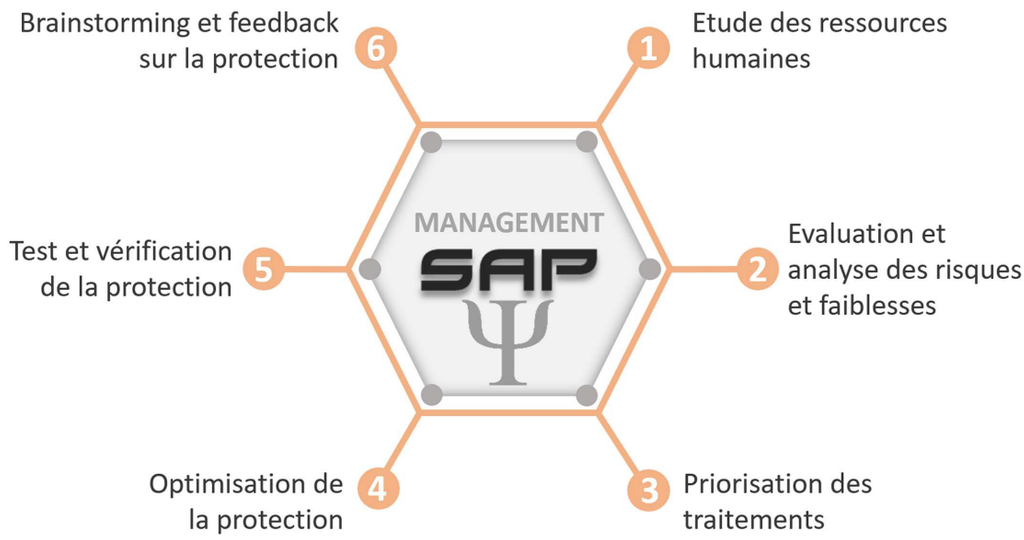


Figure 15. SAP : un management en six grandes étapes.

- **1 - Étude des ressources humaines**
  Il s'agit de faire le bilan sur les utilisateurs concernés par la surface d'attaque psychologique. Par exemple, les utilisateurs qui traitent les courriels et les réseaux sociaux.

- **2 - Évaluation et analyse des risques et faiblesse**
  Cette étape consiste à étudier les vulnérabilités psychologiques des utilisateurs concernés.

- **3 - Priorisation des traitements**
  Selon la charge de travail nécessaire, il peut être important de traiter en priorité les utilisateurs les plus susceptibles à être ciblé par l'ingénierie sociale.

- **4 - Optimisation de la protection**
  L'objectif de cette étape est de réaliser tous les traitements nécessaires (présentations des outils et des procédures de protections…).

- **5 - Test et vérification de la protection**
  Des exercices et des simulations peuvent être appliqués pour tester la résistance des utilisateurs face à l'ingénierie sociale.

- **6 - Brainstorming et feedback**
  Être à l'écoute des utilisateurs sur leurs opinions et ressentis vis-à-vis des traitements (outils, aides…). Le feedback permet d'obtenir une modification ou un renforcement des actions. Le brainstorming permet d'échanger et d'être à l'écoute de nouvelles idées et améliorations.

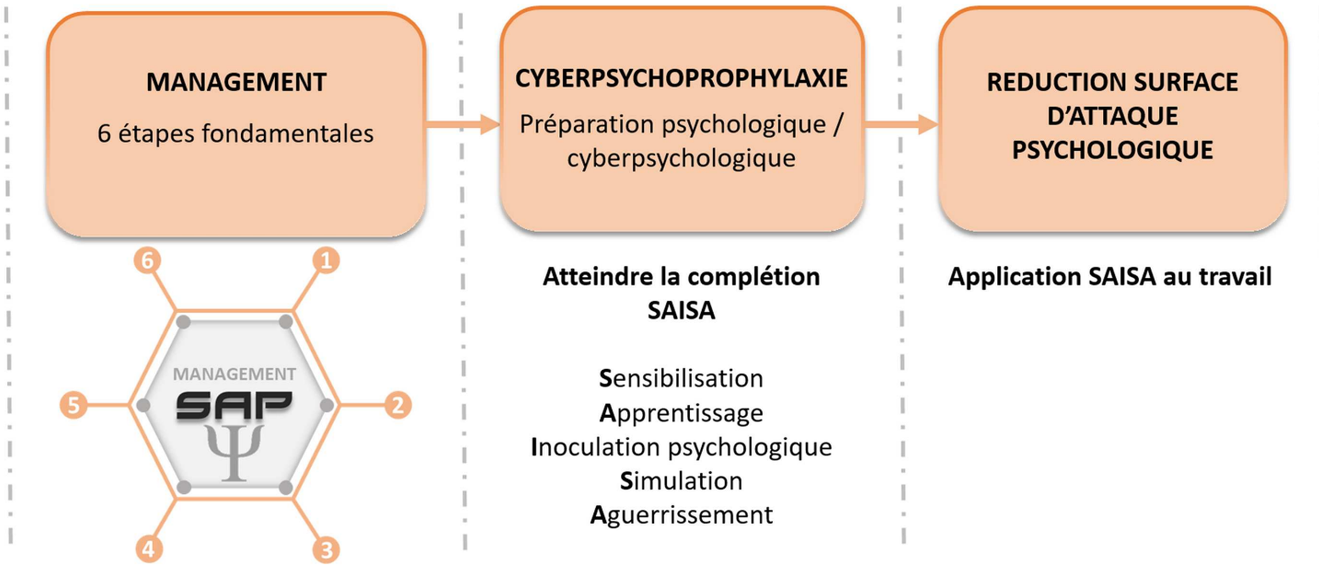


Figure 16. Du management à la réduction de la surface d'attaque.

