aDvens

Security for the greater good

Bulletin mensuel CTI

de Mars

CERT aDvens
CERT aDvens - CTI
Advens - 38 rue des Jeuneurs - 75002 Paris

SOMMAIRE

1. SYNTHÈSE

Ce mois-ci, le CERT aDvens vous présente une matrice d'analyse des procédés d'ingénierie sociale et des vulnérabilités critiques à surveiller :

- trois vulnérabilités d'intérêt, en supplément de celles déjà publiées.
- une exposition de l'outil *DECEPTION* destiné à l'observation des mécanismes psychologiques de manipulation cybercriminelle.

Autant de sujets essentiels pour anticiper les risques et renforcer votre posture de cybersécurité.

2. VULNÉRABILITÉS

2.1. Kubernetes - CVE-2025-1974

Les chercheurs de la société de sécurité cloud Wiz ont découvert des vulnérabilités dans l'Ingress Nginx Controller de Kubernetes, un composant utilisé par environ 40% des clusters hébergés sur le cloud d'après les chercheurs. Ces cinq vulnérabilités ont été surnommées IngressNightmare.

Les quatre premières vulnérabilités permettent à un attaquant de modifier sans authentification les paramètres de l'*ingress controler* en envoyant des requêtes vers le webhook d'*admission*.

La dernière est plus critique, identifiée comme CVE-2025-1974, permet à un attaquant de charger cette configuration malveillante injectée par les vulnérabilités précédentes, menant à une exécution de code arbitraire dans le pod nginx. Ce pod étant très privilégié, l'attaquant peut récupérer les secrets du cluster et devenir administrateur de ce cluster.

Le webhook *ingress controler* n'est pas exposé par défaut mais certains composants de journalisation ou de métrique vont demander qu'il soit exposé.

2.1.1. Type de vulnérabilité

- **CWE-653** : Improper Isolation or Compartmentalization

2.1.2. Risques

- Compromission du cluster
- 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

- ingress-nginx
  - Versions antérieures à 1.11.4
  - Version 1.12.0

2.1.5. Recommandations

Mettre à jour ingress-nginx vers la version 1.11.5, 1.12.1 ou ultérieure.

Il est également recommandé de limiter l'accès au *webhook* d'*admission* en limitant son exposition sur internet et en mettant en place des règles *NetworkPolicies* pour autoriser uniquement le ControlPlane à accéder à ce *webhook*.

Des informations complémentaires sont disponibles dans le bulletin de Kubernetes.

2.1.6. Preuve de concept

Une preuve de concept est disponible en sources ouvertes.

2.2. Veeam - CVE-2025-23120

Découverte par les chercheurs en sécurité de Watchtowr, cette faille est due à l'utilisation de listes de blocage.

Une désérialisation non sécurisée dans Veeam Backup & Replication permet à un attaquant authentifié d'exécuter du code arbitraire.

Les vulnérabilités dans Veeam Backup and Replication sont souvent exploitées par les groupes de rançongiciel.

2.2.1. Type de vulnérabilité

→ **CWE-502** : Deserialization of Untrusted Data

2.2.2. Risque

→ Exécution de code arbitraire

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

Vecteur d'attaque	Réseau	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

2.2.4. Produits impactés

→ Veeam Backup & Replication versions antérieures à 12.3.1 (build 12)

2.2.5. Recommandations

Mettre à jour Veeam Backup & Replication vers la version 12.3.1 (build 12) ou ultérieure.

Des informations complémentaires sont disponibles dans le bulletin de Veeam.

2.2.6. Preuve de concept

Une preuve de concept est disponible en sources ouvertes.

2.3. Ruby SAML - CVE-2025-25291

Une vulnérabilité liée à la différence de traitement de fichiers XML par les librairies ReXML et Nokogiri a été découverte dans Ruby SAML. En menant une attaque de type XML Signature Wrapping, un attaquant peut contourner l'authentification.

