aDvens

Security for the greater good

Renseignement sur les menaces
Bulletin du mois d’avril

2024-05-02 | **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 cheval de Troie Mispadu utilisé lors de campagnes d'attaques ciblant des pays européens.
- une étude en cyberpsychologie extrapolant les techniques de mimitisme et de camouflage du milieu naturel à la sphère cyber.

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. GLPI - CVE-2024-31705

Une vulnérabilité critique a été découverte dans le plugin GLPI *Shell Commands* développé par Infotel.

Un défaut de contrôle des données fournies par les utilisateurs dans le plugin permet à un attaquant non authentifié, en envoyant des requêtes spécifiquement forgées, d'exécuter du code arbitraire.

2.1.1. Type de vulnérabilité

- CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

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

- GLPI 10.x incluant la dernière version disponible

2.1.5. Recommandations

- Désactiver le plugin Shell Commands dans GLPI ou restreindre son accès. L'éditeur a retiré le plugin de son marché en ligne.

2.1.6. Preuve de concept

Une preuve de concept est disponible en sources ouvertes.

2.2. PHP - CVE-2024-1874

Le 9 avril 2024, le chercheur en sécurité RyotaK de Flatt Security Inc a dévoilé de multiples vulnérabilités dans plusieurs langages de programmation sous Windows. Ces langages comportent un défaut de traitement des arguments lorsque la fonction Windows **CreateProcess()** est appelée en exécutant un fichier batch (.bat,.cmd,etc…).

Cette vulnérabilité de type injection de commande dans le paramètre *$command* de la fonction PHP **proc_open** permet à un attaquant non authentifié, en envoyant des commandes spécifiquement forgées, d'exécuter du code arbitraire.

2.2.1. Type de vulnérabilité

- CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

2.2.2. Risque

- Exécution de code arbitraire

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	Faible

2.2.4. Produits impactés

PHP :

- Versions 8.1.x antérieures à 8.1.28
- Versions 8.2.x antérieures à 8.2.18
- Versions 8.3.x antérieures à 8.3.6

2.2.5. Recommandations

- Mettre à jour PHP vers la version 8.1.28, 8.2.18, 8.3.6 ou ultérieure.

2.2.6. Preuve de concept

Une preuve de concept est disponible en sources ouvertes.

2.3. Cisco IMC - CVE-2024-20295

Un défaut de contrôle des données envoyées par les utilisateurs dans la console Cisco IMC permet à un attaquant authentifié, en envoyant une commande CLI spécifiquement forgée, d'exécuter du code arbitraire et d'obtenir les privilèges root.

2.3.1. Type de vulnérabilité

- CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

2.3.2. Risques

- Exécution de code arbitraire
- Élévation de privilèges

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

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

2.3.4. Produits impactés

Produits exécutant une version de Cisco IMC configurée par défaut :

- Enterprise Network Compute Systems (ENCS) série 5000
- Serveurs série Catalyst 8300 Edge uCPE
- Serveurs rack UCS série C en mode autonome
- Serveurs UCS série E

Appliances Cisco avec une version préconfigurée de Cisco UCS série C et un accès exposé à Cisco IMC CLI :

- Contrôleurs Wi-Fi 5520 et 8540
- Serveurs Application Policy Infrastructure Controller (APIC)
- Appliances Business Edition 6000 et 7000
- Appliances Catalyst Center, anciennement DNA Center (DNAC)
- Appliance Cisco Telemetry Broker
- Cloud Services Platform (CSP) 5000 Series
- Appliances Common Services Platform Collector (CSPC)
- Appliances Connected Mobile Experiences (CMX)
- Serveurs Connected Safety et Security UCS Platform Series
- Appliances Cyber Vision Center
- Appliances Expressway Series
- Serveurs HyperFlex Edge
- Serveurs HyperFlex dans HyperFlex Datacenter sans le mode de déploiement Fabric Interconnect (DC-NO-FI)
- Appliances IEC6400 Edge Compute

- Appliances IOS XRv 9000
- Appliances Meeting Server 1000
- Appliances Nexus Dashboard
- Appliances Prime Infrastructure
- Appliances Prime Network Registrar Jumpstart
- Secure Email Gateways
- Secure Email and Web Manager
- Appliances Secure Endpoint Private Cloud
- Appliances Secure Firewall Management Center, anciennement Firepower Management Center
- Appliances Secure Malware Analytics
- Appliances Secure Network Analytics
- Appliances Secure Network Server
- Appliances Secure Web
- Serveurs Secure Workload

2.3.5. Recommandations

- Les serveurs ENCS série 5000 et série Catalyst 8300 Edge uCPE nécessitent une mise à jour du logiciel Cisco NFVIS. Cette étape met simultanément à niveau Cisco IMC. Mettre à jour Cisco NFVIS vers la version 4.14.1 ou ultérieure.

- Pour les autres produits vulnérables avec la configuration par défaut, mettre à jour la version de Cisco IMC :
  - Serveur rack Cisco UCS série C M4 : Mettre à jour vers la version 4.1(2m) ou ultérieure.
  - Serveur rack Cisco UCS série C M5 : Mettre à jour vers la version 4.1(3m), 4.2(3j), 4.2(3j) ou ultérieure.
  - Serveur rack Cisco UCS série C M6 : Mettre à jour vers la version 4.2(3j), 4.3(2.240002) ou ultérieure.
  - Serveur rack Cisco UCS série C M7 : Mettre à jour vers la version 4.3(2.240002) ou ultérieure.
  - Serveurs Cisco UCS série E M2 et M3 : Mettre à jour vers la version 3.2.15 ou ultérieure.
  - Serveur Cisco UCS série E M6 : Mettre à jour vers la version 4.12.2 ou ultérieure.

- Pour les appliances avec une version préconfigurée de serveur Cisco UCS série C, les administrateurs peuvent réaliser une mise à niveau du logiciel Cisco IMC vers l'une des versions corrigées mentionnées en supra. Les exceptions sont listées en infra :
  - Appliance Cisco Telemetry Broker : Mettre à jour vers la version 4.3(2.240009) ou ultérieure.
  - Appliances IEC6400 Edge Compute : Mettre à jour vers la version 4.2(3j) ou ultérieure.
  - Secure Email Gateways : Mettre à jour vers la version 4.2(3j) ou ultérieure.
  - Secure Email and Web Manager : Mettre à jour vers la version 4.2(3j) ou ultérieure.
  - Appliances Secure Endpoint Private Cloud : Mettre à jour vers la version 4.3(2.240009) ou ultérieure.
  - Appliances Secure Firewall Management Center : Mettre à jour vers la version 4.3(2.240009) ou ultérieure.
  - Appliances Secure Malware Analytics : Mettre à jour vers la version 4.3(2.240009) ou ultérieure.
  - Appliances Secure Network Analytics M4 : Mettre à jour vers la version 4.1(2m) ou ultérieure.
  - Appliances Secure Network Analytics M5 et M6 : Mettre à jour vers la version 4.3(2.240009) ou ultérieure.
  - Appliances Secure Network Server : Mettre à jour vers la version 4.3(2.240009) ou ultérieure.
  - Appliances Secure Web : Mettre à jour vers la version 4.2(3j) ou ultérieure.

- Des informations complémentaires sont disponibles dans le bulletin de Cisco.

2.3.6. Preuve de concept

Une preuve de concept est disponible en sources ouvertes.

3. Mispadu, la globalisation d'un malware sud-américain

Dans un rapport publié le 26 mars 2024, le groupe de cybersécurité *Morphisec Labs* a signalé une extension du périmètre géographique d'activité concernant le cheval de Troie Mispadu. En effet, ce dernier a été détecté dans trois pays européens lors de sa dernière campagne d'attaque en avril 2023 : l'Italie, la Suède et la Pologne.

3.1. Origines

Le Cheval de Troie bancaire Mispadu a été détecté en 2019 par le groupe ESET. Développé en Delphi, Mispadu s'exécute sur les systèmes Windows. Il est généralement distribué au travers des fichiers exécutables malveillants, souvent camouflés en bons de réduction ou logiciels populaires. Une fois activé, Mispadu déploie divers modules pour capturer des informations d'identification et manipuler des transactions bancaires.