3.3.6. Conclusion

La Surface d'Attaque Psychologique (SAP) regroupe les différents points vulnérables psychiques par lesquels un attaquant pourrait potentiellement manipuler un individu. Réduire cette surface permettrait de contrer les tentatives d'ingénierie sociale de l'attaquant. Il est estimé que, pour atteindre une réduction optimale de cette surface, une préparation psychologique des utilisateurs, appelée cyberpsychoprophylaxie, est indispensable.

Un plan de gestion en six étapes pourrait permettre d'atteindre ce niveau de préparation :

1. Analyse des ressources humaines,
2. Évaluation des risques et des vulnérabilités psychologiques,
3. Priorisation des mesures correctives,
4. Optimisation des protections psychologiques,
5. Tests et vérifications des dispositifs de protection,
6. Sessions de brainstorming avec retour d'expérience (feedback).

Ce processus vise à renforcer la résilience des individus face aux cyberattaques psychologiques.

4. Copyscam : grande braderie sur le secteur de la vente au détail

Dans le cadre de la surveillance de la surface d'attaque externe d'un client du prêt-à-porter, le CERT aDvens a identifié une campagne de scams ciblant le secteur de la vente au détail à travers le monde. L'acteur de la menace baptisé Window Shopper, en raison de son fort penchant pour cibler les grands noms du secteur de la vente au détail, semble spécialisé dans la création de faux sites de vente en ligne usurpant des sites légitimes. Des produits à prix cassés sont proposés aux victimes qui sont invitées à rentrer leurs identifiants pour se connecter et procéder au paiement. Les paiements sont virés vers des sociétés de blanchiment.

4.1. Victimologie

Les entreprises usurpées sont principalement des **marques occidentales** allant des grandes chaînes commerciales Neiman Marcus ou de discount alimentaire Lidl, aux entreprises de prêt-à-porter tel que Scotch & Soda et de luxe comme Jimmy Choo ou Jacquemus. On trouve aussi des sites spécialisés proposant à la vente des articles de sport (football, natation ou encore cyclisme), des outils de bricolage ou d'équipement. Window Shopper **a ciblé plusieurs sites français** mais les marques américaines (Amazon, Neiman Marcus, Cuyana, Victoria's Secret), hollandaises (G-STAR, Scotch & Soda), portugaises (Salsa Jeans), anglaises (Jimmy Choo, ASOS), australiennes (Ripcurl), danoises (Pandora), espagnols (Massimo Dutti) ou encore allemandes (Lidl) ne sont pas épargnées.

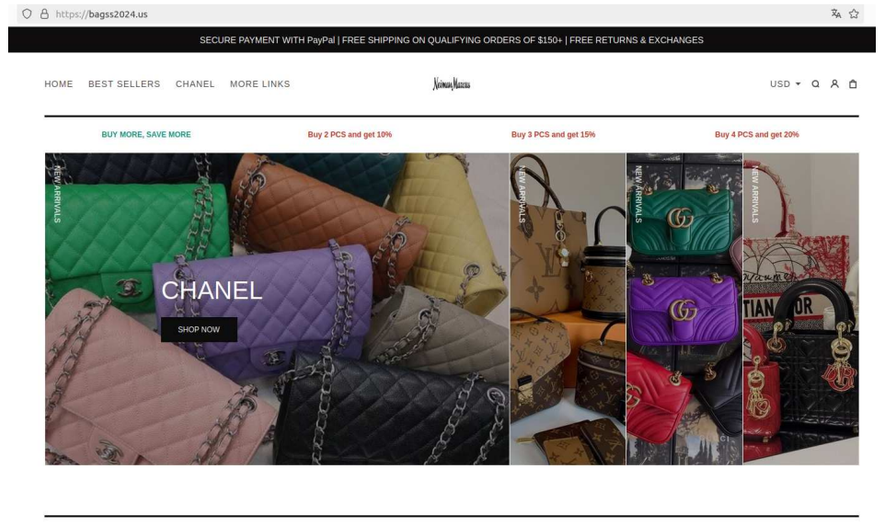


Figure 17. Exemple de site illégitime usurpant la marque Neiman Marcus.

4.2. Localisation

Tous les noms de domaine ont été enregistrés avec la même adresse IP 104.18.73[.]116. La géolocalisation de cette adresse IP est située à San Francisco en Californie. Cette information doit néanmoins être prise à la légère car elle provient du réseau de diffusion de contenu (RDC) Cloudflare. Vue l'abondance des noms de domaines français usurpés (Cabaïa, Cyrillus, Decathlon, Jacadi, Lacoste, Le Coq Sportif, Zadigue & Voltaire) proportionnellement aux autres marques observées, il semblerait que Window Shopper ait une bonne connaissance du marché de la vente au détail français. Par ailleurs, la création à plusieurs reprises de noms de domaine comportant le nom du président français peut laisser penser, avec un degré de confiance modéré, que cet acteur de la menace est français. En effet, il s'agit d'une des rares références qui sort du cadre du secteur de la vente au détail et la seule qui a une connotation politique de toute cette vague de scams.