2.3.1. Type de vulnérabilité

- **CWE-347** : Improper Verification of Cryptographic Signature

2.3.2. Risque

- Contournement d'authentification

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	Aucun

2.3.4. Produits impactés

- RUBY-SAML
  - Versions 1.10.5 et antérieures
  - Versions 1.12.3 et antérieures
  - Versions antérieures à 1.18.0
  - Versions 2.2.2 et antérieures
- GitLab CE/EE
  - Versions antérieures à 17.7.7
  - Versions antérieures à 17.8.5
  - Versions antérieures à 17.9.2
- omniauth-saml (RubyGems)
  - Versions antérieures à 1.10.6
  - Versions antérieures à 2.1.3
  - Versions antérieures à 2.2.3
- NetApp
  - ONTAP tools for VMware vSphere 10
  - StorageGRID (formerly StorageGRID Webscale)

2.3.5. Recommandations

Mettre à jour RUBY-SAML vers la version 1.10.6, 1.12.4, 1.18.0, 2.2.3 ou ultérieure.

Mettre à jour GitLab CE/EE vers la version 17.7.7, 17.8.5, 17.9.2 ou ultérieure.

Mettre à jour omniauth-saml (RubyGems) vers la version 1.10.6, 2.1.3, 2.2.3 ou ultérieure.

Mettre à jour NetApp StorageGRID (formerly StorageGRID Webscale) vers la version 11.9.0.5 ou ultérieure.

Des informations complémentaires sont disponibles dans le bulletin de RUBY-SAML.

2.3.6. Preuve de concept

Une preuve de concept est disponible en sources ouvertes.

3. PSYCHOLOGIE OFFENSIVE : LE NOUVEAU MODÈLE DECEPTION

3.1. Le risque de psychologie offensive

Dans un monde où les menaces cybernétiques évoluent constamment, les attaquants ajustent également leurs stratégies psychologiques de manière de plus en plus sophistiquée. Face à ce brouillard de guerre numérique, les analystes disposent de modèles technologiques, tels que la Matrice MITRE ATT&CK ou la chaine d'attaque de Lockheed Martin, qui fournissent une base de connaissances précieuse. Cependant, au-delà de l'aspect technologique, la dimension psychologique reste encore largement ignorée ou sous-estimée. Le modèle DECEPTION s'efforce de combler ce vide en offrant une première base de connaissances sur les tactiques et techniques de psychologie offensive fréquemment observées lors des cyberattaques.

3.2. Comprendre le modèle DECEPTION

3.2.1. Description

Le modèle **DECEPTION** est une base de connaissances conçue pour cataloguer et analyser les tactiques et techniques de manipulation psychologique offensives utilisées par les cybercriminels lors de leurs attaques contre les infrastructures d'entreprise. Ce modèle se concentre principalement sur l'ingénierie sociale, un domaine essentiel des cyberattaques, et s'organise autour de six grandes tactiques : **reconnaissance**, **ressources**, **initialisation**, **intrusion**, **exploration** et **impact**. Ces étapes décrivent de manière détaillée le parcours typique d'un attaquant utilisant un arsenal psychologique pour manipuler, décevoir et exploiter les utilisateurs.

Lancé en mars 2024, **DECEPTION** est actuellement dans sa version 1.0 et représente un outil de référence en matière de compréhension des méthodes d'ingénierie sociale. Ce modèle peut être utilisé de manière autonome ou en complément d'autres bases de cybersécurité reconnue, telle que la matrice MITRE ATT&CK ou la chaine d'attaque cybercriminelle de Lockheed Martin. Utilisées de manière complémentaire, ces bases permettent ainsi une approche plus holistique (techniques informatiques et psychologiques) et approfondie de la défense contre les cybermenaces.

Figure 1. Le logo officiel.

3.2.2. Importance

Trop souvent négligés, les aspects psychologiques, tant sur le plan défensif qu'offensif, représentent bien plus qu'un simple pilier fondamental de la cybercriminalité et de la cybersécurité. Il n'est pas rare qu'un analyste rencontre des éléments relatifs à la psyché lors de l'étude d'une compromission, notamment lorsqu'il analyse des courriels d'hameçonnage, qui regorgent fréquemment de techniques de manipulation psychologique. En somme, la guerre psychologique est indissociable de la guerre technologique. Comprendre et cataloguer ces tactiques et techniques peut s'avérer essentiel pour renforcer la protection contre les cyberattaques présentes et avenirs.