3.2. Campagne européenne

Mispadu se concentrait lors de ses campagnes précédentes sur les pays d'Amérique latine, avec un focus sur le Brésil et le Mexique. Lors de la campagne d'avril 2023, bien que le Mexique fut le premier pays ciblé, des attaques contre des entités situées en Italie, en Pologne et en Suède ont été détectées. Les types d'entités ciblées sont des acteurs de la finance et des services ou encore de l'industrie automobile. Cette récente expansion en Europe témoigne d'une évolution dans la stratégie du groupe derrière le malware pour toucher un public plus large. À la suite de cette campagne, le malware a par ailleurs suscité l'intérêt du groupe Hacktiviste pro-russe NoName057 qui lui a consacré une publication fin mars 2024

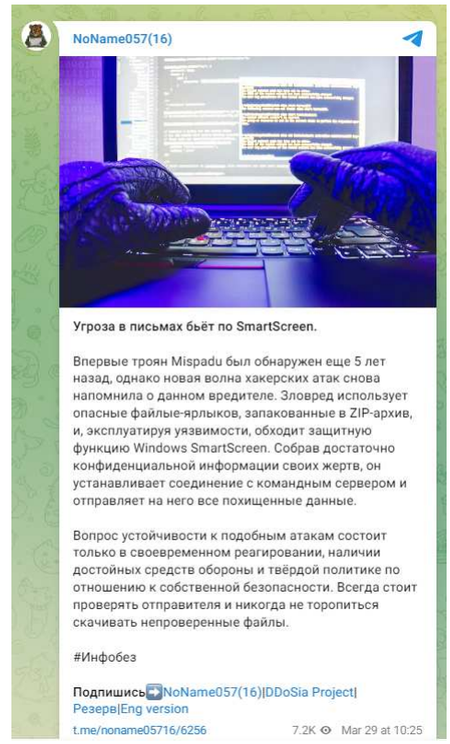

Figure 1. Publication NoName057

3.3. TTPs

Le malware Mispadu fonctionne de la manière suivante : à la suite d'un mail de spear phishing, lorsque les victimes tentent de "consulter la facture complète", elles sont incitées à télécharger un fichier ZIP déclenchant le processus d'infection. Ce fichier contient généralement un script Visual Basic (VBScript) qui, une fois exécuté, télécharge un autre VBScript. Ce dernier charge et exécute le payload de Mispadu en utilisant un script AutoIT après avoir été déchiffré et injecté en mémoire par un chargeur (loader). Cette utilisation des scripts est nouvelle par rapport aux précédentes campagnes de Mispadu. Par ailleurs, ces attaques sont caractérisées par l'utilisation de deux serveurs de commande et de contrôle distincts : l'un pour récupérer les payloads intermédiaires et finaux, et l'autre pour exfiltrer les identifiants volés.

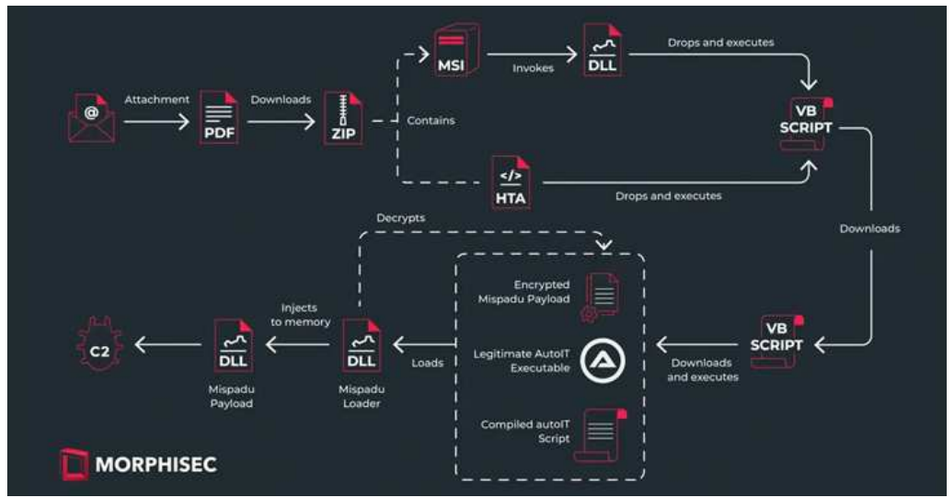

Figure 2. Kill Chain Mispadu – source : Morphisec

- **Accès Initial:** Mispadu utilise principalement le spear phishing via de faux mails de factures pour atteindre ses victimes. Il semble avoir délaissé les publicités malveillantes de ses campagnes précédentes. Mispadu utilise notamment la vulnérabilité CVE-2023-36025 (CVSS 8.8) dans Windows SmartScreen. Cette faille permet aux cybercriminels de créer des fichiers de raccourci Internet ou des hyperliens spécialement conçus pour contourner les avertissements de SmartScreen, exposant ainsi les utilisateurs à des binaires malveillants hébergés sur des partages réseau d'acteurs de menaces.

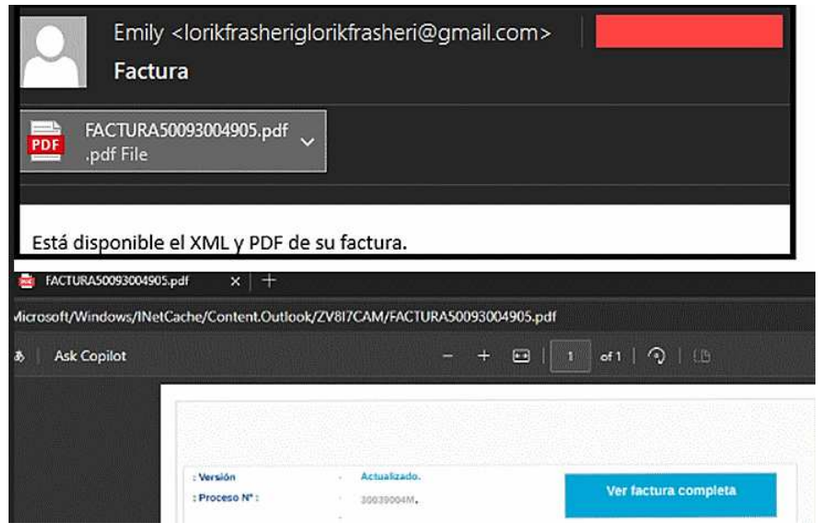

Figure 3. Spear Phishing Mispadu – source : Morphisec

- **Exécution:** Le malware s'exécute via des scripts PowerShell ou des macros malveillantes intégrées dans des documents.
- **Persistance:** Le malware modifie les entrées de registre Windows ou crée des tâches planifiées qui réactivent le malware à chaque redémarrage du système.
- **Élévation de privilèges:** Mispadu tente de gagner des droits d'administration pour exécuter ses processus sans entraves.
- **Injection de code:** Mispadu est capable d'injecter du code malveillant dans des processus légitimes pour éviter la détection.
- **Evasion et Défense :** Mispadu utilise l'injection de DLL (Dynamic Link Library) pour insérer discrètement son code malveillant dans les processus en cours d'exécution. Cette technique lui permet de masquer son activité malicieuse derrière des processus légitimes, réduisant ainsi les chances de détection par les logiciels de sécurité. Par exemple, il peut injecter son code dans des processus tels que *explorer.exe* ou *svchost.exe*, qui sont essentiels pour le fonctionnement de Windows et

souvent exclus des analyses détaillées par les solutions antivirus.

Le malware emploie également des techniques de rootkit pour masquer ses fichiers et clés de registre, rendant sa détection et sa suppression difficiles. Mispadu peut également désactiver les paramètres de sécurité de Windows et les logiciels antivirus via des commandes qui modifient les politiques de groupe ou des entrées de registre qui contrôlent les fonctionnalités de sécurité. Enfin, Mispadu utilise des techniques de polymorphisme pour changer régulièrement son code exécutable, ce qui complique la tâche des signatures antivirus traditionnelles de l'identifier. En outre, il emploie des méthodes pour détecter l'environnement d'exécution et suspendre ses activités s'il détecte qu'il fonctionne dans une machine virtuelle ou un environnement de sandbox.

- **Collecte d'informations:** le malware est équipé de fonctionnalités de keylogging et de surveillance du presse-papiers pour collecter des informations d'identification telles que les noms d'utilisateur et les mots de passe, une tactique utilisée pour intercepter les informations copiées lors des transactions financières ou autres échanges de données sensibles. Il surveille également l'activité de navigation web, capturant les données de formulaires et les cookies. Mispadu peut intercepter les données en transit entre le navigateur et les sites web, permettant ainsi le vol de données de session et d'autres informations sensibles.
- **Commande et contrôle (C2):** Une fois les données collectées, Mispadu communique avec un serveur de commande et de contrôle (C2) pour exfiltrer les informations. Il utilise généralement des protocoles HTTP ou HTTPS, souvent avec des données chiffrées ou encodées pour masquer le trafic malveillant dans le flux réseau habituel. Le malware peut recevoir des commandes du serveur C2 qui lui permettent de télécharger et d'exécuter des fichiers supplémentaires, de mettre à jour ses composants, ou de changer de tactique en fonction des directives reçues.