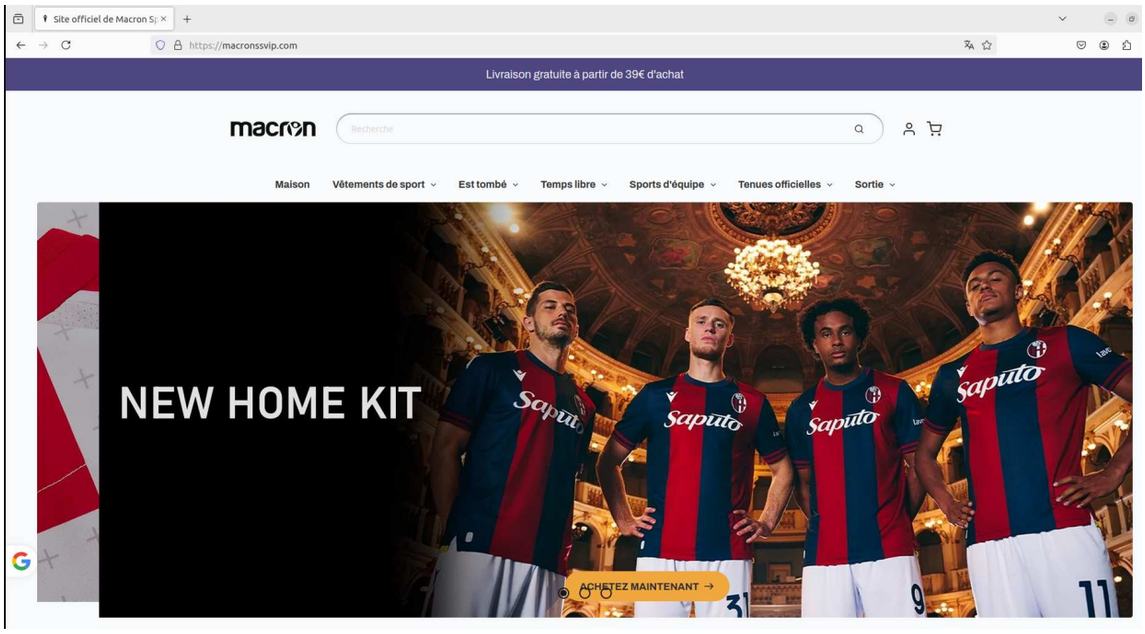


Figure 18. Capture d'écran de la page d'accueil du site illégitime macronssvip[.]com.

4.3. Mode opératoire

4.3.1. Adresse IP

L'acteur de la menace Window Shopper se sert toujours de la même adresse IP 104.18.73[.]116 (hébergée chez Cloudflare) pour enregistrer ses noms de domaine. Ce mode opératoire a permis au CERT aDvens, par recherche IP inversée, d'identifier des centaines d'autres noms de domaine se faisant passer pour des entreprises du secteur de la vente au détail. Pour cette analyse, un échantillon de 718 noms de domaine ont été sélectionnés dont 342 sont encore actifs en date du 20 septembre 2024.

4.3.2. Utilisation de la technique du typosquatting pour enregistrer des noms de domaine

Window Shopper a recours au typosquatting pour enregistrer ses noms de domaine. Le typosquatting (MITRE ATT&CK : Acquire Infrastructure : Domains, T1583.001) est une technique d'attaque par ingénierie sociale qui consiste à enregistrer des noms domaines similaires à des noms de domaine légitimes. L'objectif est double : se faire passer pour le nom de domaine légitime et capter une partie du trafic qui lui est adressé. L'étude des noms de domaines achetés ou créés par l'attaquant a permis de repérer un pattern de nommage autour de différentes formes de typosquatting :

- **la faute d'orthographe ou de frappe** au sein d'un mot du nom de domaine
  (ex : échange de voyelle, ajout de caractères dans le nom de domaine : garminstore[.]shop vs garmin[.]com).

- le recours à un **domaine de premier niveau** (de l'anglais Top-Level Domain TLD) différent
  (ex : lecoqsport[.]shop vs lecoqsportif[.]com). Le mode opératoire de l'attaquant montre une tendance marquée pour l'utilisation de TLD en .shop, .com et .top.

- **modification de la ponctuation au sein du domaine**
  ajout d'un tiret au nom de domaine, suppression d'un point au nom de domaine (ex : jimmychoo -eu [.]com vs row. jimmychoo[.]com.

Bien que fréquemment utilisée par les attaquants, la technique de l'homoglyphe -qui consiste à remplacer un caractère qui ressemble à un autre- n'est pas du tout employée par Window Shopper.