3.2.3. Objectif

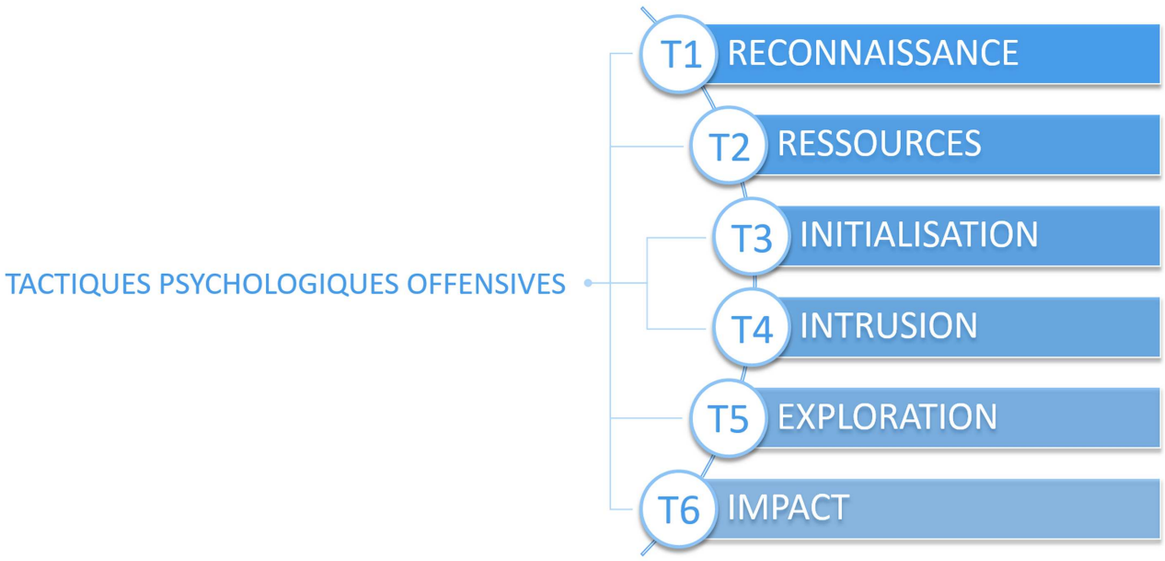
Ce modèle permet d'aider les analystes et les psychologues à comprendre comment les attaquants opèrent pour manipuler et décevoir leurs victimes. Avec ce type de connaissance, des moyens appropriés peuvent être mis en œuvre pour protéger les collaborateurs de l'entreprise.

3.2.4. Fonctionnement

Lors de l'étude d'une cyberattaque, l'analyste commence par identifier, si possible, les tactiques employées, puis sélectionne les techniques les plus adaptées. Ce qui distingue cette base de connaissances, c'est que les techniques sont flexibles et peuvent être appliquées à différentes tactiques, ce qui signifie qu'elles ne sont pas rigoureusement limitées à un cadre spécifique. Par exemple, l'analyste peut choisir la technique d'exploitation des habitudes pour les tactiques d'initialisation et d'exploration. Une fois cette première étape accomplie, il revient à l'analyste de réaliser un tableau ou un texte pour mettre en avant ses choix.

3.2.5. Les Tactiques

Le modèle **DECEPTION** s'articule autour de six tactiques de psychologies offensives. Il s'agit de moyens habiles employés par l'attaquant pour obtenir le résultat voulu.



T1 - Reconnaissance

La première tactique utilisée est la reconnaissance, celle-ci consiste pour l'attaquant à recueillir des informations cruciales susceptibles d'être exploitées pour planifier des actions futures. Cette phase de reconnaissance est primordiale, car elle permet à l'attaquant d'obtenir une vue d'ensemble de l'environnement cible et d'identifier les failles potentielles à exploiter (vulnérabilités psychologiques). Selon les informations récoltées, il pourra alors ajuster ses méthodes et stratégies d'attaque de manière plus ciblée et efficace. Par exemple, l'attaquant peut se renseigner sur des éléments aussi variés que le nombre d'employés, leur niveau de compétence en matière de cybersécurité, la hiérarchie, ou même les processus internes de l'organisation. Cette information permet de personnaliser l'attaque en fonction des vulnérabilités spécifiques de la cible.