3.4. Conclusion

Mispadu peut avoir un impact significatif sur les victimes en volant des informations financières et personnelles, en compromettant l'accès aux systèmes et en permettant d'autres intrusions. La réutilisation de ces données financières pour forger de nouveaux scenarii de spear phishing plus élaborés témoigne de l'importance de ces données pour les groupes cybercriminels. Pour atténuer les risques associés à ce malware, les entreprises doivent mettre en œuvre des solutions de sécurité multicouches, tels que des systèmes de détection et de réponse aux endpoints (EDR), et des formations régulières à la sensibilisation à la sécurité pour les employés.

4. Cyberpsychologie : s'inspirer du mimétisme et du camouflage naturel

Cet article propose de **s'inspirer du mimétisme et du camouflage naturel** pour **imaginer des concepts utiles en cybersécurité**. En se basant sur ces concepts, **des tactiques et stratégies psychologiques peuvent être élaborées** pour contribuer à la **cyberdéfense** et le **renseignement** de la menace cyber.

L'article est composé de 4 sections. La première est une description sommaire du mimétisme et du camouflage naturel. La seconde section propose d'explorer le mimétisme, tandis que la troisième est consacrée au camouflage. Enfin, la quatrième section présente les tactiques et stratégies psychologiques qui découlent de ce travail de réflexion.

4.1. Les bases du mimétisme et du camouflage

4.1.1. Un but ultime : survivre

Pour survivre dans le milieu naturel, certains organismes utilisent des **stratégies adaptatives d'imitation** et des **méthodes de dissimulation**.

Ces dernières peuvent être utilisées par une proie pour décevoir psychologiquement son prédateur, par exemple : la proie imite les signaux d'avertissement d'un organisme toxique pour dégouter son prédateur (mimétisme : Batésien). De son côté, le prédateur peut exploiter son camouflage pour se fondre dans l'environnement afin de ne pas être vu par sa proie (camouflage : Coloration disruptive).

Ci-dessous, une infographie qui regroupe de manière simplifiée et non exhaustive quelques stratégies d'imitations et méthodes de camouflage.

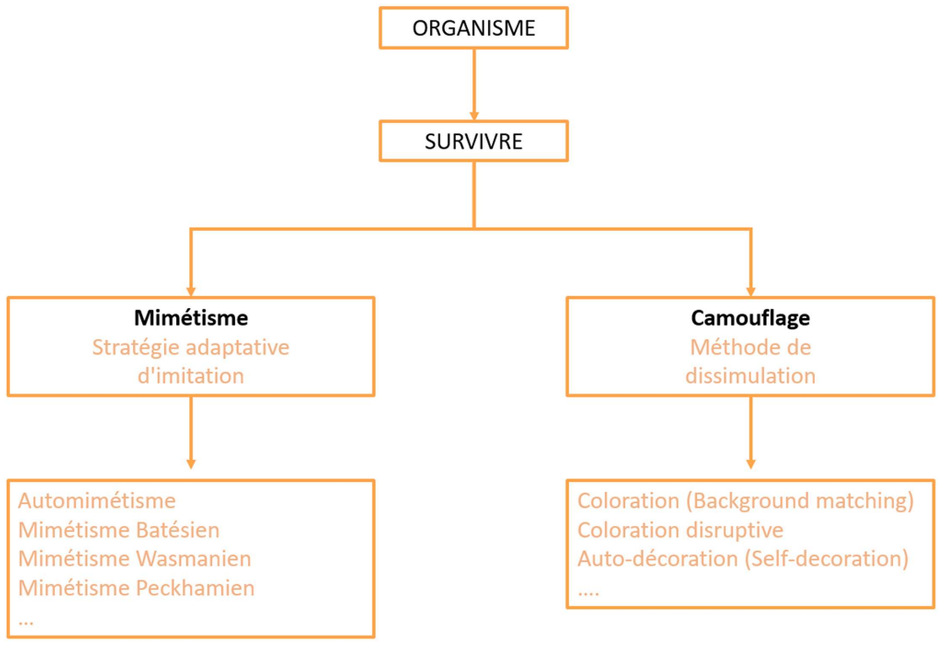

Figure 4. Mimétisme et camouflage.

4.1.2. Comprendre le mimétisme

Le mimétisme est une stratégie adaptative d'imitation qui permet à un organisme de **ressembler partiellement ou complètement à d'autres organismes de son environnement**. L'effort consiste à l'**organisme mime** de copier la morphologie ou le comportement d'un **organisme modèle**. Celui qui est ciblé par le mimétisme est l'**organisme dupé**. Il est possible que le modèle soit aussi celui qui soit dupé par le mime. Le mimétisme peut être exploité de plusieurs manières : olfactif, tactile, acoustique, gustatif, comportemental et visuel. Plusieurs catégories de mimétismes existent : automimétisme, mimétisme Batésien, mimétisme Pekhamien, mimétisme Wasmanien, mimétisme Mullerien…

Dans cet article, deux stratégies sont explorées :

Stratégie de l'automimétisme

- Iphiclides podalirius - Papillon "Le Flambé"
- Chelmon rostratus - Poisson "Copperband butterfly"

Stratégie du mimétisme agressif

- Hymenopus coronatus - La mante orchidée

4.1.3. Comprendre le camouflage

Le camouflage est l'ensemble de méthodes qui permettent à un organisme de **se rendre indiscernable de son milieu**. L'effort consiste à se fondre dans l'environnement pour être, par exemple, méconnaissable des prédateurs, ce qui contribue ainsi à la survie de l'organisme. Les méthodes de camouflages sont nombreuses : coloration (*Background matching*), coloration disruptive, auto-décoration (*self-decoration*)…

Dans cet article, deux méthodes sont explorées :

Camouflage par la coloration (*background matching*)

- Nezara viridula - Punaise verte puante

Camouflage par la coloration disruptive

- Leopardus Paradalis - Léopard Ocelot

4.2. S'inspirer du mimétisme

4.2.1. Automimétisme : description et exemples naturels

Parmi les différentes stratégies adaptatives d'imitation, il existe l'automimétisme : l'organisme imite une portion de son propre corps ou de celui d'un autre organisme. Un des phénomènes le plus célèbres est celui de l'ocelle, une tâche qui imite un oeil. Cette stratégie peut, par exemple, être utilisée pour **psychologiquement leurrer le prédateur** : **faire perdre du temps**, **provoquer de la peur** ou **détourner son attaque** vers une zone moins vitale.

Organisme : Papillon Iphiclides podalirius

Ci-dessous, une photographie d'un papillon "Le Flambé" Iphiclides podalirius. Au bas de ses ailes, vers l'extrémité de l'abdomen, il y a la présence d'un ocelle bleu entouré de noir et d'un arc orange. Cet ocelle permet de détourner l'attaque du prédateur pour l'attirer vers une zone non vitale du papillon.

Figure 5. Papillon Iphiclides podalirius. Photographe : Analyste CTI. Garrigue de la région du Gard. juillet 2021.

Organisme : Poisson Chelmon rostratus

Ci-dessous, une photographie d'un poisson "Chelmon à bec médiocre" Chelmon rostratus. Cet animal possède un ocelle sur la nageoire dorsale lui permettant d'échapper à un prédateur. Les vrais yeux sont dissimulés par une rayure jaune tandis que le "faux oeil" est mis en évidence par un contraste fort.

À l'instar du papillon "Le Flambé", cet ocelle détourne l'attaquant et lui fait perdre du temps lors de l'offensive. Ce temps perdu offre à la proie la possibilité de prendre la fuite.