Les principales extensions de noms de domaine (TLD) représentées sont les suivants :

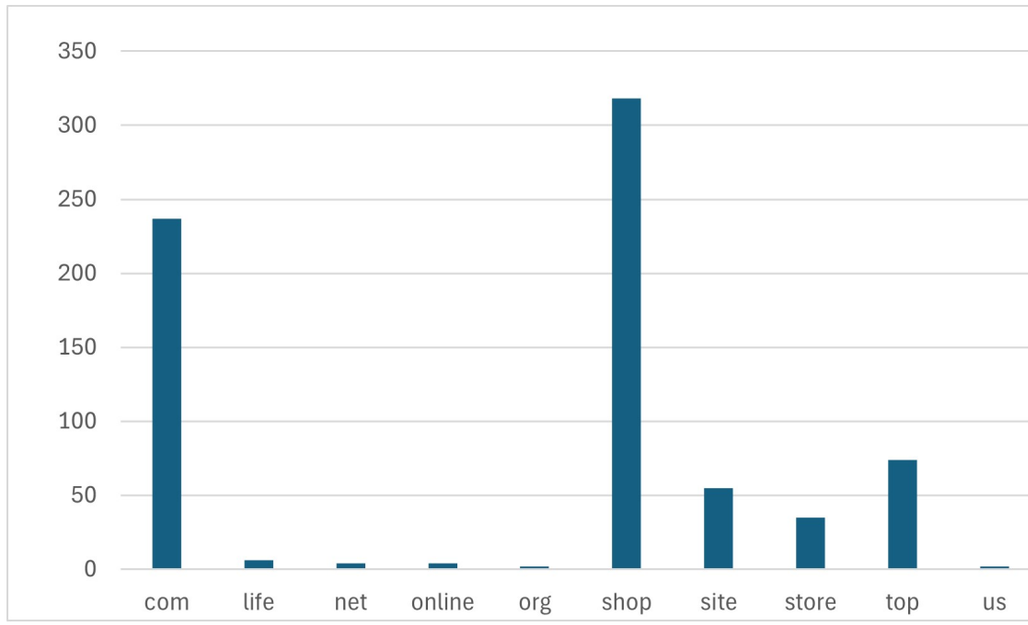


Figure 19. Top 10 des TLD. Source: CERT Advens.

4.3.3. Date de création des noms de domaine

La technique la plus largement utilisée par l'attaquant est l'enregistrement de noms de domaine. Dans certains cas, les dates de création de noms de domaine laissent penser que Window Shopper les a rachetés. Cette technique est toutefois rarement utilisée par l'attaquant et représente moins de 1% des noms de domaine. Presque 90% des noms de domaines analysés ont été enregistrés au cours de l'année 2024. Les autres ont pour la plupart été enregistrés lors du second semestre de 2023.

4.3.4. Habillage des sites de vente au détail

Dans sa campagne de scam, Window Shopper utilise toujours le même mode opératoire qui consiste à habiller les noms de domaine qu'il a acheté ou créé avec l'habillage de sites légitimes. Certains habillages de sites légitimes sont également repris et apposer à des noms de marques factices, inventées par le cybercriminel.

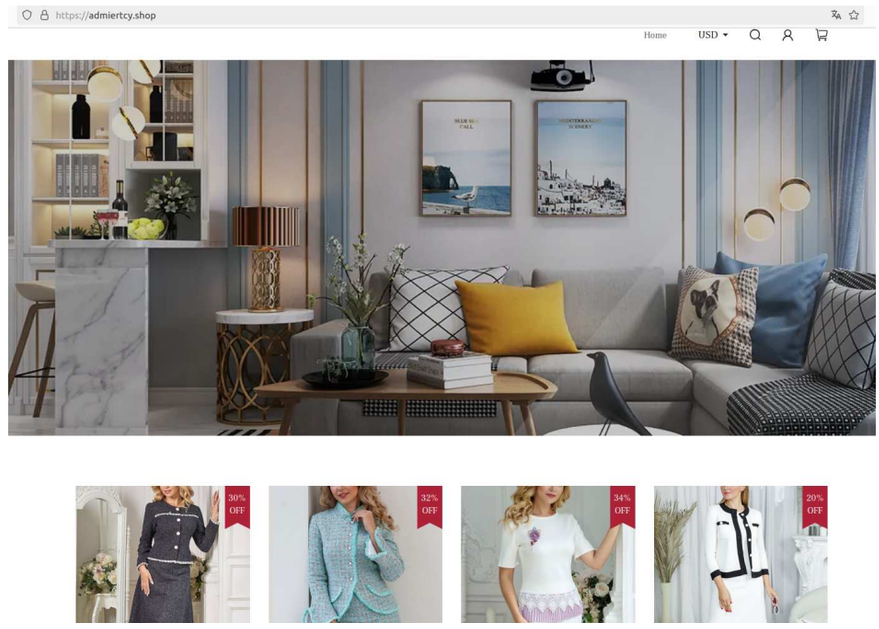


Figure 20. Habillage de site web repris pour plusieurs noms de domaine créé par l'attaquant.

A l'inverse, des noms de marque peuvent être utilisés sur différents sites.