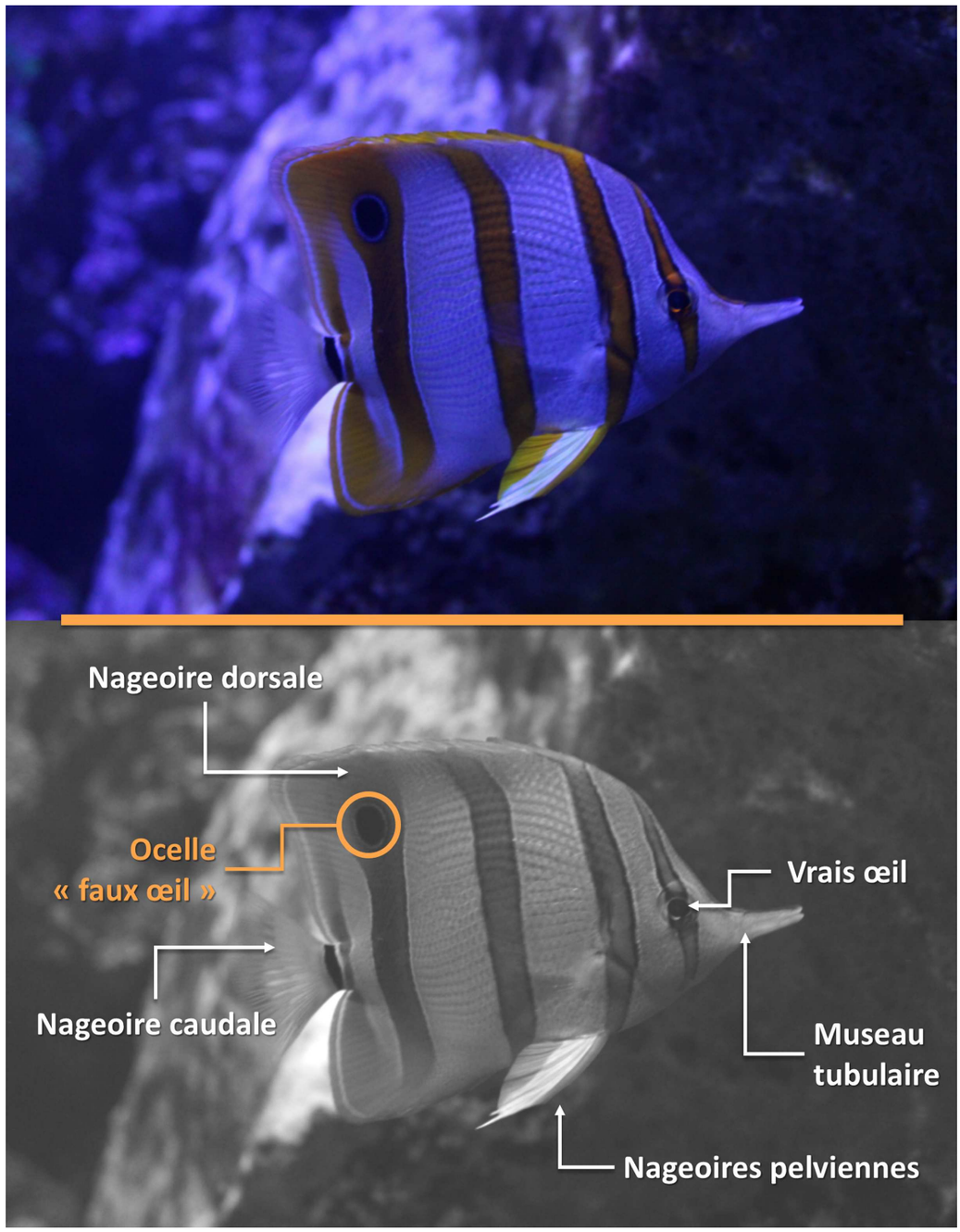

Figure 6. Poisson Chelmon rostratus. Photographe : Analyste CTI. Seaquarium du Grau du Roi. Juillet 2022.

4.2.2. Automimétisme : Application cybersécurité

Ci-dessous, deux exemples de concepts pour le milieu cyber.

Concept : détourner l'attaquant vers une cible non sensible

L'objectif de ce premier concept consiste à **détourner l'attention et l'effort de l'attaquant**. Pour cela, l'utilisateur créer un dossier attractif (ocelle) avec comme intitulé *Confidentiel*. Dans ce dernier, un fichier contient de fausses informations pour leurrer l'attaquant : faux identifiants et mots de passe. Le véritable fichier sensible contenant les informations d'authentification est dissimulé dans un autre dossier dont l'intitulé n'est pas explicite.

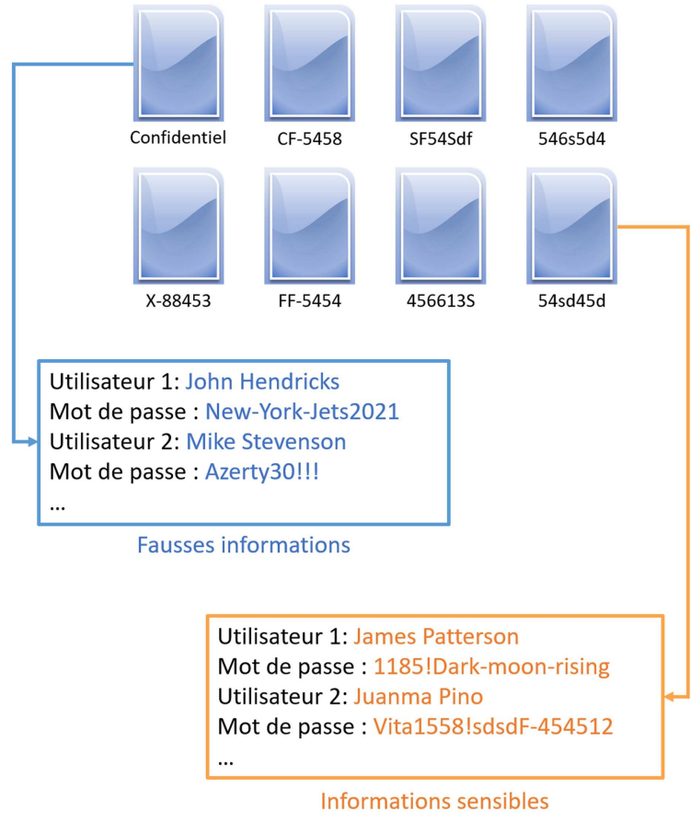

Figure 7. Scénario : détourner l'attaquant.

Concept : détourner et faire perdre du temps à l'attaquant

Si un dossier peut être forgé pour attirer l'attaquant afin de **détourner son attention et ses efforts**, alors il est possible de compliquer le contexte pour lui **faire perdre du temps**. Dans ce concept imaginé, plusieurs dossiers et fichiers attrayants sont créés. Ces derniers sont constitués de fausses informations dont la quantité est importante. Tel un bruit de fond perturbant, cette complication rend l'environnement pour l'attaquant difficile à explorer et à concevoir. Le temps perdu par l'adversaire offre à la sécurité un avantage temporel pour détecter, identifier et réagir face à la menace.

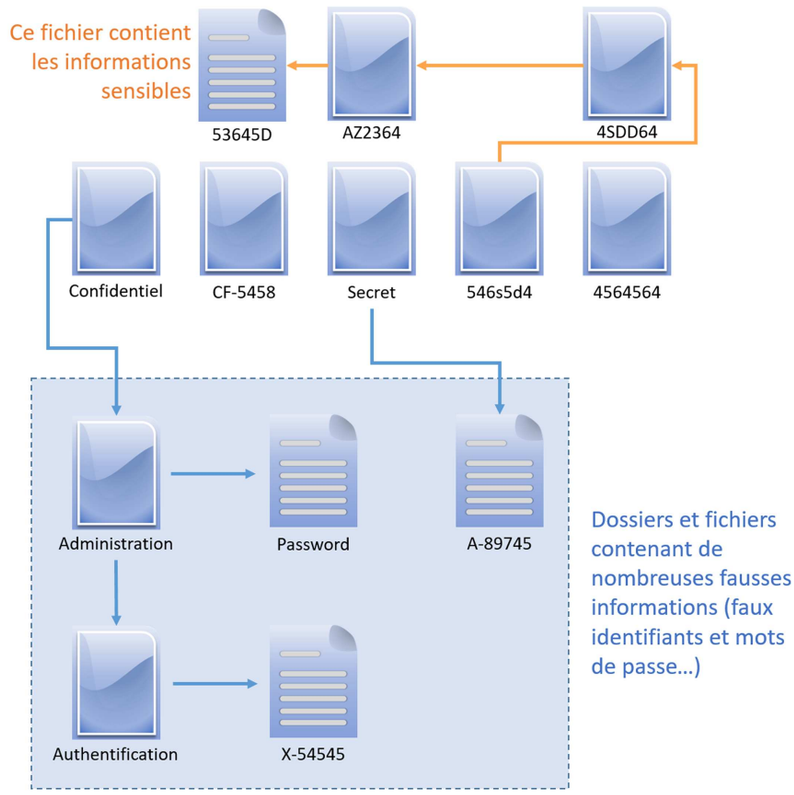

Figure 8. Scénario : détourner l'attaquant et lui faire perdre du temps.

4.2.3. Mimétisme agressif : description et exemples naturels

Le mimétisme agressif est utilisé par certains prédateurs pour éviter d'être identifié par leurs proies. De tels prédateurs peuvent, par exemple, ressembler à une fleur ou une feuille morte.

Organisme : Hymenopus coronatus

Hymenopus coronatus est une mante orchidée, elle fait partie des mantes fleurs (ressemblance et comportement). Elle est insectivore et se nourrit notamment de papillon. Hymenopus coronatus pratique un mimétisme agressif pour leurrer ses proies: ces dernières viennent butiner la mante orchidée sans méfiance.