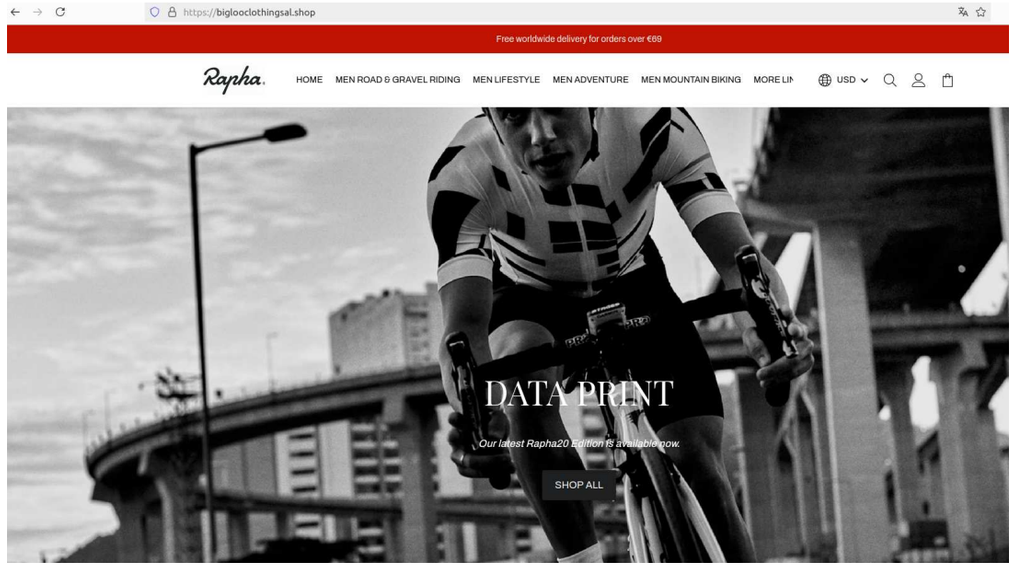
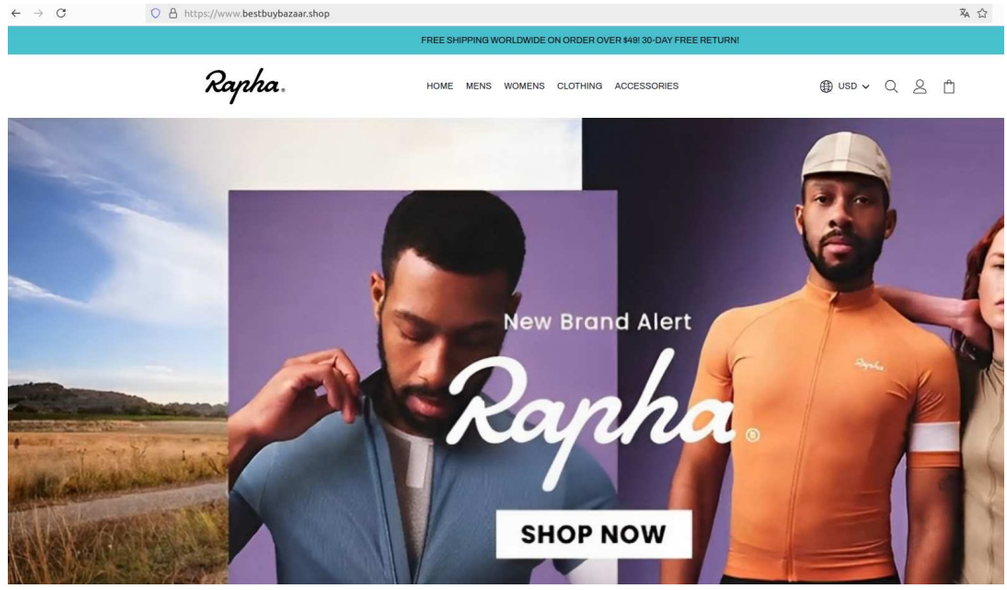


Figure 21. Habillage de site web illégitime différents pour le même nom de marque.



Le CERT aDvens a également pu repérer des clusters de noms de domaine. Plusieurs noms de domaine autour de la même thématique ont été créés sur un temps restreint. Certains peuvent rediriger vers un nom de domaine principal illégitime.

Nom de domaine	Statut	IP	Date de création	Registrar	Commentaire
bagsflash[.]com	Actif	104.18.73.116	18/11/2010	Namebright	Redirection vers bagstores[.]us
bagsgalaxy[.]com	Actif	104.18.73.116	07/07/2024	inwx	Redirection vers bagstores[.]us
bagss[.]us	Actif	104.18.73.116	08/07/2024	Dynadot	Redirection vers bagstores[.]us
bagstores[.]us	Actif	104.18.73.116	07/07/2024	Dynadot	Usurpation de Neiman Marcus

Figure 22. Exemple de cluster avec création de noms de domaine en série et redirection vers un nom de domaine principal. Source: CERT Advens.

4.3.5. Registraire des noms de domaines

Plus de 40 registraires ont servi à enregistrer les noms de domaines de cette campagne de scam. Ceci est élevé, si on tient compte du fait que Window Shopper utilise à l'inverse seulement une adresse IP pour ses créations de noms de domaine. Les principaux registraires utilisés sont Namesilo suivi de Dynadoc Inc, Namecheap et Alibaba Cloud Computing. Ils concentrent à eux seuls plus de la moitié des enregistrements de noms de domaine.