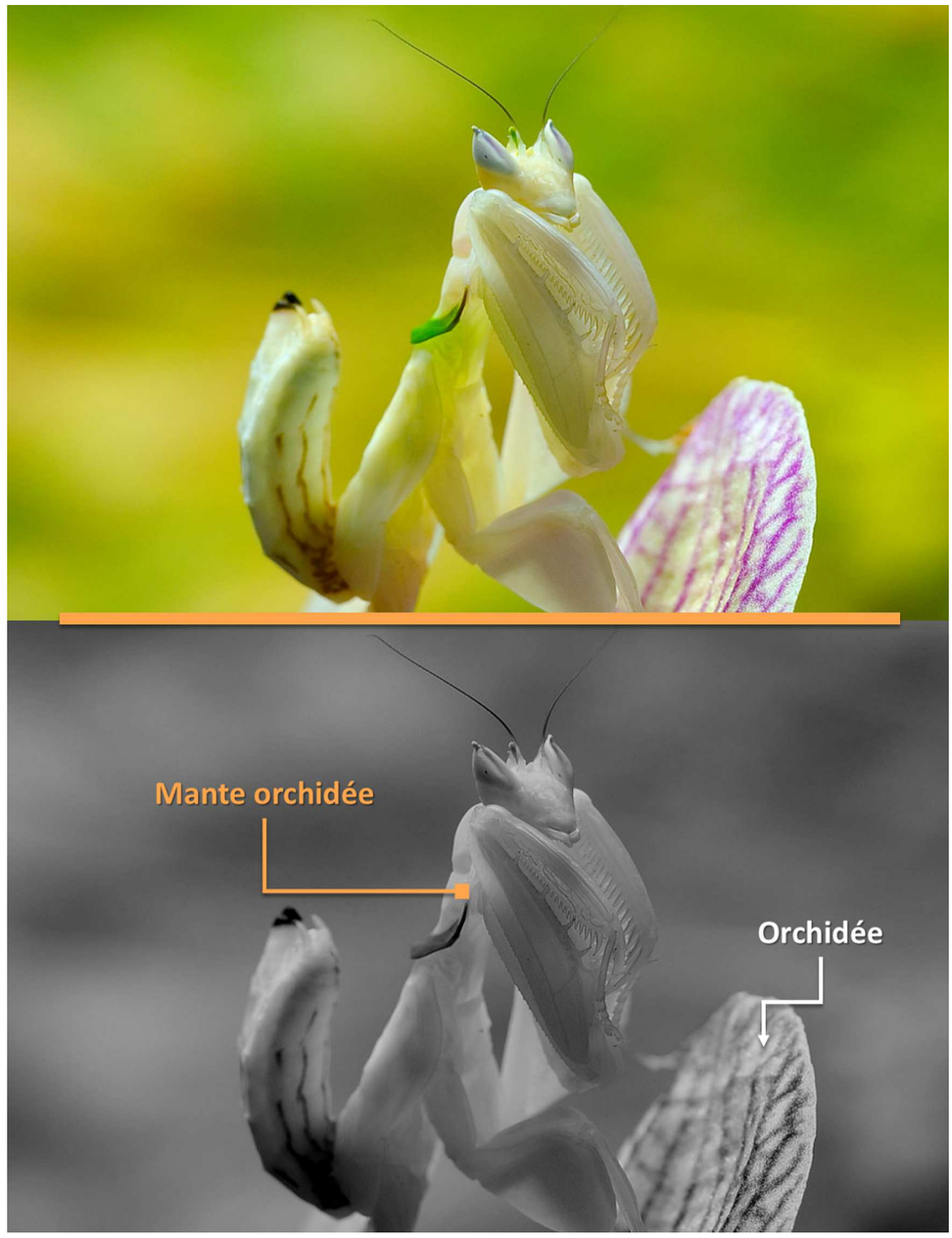

Figure 9. Hymenopus coronatus. Photographe : Luc Viatou. Novembre 2008.

4.2.4. Mimétisme agressif : Application cybersécurité

Ci-dessous, deux exemples de concepts pour le milieu cyber.

Concept : perturber les efforts de l'attaquant et l'avertir

Plusieurs documents sont forgés de manière à contenir de fausses informations ainsi qu'une charge utile dissimulée. Ces documents sont stratégiquement placés de manière à attirer l'attention de l'attaquant en cas d'intrusion et de reconnaissance.

Le document qui contient les véritables informations sensibles est chiffré et dissimulé parmi les documents forgés. En cas d'intrusion et d'exfiltration, il est probable que l'attaquant soit dupé : il exfiltre un document forgé qui contient une charge utile.

Lorsque ce dernier est consulté par l'attaquant sur son système : la charge s'active et **peut enclencher l'auto-suppression du document**. D'autres actions sont possibles, par exemple : la charge affiche **un message d'avertissement sur les risques et sanctions du crime réalisé**. Ces diverses actions possibles ont aussi pour but de **surprendre l'adversaire** et de **provoquer de l'inquiétude**.

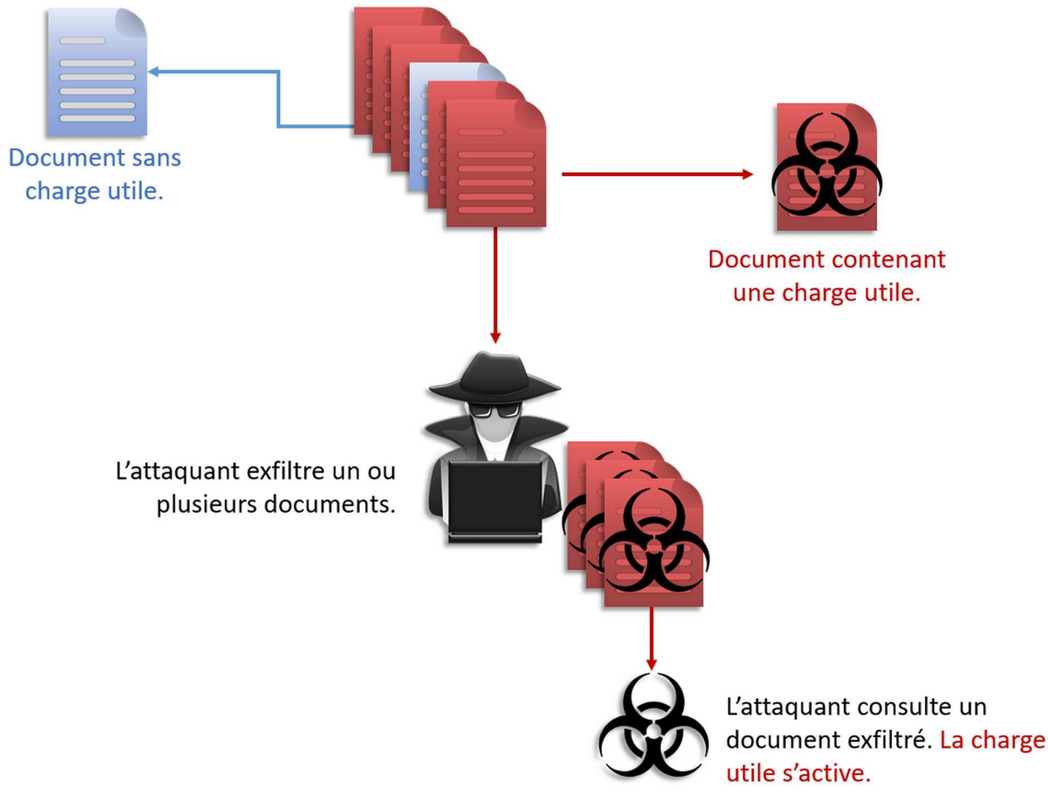

Figure 10. Documents forgés pour perturber l'effort de l'attaquant.

Concept : récolter des informations sur l'attaquant

Ce second concept propose que l'activation de la charge utile enclenche une collecte discrète d'informations sur l'environnement de l'attaquant (adresse IP, nom de machine…). Ces dernières sont téléversées vers un serveur C2 maitrisé par des analystes (cybersécurité). Ce concept contribue à la stratégie du **renseignement sur la menace**.