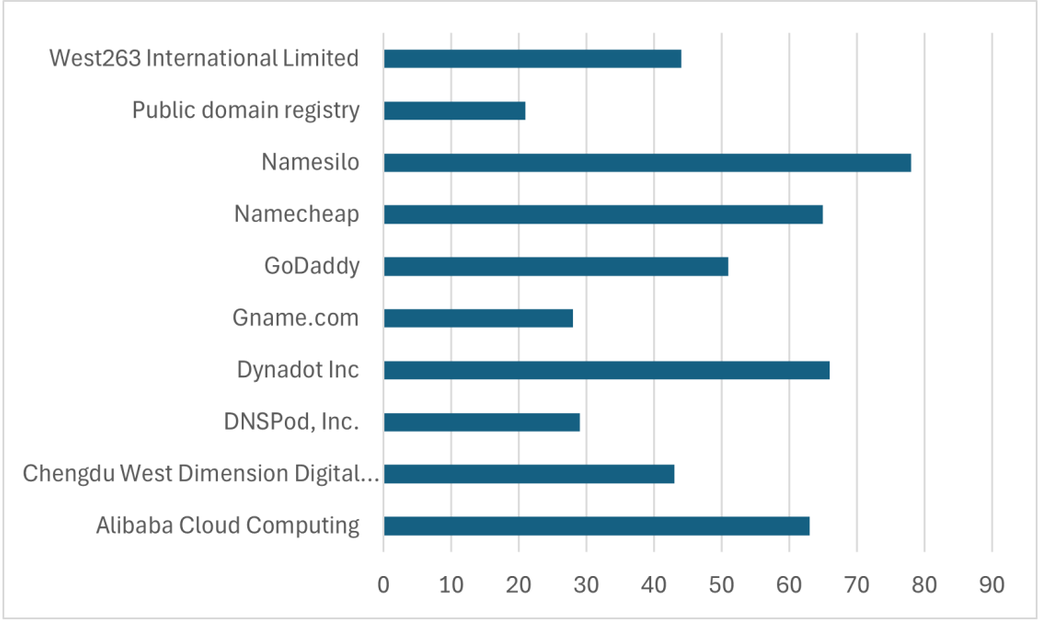


Figure 23. Top des registraires des noms de domaines illégitimes. Source: CERT Advens.

4.3.6. Mode de paiement

La victime est invitée à régler ses achats sur la page de paiement du site. Elle doit rentrer ses données personnelles et ses coordonnées bancaires.

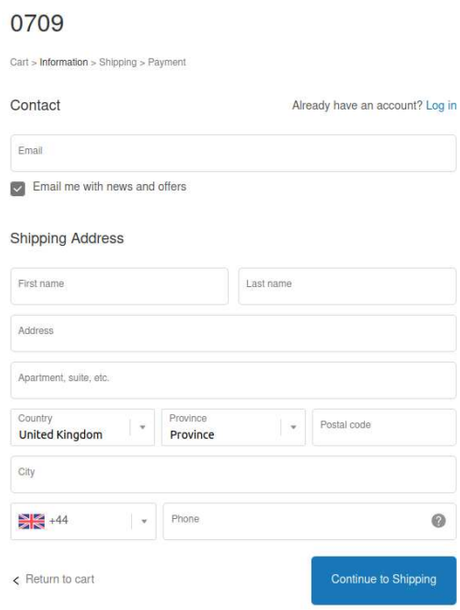


Figure 24. Exemple de page de paiement d'un site illégitime.

Une fois que le portail de paiement s'affiche, le CERT aDvens a pu identifier des portails de paiement PayPal ou Stripe. Ce dernier est un fournisseur de services de paiement permet notamment aux entreprises d'avoir une solution de paiement en ligne sur leur site web. Pour cela, l'entreprise doit créer un compte Stripe qui répond à des obligations Know Your Customer (KYC).

4.3.7. Création de sociétés pour blanchir l'argent

En faisant des recherches en sources ouvertes, le CERT aDvens a constaté que les noms des comptes Stripe affichés sur les sites illégitimes renvoyés à **des sociétés écrans probablement créés par l'attaquant**.

Parmi ces sociétés écran, on compte SARTORI PAINTING Sàrl, spécialisé dans la décoration d'intérieur et basé au Luxembourg, ou encore 29X LLC basé au Colorado aux Etats-Unis. 29X LLC est enregistré au nom de Victoria Shell (pour des questions d'anonymat, le CERT aDvens a utilisé un alias). Cette personne apparaît sur Linkedin comme travaillant en tant qu'assistante executive chez Adaapta, entreprise de conseil en environnement localisée à la même adresse que celle enregistrée pour 29X LLC. Il est probable que l'acteur de la menace ait usurpé ces informations pour enregistrer une entreprise fantôme.