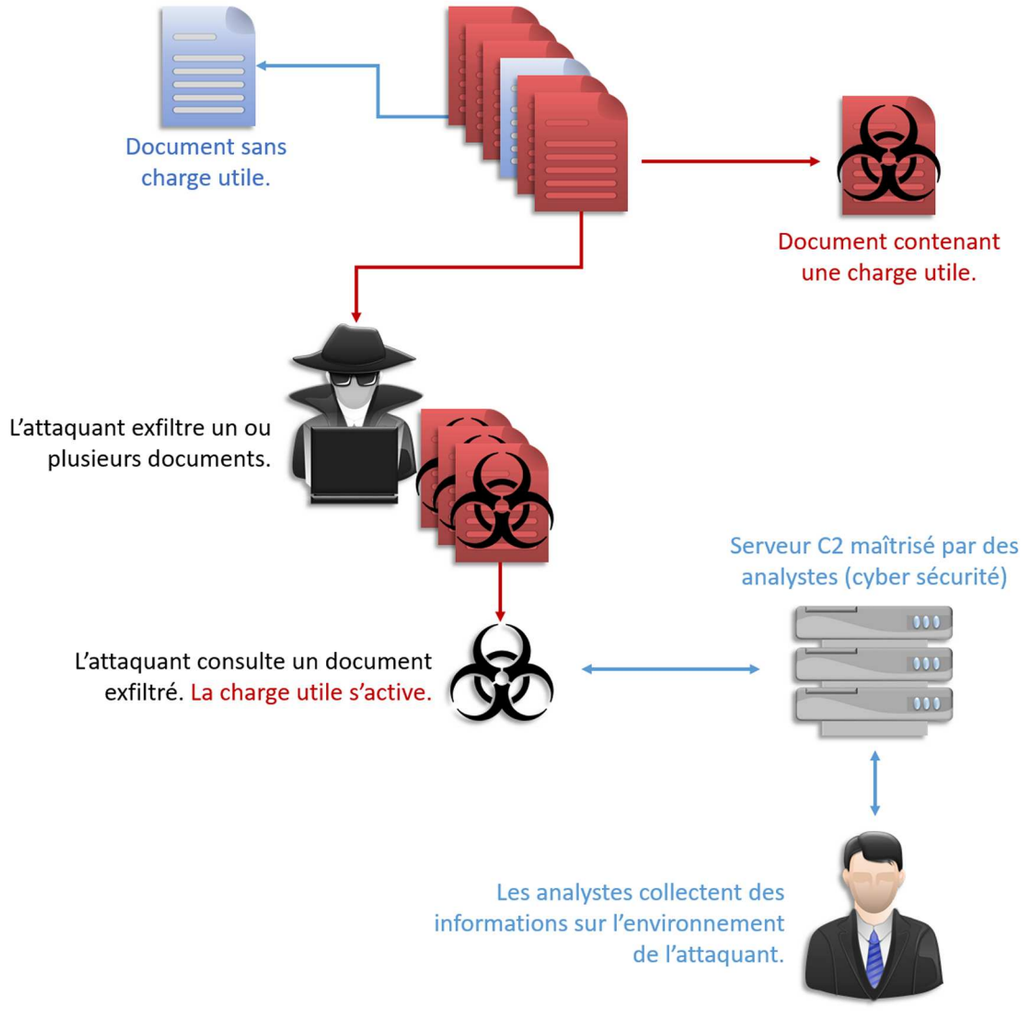

Figure 11. Documents forgés pour collecter des informations sur l'attaquant.

4.3. S'inspirer du camouflage

4.3.1. Coloration : description et exemple naturel

Une méthode de camouflage très répandue dans le milieu naturel est la coloration. Cette dernière consiste à l'organisme de développer une couleur qui lui permet de se fondre dans l'environnement qui l'entour (*Background matching*). La méthode de la coloration peut, par exemple, être utilisée pour **psychologiquement leurrer le prédateur** : **déception par la dissimulation** et faire **perdre du temps** (le prédateur doit chercher les détails).

Organisme : Nezara viridula

Ci-dessous, une photographie d'une larve de punaise verte " puante " Nezara viridula. Bien qu'étant encore au stade larvaire (été), la coloration verte commence à recouvrir plusieurs parties du corps.

Figure 12. Punaise Nezara viridula. Photographe : Analyste CTI. Garrigue de la région du Gard. Champ de tomate. Juillet 2021. Punaise adulte : photograpie pixabay Fablegros.

4.3.2. Coloration : Application cybersécurité

Ci-dessous, un exemple de concept pour le milieu cyber.

Concept : rendre une information indiscernable à l'attaquant

L'objectif de ce concept est de **décevoir par dissimulation** et de **faire perdre du temps** à l'attaquant. Pour cela, de nombreuses pages contenant de fausses informations sont créées dans un document Word. Les informations sensibles sont écrites, en blanc sur fond blanc, dans une page insérée aléatoirement entre les autres. Dans ce concept d'obfuscation, la visibilité des informations sensibles se confond avec l'arrière-plan (*Backgound matching*).

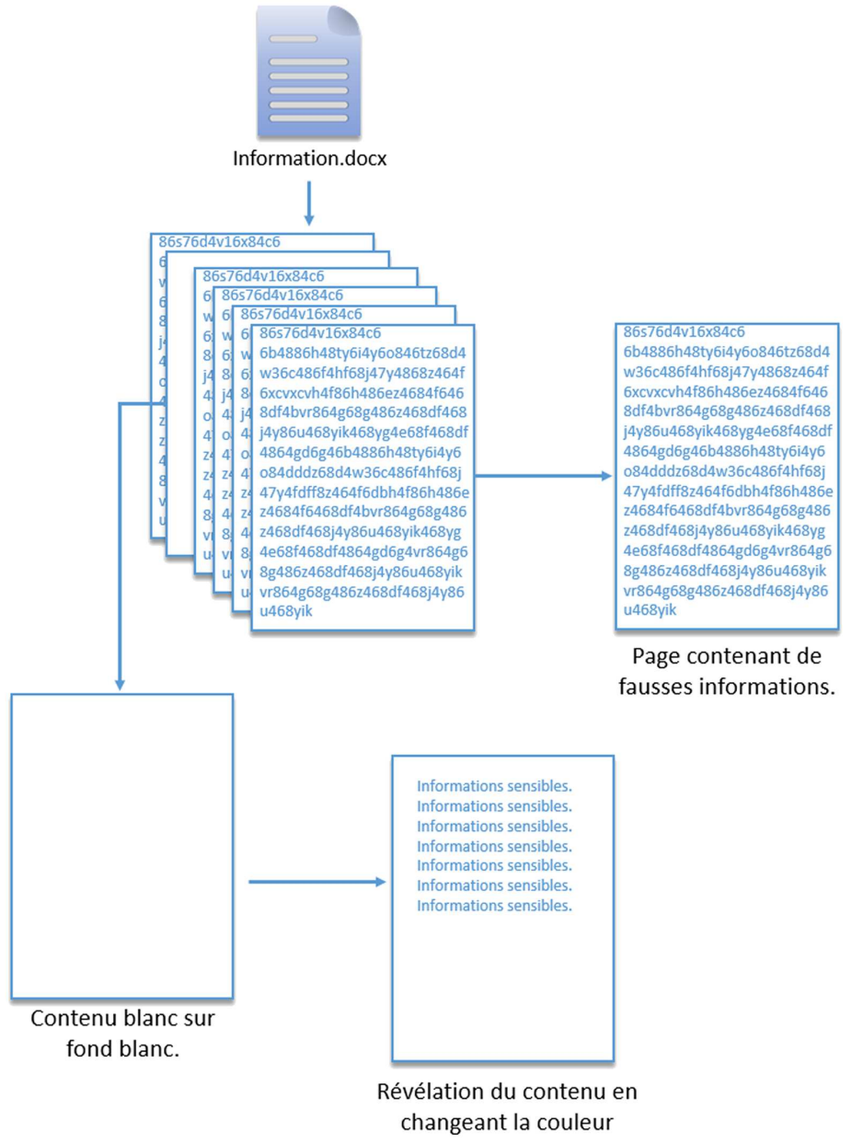

Figure 13. Les informations sensibles sont dissimulées via une coloration qui correspond à celle de l'arrière-plan.

4.3.3. Coloration disruptive : description et exemple naturel

La coloration disruptive est un camouflage optique qui permet à un organisme de se dissimuler dans l'environnement. Ce type de camouflage peut être caractérisé par des rosettes (motifs arrondis). Les motifs rompent la silhouette d'ensemble de l'animal afin de réduire sa détectabilité. Il est ainsi très difficile, par exemple, pour une proie d'identifier un léopard dans la végétation herbacée.

Organisme : Leopardus Paradalis

Ci-dessous, une photographie d'un léopard Leopardus Paradalis. Ce félin vit en Amérique du Sud et en Amérique Central. Le pelage de ce félin correspond à un camouflage optique : **la coloration disruptive**. Celui-ci est constitué de rosettes (motifs arrondis).

Figure 14. Organisme: Leopardus Paradalis. Photographe : Analyste CTI. Muséum d'Histoire Naturelle et Préhistoire de Nîmes. Juillet 2021. Ocelot camouflé au sol : Photographie U.S. Fish and Wildlife Service - Wikipedia - Domaine public.

4.3.4. Coloration disruptive : Application cybersécurité

Ci-dessous, un exemple de concept pour le milieu cyber.

Concept : rendre une information indiscernable à l'attaquant (version texte)

Identifier un code sensible dans le contenu ci-dessous peut être extrêmement difficile pour un attaquant. Premièrement, l'attaquant peut **subir l'effet du camouflage et ne pas discerner la présence potentielle du code sensible**. Deuxiément, toutes tentatives de discerner le code sensible **peuvent demander énormément de temps**.

```
Iqs4////46qd41q13////w5xc1e78 047 8g4////0t86uk4086om470fg87vx3v4d3b////48ghnj4768g7////86z64dfsd6
68j46b48x68c4086///e4fr0///8h4ty860k4060m4//86k4f8s6f04dfty6k4////m68m/64068jk46g1sd53f21s,2df46z
e5r///7j48i3006l1435b13v4568f86az48////6tj460y13510bg,sdf1ze34z53g4////13h4ffh5h41z864fsdgf41xv123b
45f4jg863///k4g8//64d3f1wscxv1523n4g6,4g86h486///sdx4xv51b254g/h58j4df86g4s6dq6x////3c14wx0vfvgf1x
05b1fn254j,;8604gfh86s4d//f6qxw3xv456n4gj86k476g8h4s35////7fg56g486d6dg4df86jghjgjgjn,kilyzeadwcxvvv
786b4,////k7op78m4/op89m40lui9////847z89erazd4sd568q4r4t89k474////654t35ze484rr48erfeee456570/bkb
98879u87/o9i/8p/79k8l4x7jk68l7j68jkgth45dg1d314a78azd7cd48c53xcv////4f58sd8cs4dcwx5cv4x8cv76c14//cv
68///s4c6s4cx56cv4x866bxg4////d864ger46de4a086///z4s6qs4ws23f4/vj8k48/6ol468j4;3n,46bv83n4,86hj4;l6j;
k//486g///hj4nf860//g/////4gh86k4j86486io4p00847u89789798k46436453514068k46///8y4k4bh648j8y9jk4b
h64g8/6j469x947y86i76r8t/4z68/e4a64kg0hj878f///sd9fsf4s////df32b012gh,1jk;1/4/////5lm/45/m4/7io/m4///
4kt5j8gz4d4/////0azd5sdv5w///4ng4j78th58df4gd/fg48xdrgt7600ef4/a84t64u4hgf6h46h46h406555gh46df//46
dfg454v4v4x45v680sdf47684xfz0/6/ettyty6ty4gf5h4j4i4k6kll654h3dv1s34a6zaa//64//dq6sc14s6v4dt84t6t/46d
v46//dv46dv486f4gry684htu6j4yu4j86uj487////89u7t89u7yu89i7yui7///056ty45h1h21tr////1rt40rh4r6gh4s08
```

Figure 15. Code dissimulé dans un contenu.

Dans ce concept d'obfuscation, le code sensible **df32b012gh,1jk;145lm45m47iom4** est dissimulé en s'inspirant du pelage du léopard. Le caractère typographique **/** est ajouté de manière aléatoire dans le code sensible : **df32b012gh,1jk;1/4/////5lm/45/m4/7io/m4**. Ajouté, le caractère **/** agit telle une rosette (la coloration disruptive) : il rompt la "silhouette" du code sensible et fait confondre ce dernier avec tout le reste du contenu. Seul un utilisateur ayant eu connaissance de ce code peut l'identifier facilement.

```
Iqs4////46qd41q13////w5xc1e78 047 8g4////0t86uk4086om470fg87vx3v4d3b////48ghnj4768g7////86z64dfsd6
68j46b48x68c4086///e4fr0///8h4ty860k4060m4//86k4f8s6f04dfty6k4////m68m/64068jk46g1sd53f21s,2df46z
e5r///7j48i3006l1435b13v4568f86az48////6tj460y13510bg,sdf1ze34z53g4////13h4ffh5h41z864fsdgf41xv123b
45f4jg863///k4g8//64d3f1wscxv1523n4g6,4g86h486///sdx4xv51b254g/h58j4df86g4s6dq6x////3c14wx0vfvgf1x
05b1fn254j,;8604gfh86s4d//f6qxw3xv456n4gj86k476g8h4s35////7fg56g486d6dg4df86jghjgjgjn,kilyzeadwcxvvv
786b4,////k7op78m4/op89m40lui9////847z89erazd4sd568q4r4t89k474////654t35ze484rr48erfeee456570/bkb
98879u87/o9i/8p/79k8l4x7jk68l7j68jkgth45dg1d314a78azd7cd48c53xcv////4f58sd8cs4dcwx5cv4x8cv76c14//cv
68///s4c6s4cx56cv4x866bxg4////d864ger46de4a086///z4s6qs4ws23f4/vj8k48/6ol468j4;3n,46bv83n4,86hj4;l6j;
k//486g///hj4nf860//g/////4gh86k4j86486io4p00847u89789798k46436453514068k46///8y4k4bh648j8y9jk4b
h64g8/6j469x947y86i76r8t/4z68/e4a64kg0hj878f///sd9fsf4s////df32b012gh,1jk;1/4/////5lm/45/m4/7io/m4///
4kt5j8gz4d4/////0azd5sdv5w///4ng4j78th58df4gd/fg48xdrgt7600ef4/a84t64u4hgf6h46h46h406555gh46df//46
dfg454v4v4x45v680sdf47684xfz0/6/ettyty6ty4gf5h4j4i4k6kll654h3dv1s34a6zaa//64//dq6sc14s6v4dt84t6t/46d
v46//dv46dv486f4gry684htu6j4yu4j86uj487////89u7t89u7yu89i7yui7///056ty45h1h21tr////1rt40rh4r6gh4s08
```

Figure 16. Code dissimulé dans un contenu.

Concept : rendre une information indiscernable à l'attaquant (version graphique)

Le principe est identique au concept précédent, mais la technique est différente. Un mot de passe est dissimulé dans l'image ci-dessous. Chaque lettre du mot de passe à une coloration qui correspond à son arrière-plan. De plus, les lettres sont dispersées de manière à rompre la "silouhette" du mot de passe.

Figure 17. Mot de passe dissimulé dans une image.

En réalisant une recherche de contour avec un logiciel de dessin, les lettres sont révélées :

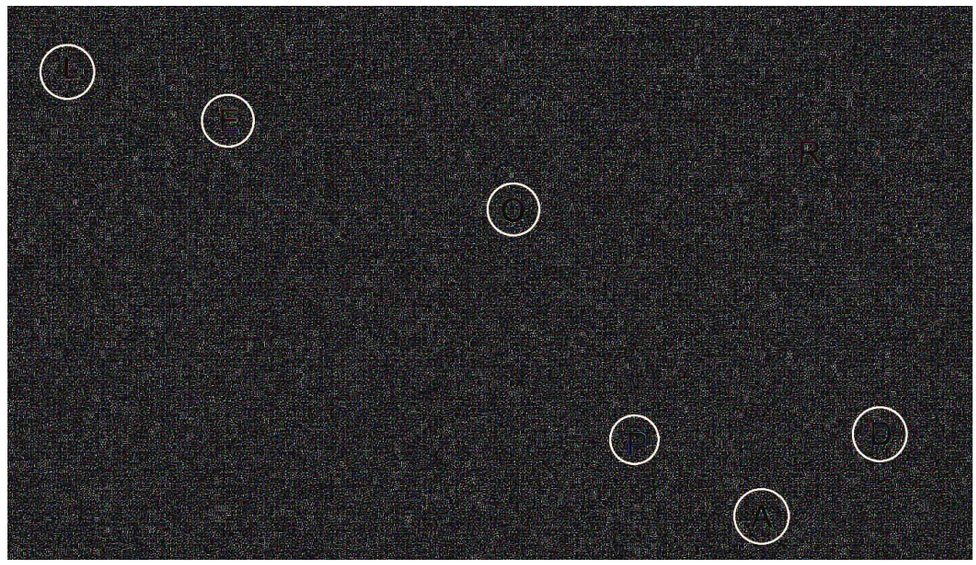

Figure 18. Mot de passe révélé dans l'image.

Le mot de passe est **LEOPARD** :

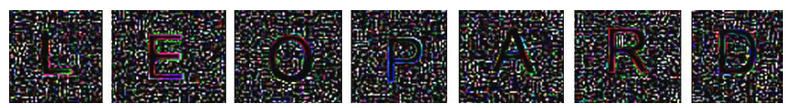

Figure 19. Mot de passe réassemblé.

4.4. Cyberpsychologie

Les sections précédentes ont démontré comment développer des concepts utiles en cybersécurité en s'inspirant du mimétisme et du camouflage naturel. De ces efforts de réflexion, il en découle des tactiques psychologiques intéressantes.

4.4.1. Tactiques psychologiques

Cette section présente une liste (non exhaustive) de quelques tactiques identifiées précédemment.