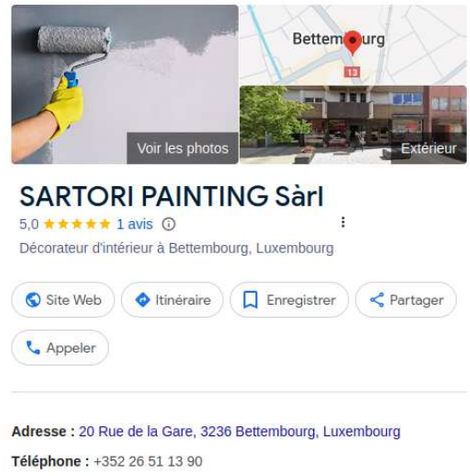
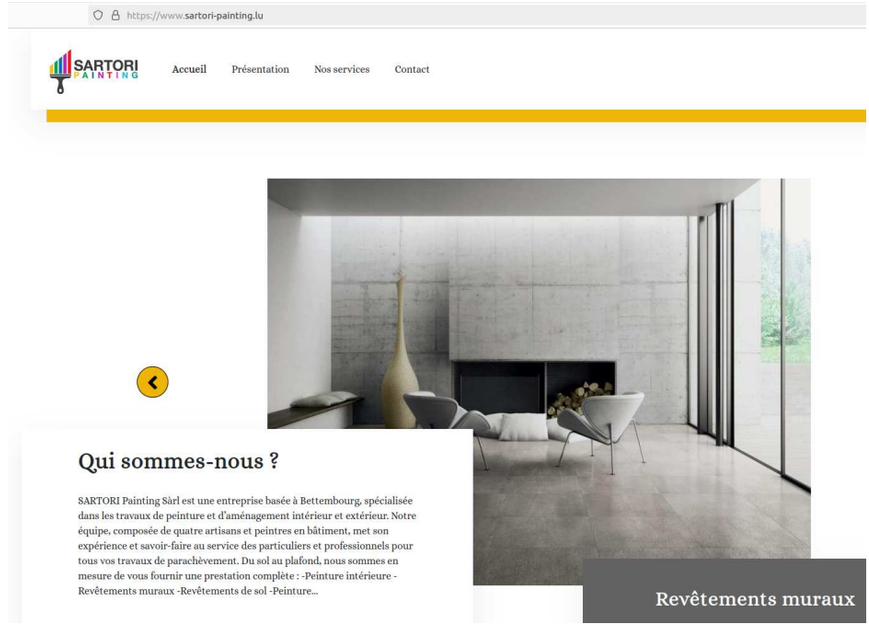


Figure 25. Information de contact de Sartori Painting collectées en source ouverte.



Ces sociétés écran permettent à l'attaquant de blanchir l'argent gagner à partir des faux sites de vente en ligne. Cela veut donc dire qu'elles ont passé la barrière de vérification de Stripe sans se faire repérer. Des actions menées par le CERT aDvens sont en cours auprès de Stripe pour les alerter des activités de ces sociétés.

4.3.8. Une campagne qui va au-delà du scam de site de vente au détail

Fait étonnant, l'adresse IP 104.18.73[.]116 a épisodiquement été utilisée pour du scam sanitaire. Un même narratif sur le diabète est relayé par plusieurs sites de désinformation qui usurpent les logos des chaînes audiovisuelles américaines NMC et MSNBC. Le but de ce scam est de vendre un produit miracle contre cette maladie chronique.

Figure 26. Information de contact de Sartori Painting collectées en source ouverte.

Nom de domaine	Média usurpé
cannier[.]shop	NBC
cinerrty[.]shop	MSNBC
cuineer[.]shop	MSNBC
hotheimall[.]com	-

5. Références

CVE-2024-40711

- https://www.veeam.com/kb4649
- https://censys.com/fr/cve-2024-40711/
- https://nvd.nist.gov/vuln/detail/cve-2024-40711

CVE-2024-40766

- https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0015
- https://www.cert.ssi.gouv.fr/alerte/CERTFR-2024-ALE-011/
- https://nvd.nist.gov/vuln/detail/cve-2024-40766

CVE-2024-6670

- https://community.progress.com/s/article/WhatsUp-Gold-Security-Bulletin-August-2024
- https://nvd.nist.gov/vuln/detail/cve-2024-40766

Article Cyberpsychologie : référence principale utilisée

- Ribeiro, L., Guedes, I. S., Cardoso, C. S. (2024). Which factors predict susceptibility to phishing? An empirical study. *136*. *Computers & Security*. https://www.sciencedirect.com/science/article/pii/S0167404823004686#bib0077

Article Cyberpsychologie - Définition

- Congnitif (LeRobert, 2024). https://dictionnaire.lerobert.com/definition/cognitif
- Cyberespace (LeRobert, 2024). https://dictionnaire.lerobert.com/definition/cyberespace
- Cyberpsychologie (Bouchard, 2016). https://www.cairn.info/revue-rhizome-2016-3-page-17.htm
- Heuristique et Systémique (Cuofano, 2024). https://fourweekmba.com/fr/mod%C3%A8le-syst%C3%A9matique-heuristique/
- Postmodernité (Yousfi, 2013). https://www.scienceshumaines.com/les-penseurs-de-la-postmodernite_fr_30366.html
- Psychoprophylaxie (Larousse, 2024). https://www.larousse.fr/dictionnaires/francais/psychoprophylaxie/64875