- Détourner / distraire l'attention
- Réorienter les efforts de l'offensive
- Provoquer du stresse
- Provoquer de la frustration et de la colère
- Décourager l'aboutissement de l'offensive
- Déception par dissimulation
- Embrouiller l'esprit
- Surprendre / choquer
- Avertir que l'offensive aura des conséquences (sanctions prévues par le Code pénal. Imposer la supériorité de la loi)
- Avertir que l'offensive est vaine (imposer la supérioté défensive)
- Provoquer de l'inquiétude

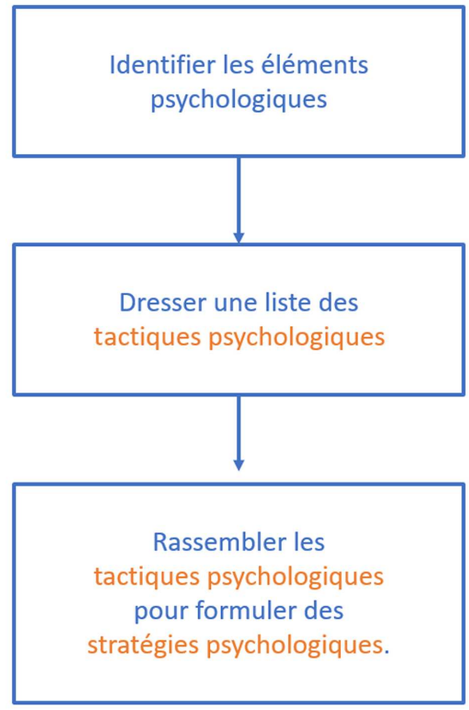

Figure 20. De l'inspiration vers la stratégie.

4.4.2. Stratégies psychologique

Les **tactiques psychologiques** peuvent être regroupées, par exemple, dans deux **stratégies psychologiques** : **Démoraliser** et **Etudier**. Ces dernières se conjuguent aux grands axes d'effort de la cybersécurité : la **cyberdéfense** et le **renseignement** de la menace cyber.

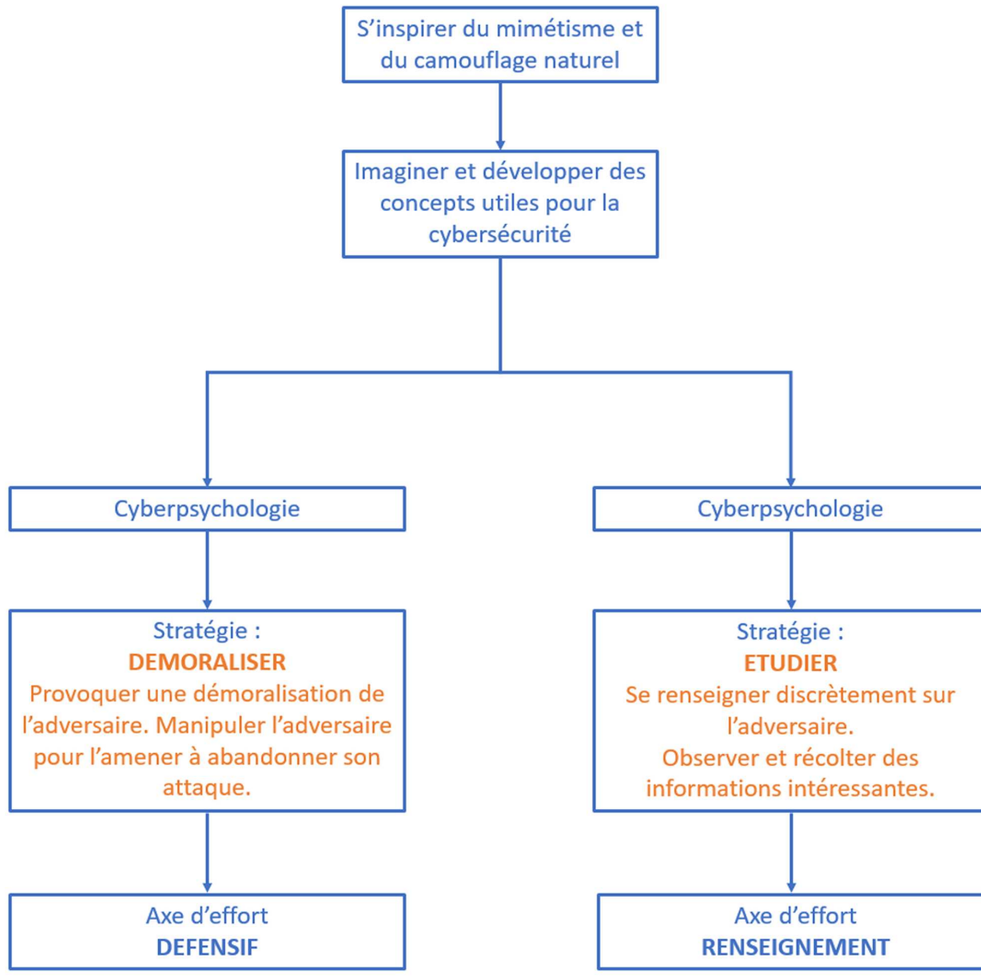

Figure 21. De l'inspiration vers la stratégie.

4.5. Observer, imaginer et conceptualiser

4.5.1. Un petit guide

Ci-dessous, un petit guide pour s'entrainer et développer ses propres concepts. Les étapes conseillées sont les suivantes :

- Étape 0 - **Curiosité et exploration**. Que se passe-t-il dans la nature ? (Prendre des photographies)
- Étape 1 - **Observation de la photographie**. Y a-t-il un organisme ?
- Étape 2 - **Identification de l'organisme**. De quoi s'agit-il ?
- Étape 3 - **Identification de la méthode**. Que fait l'organisme pour se dissimuler dans son environnement ?
- Étape 4 - **Imagination et conceptualisation**. Quelle utilité pourrait avoir cette méthode dans la cybersécurité ?
- Étape 5 - **Cyberpsychologie**. Y a-t-il des éléments psychologiques utiles pour la cybersécurité ?

4.5.2. Entrainement

Ci-dessous, une photographie pour s'entrainer. Pour cela, il suffit d'appliquer les étapes 1 à 5 :

Figure 22. Observation, imagination et conceptualisation. Photographe : Analyste CTI. Garrigue de la région du Gard. Avril 2024.

4.6. Conclusion

Le mimétisme et le camouflage naturel représentent une source infinie d'inspiration. Explorer et comprendre ces phénomènes naturels permet aux analystes d'imaginer et de développer des concepts utiles à la cybersécurité.

C'est au coeur de cet effort de réflexion que s'illustrent de potentielles tactiques psychologiques. Ensemble, ces tactiques peuvent être coordonnées de manière stratégique : **démoraliser** l'adversaire et l'**étudier**.

Ces **stratégies psychologiques** se conjuguent et enrichissent les grands axes d'efforts de la cybersécurité que sont la **cyberdéfense** et le **renseignement** de la menace cyber.

5. Références

CVE

- https://www.cve.org/CVERecord?id=CVE-2024-31705
- https://www.cve.org/CVERecord?id=CVE-2024-1874
- https://www.cve.org/CVERecord?id=CVE-2024-20295
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-cmd-inj-mUx4c5AJ

MISPADU

- https://thehackernews.com/2024/04/mispadu-trojan-targets-europe-thousands.html
- https://blog.morphisec.com/mispadu-infiltration-beyond-latam
- https://thehackernews.com/2024/02/new-mispadu-banking-trojan-exploiting.html

Cyberpsychologie : s'inspirer du mimétisme et du camouflage naturel

- https://www.aquaportail.com/dictionnaire/definition/2761/mimetisme
- https://sciences-nature.fr/biodiversite/interactions-biologiques/camouflage-et-mimetisme/
- https://fr.wikipedia.org/wiki/Camouflage
- https://inpn.mnhn.fr/espece/cd_nom/54475
- https://lejardindesoiseaux.fr/autres/les-ocelles-des-papillons/
- https://nomadica.jimdofree.com/poissons/poissons-papillons/chelmon-rostratus/
- https://fr.wikipedia.org/wiki/Ocelot
- https://fr.wikipedia.org/wiki/Coloration_disruptive
- https://www.britannica.com/science/disruptive-coloration
- https://www.researchgate.net/figure/An-example-of-disruptive-colouration-juvenile-ocelot-Leopardus-pardalis-in_fig1_308698072
- https://fr.wikipedia.org/wiki/D%C3%A9ception_(militaire)
- https://en.wikipedia.org/wiki/Flower_mantis
- https://en.wikipedia.org/wiki/Hymenopus_coronatus
- https://pixabay.com/fr/photos/nezara-viridula-punaise-verte-3651970/