Article Cyberpsychologie - Routine Activity Theory

- Graham, R., Triplett, R. (2016) . Capable Guardians in the Digital Environment: The Role of Digital Literacy in Reducing Phishing Victimization. *Research Gate*. *38*(12), 1-12. https://www.researchgate.net/publication/310737084_Capable_Guardians_in_the_Digital_Environment_The_Role_of_Digital_Literacy_in_Reducing_Phishing_Victimization
- Leukfeldt, E. R., Yar, M. (2014) . Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Taylor & Francis Online*. *37*(3), 263-280. https://www.tandfonline.com/doi/full/10.1080/01639625.2015.1012409
- Mathieu, C., Trudel, Yves. (2021). Cycles des crimes financiers et théorie des activités routinières / Chaire Desjardins en finance responsable. Cahier de recherche de l'Université de Sherbrooke. *BAnK numérique*. https://collections.banq.qc.ca/ark:/52327/4663843
- Miró, F. (2014). Routine Activity Theory.*Wiley Online Library*. https://onlinelibrary.wiley.com/doi/full/10.1002/9781118517390.wbetc198
- Miró-Llinares, F. (2014). Routine Activity Theory. *Research Gate*. https://www.researchgate.net/profile/Fernando-Miro-Llinares/publication/328839261_Routine_Activity_Theory/links/5be5baf892851c6b27b295ac/Routine-Activity-Theory.pdf

- Routine activity theory (2024). Dans *Wikipedia*. https://en.wikipedia.org/wiki/Routine_activity_theory
- Saini, N. (2016). Routine activity theory. *Slide Share*. https://fr.slideshare.net/slideshow/routine-activity-theory/61245486#2
- Yar, M. (2005). The Novelty of "Cybercrime": An Assessment in Light of Routine Activity Theory. *Sage Journals Home*. *2*(4). https://journals.sagepub.com/doi/10.1177/147737080556056

Article Cyberpsychologie - Heuristic-Systematic Model of information processing

- Heuristic-systematic model of information processing (2024). Dans *Wikipedia*. https://en.wikipedia.org/wiki/Heuristic-systematic_model_of_information_processing
- Le modèle de Traitement Heuristique Systématique de l'information : motivations multiples et régulation du jugement en cognition sociale. *L'Année psychologique*. 527-563. https://www.persee.fr/doc/psy_0003-5033_2000_num_100_3_28658
- Chen, S., Duckworth, K., & Chaiken, S. (1999). Motivated Heuristic and Systematic Processing. *Psychological Inquiry*. *10*(1), 44-49. https://static1.squarespace.com/static/50f6f441e4b08191027c661d/t/50fffc41e4b047a6c79e9e41/1358953537000/ChenDuckworth%26Chaiken1999PsychInquiry.pdf
- Tanner, L. (2005) L'étude d'un chercheur du Vermont soulève des questions sur les tactiques publicitaires des hôpitaux. *Rutlandherald*. https://www-rutlandherald-com.translate.goog/news/vermont-researchers-study-raises-questions-about-hospitals-ad-tactics/article_77252f1d-f130-59b7-abda-d75a9b931642.html?_x_tr_sl=en&_x_tr_tl=fr&_x_tr_hl=fr&_x_tr_pto=sc
- Suri, R., Monroe, K. B. (2008). The Effects of Time Constraints on Consumers' Judgments of Prices and Products. *Journal of Consumer Research*. *30*(1), 92-104. https://www.researchgate.net/publication/221599956
- Vishwanath, A., Herath, T., Chen, R., Wang, J., RaoWhy, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems*. *51*(3), 576-586. https://www.sciencedirect.com/science/article/abs/pii/S016792361100090X
- Vishwanath, A., Harrison, B., & Ng, Y. J. (2018). Suspicion, Cognition, and Automaticity Model of Phishing Susceptibility. *Communication Research*. *45*(8), 1146-1166. https://www.researchgate.net/publication/278676335_Suspicion_Cognition_Automaticity_Model_SCAM_of_Phishing_Susceptibility
- Zanna, M. P., Olson, J. M., Herman, C. P. (1987). Social Influence : The Ontario Symposium, Volume 5. *Routledge*. *5*. https://www.routledge.com/Social-Influence-The-Ontario-Symposium-Volume-5/Zanna-Olson-Herman/p/book/9780898596786

Article Cyberpsychologie - Suspicion, cognition, and automaticity model

- Griffin, R. J., Neuwirth, K., Giese, J., & Dunwoody, S. (2002). Linking the heuristic-systematic model and depth of processing. *Communication Research*, 29, 705-732. https://epublications.marquette.edu/cgi/viewcontent.cgi?params=/context/comm_fac/article/1230/&path_info=griffin_6460pub.pdf
- Lyons, J. B., Stokes, C. K., Eschleman, K. J., Alarcon, G. M., & Barelka, A. J. (2011). Trustworthiness and IT Suspicion: An evaluation of the nomological network. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 53, 219-229. https://www.researchgate.net/publication/51560765_Trustworthiness_and_IT_Suspicion_An_Evaluation_of_the_Nomological_Network
- Vishwanath, A., Harrison, B., Ng, Y. J.(2018). Suspicion, Cognition, Automaticity Model (SCAM) of Phishing Susceptibility. *Communication Research*. *45*(8). https://www.researchgate.net/publication/278676335_Suspicion_Cognition_Automaticity_Model_SCAM_of_Phishing_Susceptibility#pf4