Bien que cette tactique soit généralement exécutée en amont (phase pré-intrusion), elle peut également se dérouler ultérieurement (phase post-intrusion) dans l'infrastructure de la cible. Ainsi, la reconnaissance n'est pas nécessairement un processus linéaire, mais peut se dérouler de manière continue et en fonction des opportunités qui se présentent.

Code de référence tactique : **T1**

T2 - Ressources

Pour mener à bien son attaque, l'adversaire peut être amené à réaliser du contenu manipulateur. Cette seconde tactique consiste à élaborer toutes les ressources nécessaires pour réaliser l'objectif. Ces ressources peuvent être, par exemple, des images dessinées manuellement ou générées par l'Intelligence Artificielle.

Code de référence tactique : **T2**

T3 - Initialisation

La troisième tactique, celle de l'initialisation, est sans doute la plus délicate et la plus risquée dans le cadre d'une attaque informatique. En effet, elle représente le premier contact hostile entre l'attaquant et sa cible : une étape décisive pour franchir la première ligne de défense. À ce stade, l'attaquant met en œuvre des techniques d'ingénierie sociale visant à exploiter les

vulnérabilités psychologiques de la cible. Cela peut inclure des techniques telles que la manipulation émotionnelle, la création d'un faux sentiment d'urgence ou l'exploitation de la confiance pour amener la victime à prendre une décision impulsive, telles que le téléchargement ou l'exécution d'un logiciel malveillant. De manière subtile, l'attaquant cherche à obtenir un consentement forgé. L'attaquant peut, par exemple, se faire passer pour un supérieur hiérarchique afin d'inciter la cible à accomplir une action compromettante pour l'organisation.

Code de référence tactique : **T3**

T4 - Intrusion

Une fois que l'attaquant a réussi à obtenir un accès initial au système ou réseau ciblé, il peut poursuivre ses efforts en matière de psychologie offensive pour consolider sa présence. L'objectif principal est de ne pas éveiller les soupçons des utilisateurs ou des systèmes de sécurité. Pour ce faire, l'attaquant peut, par exemple, adopter un comportement qui imite celui des utilisateurs légitimes, reproduisant certaines actions, en les effectuant à des horaires et dans des contextes similaires à ces derniers. Cette approche de mimétisme comportemental permet de masquer son activité, en la rendant indiscernable de celle d'un utilisateur classique.

Code de référence tactique : **T4**

T5 - Exploration

Probablement la tactique la plus difficile pour l'attaquant, celle-ci requiert énormément de patience et d'expérience. Après l'intrusion, il s'agit désormais pour l'attaquant d'explorer minutieusement les différents systèmes et réseaux de l'organisation ciblée, de collecter des informations importantes et de les exfiltrer. Tandis que la tactique d'intrusion s'illustre par une première découverte interne du système ou réseau, la tactique d'exploration vise des découvertes multiples et en profondeur. Pour mener à bien une tactique aussi complexe, l'attaquant peut recourir à des techniques de manipulation psychologique. Entre autres, l'attaquant peut être amené à établir une fausse relation de confiance avec des utilisateurs et à exercer une manipulation émotionnelle sur du long terme.

Code de référence tactique : **T5**

T6 - Impact

Cette tactique ultime consiste pour l'attaquant à effectuer les derniers efforts visant à exercer une influence psychologique sur la cible. À cette étape, l'attaquant peut chercher à provoquer un malaise en stimulant la peur et la confusion. Il peut également tenter de tirer parti de cette situation pour rallier des individus à sa cause, en utilisant l'impact de l'évènement comme un levier de domination. Par exemple, certaines notes de rançon émises par la franchise criminelle LockBit incluent des messages publicitaires spécifiquement destinés à la victime, proposant des opportunités d'affiliation et promettant une rémunération conséquente.

Code de référence tactique : **T6**

3.2.6. Les Techniques

Une utilisation versatile

Le modèle **DECEPTION** offre une conception flexible des techniques, permettant ainsi une utilisation plus versatile. Les techniques identifiées peuvent être positionnées librement en fonction des tactiques choisies. Par exemple, l'analyste peut observer l'exploitation du biais cognitif de l'effet de halo dans les tactiques d'**initialisation** et d'**exploration** : il s'agit donc de la même technique appliquée à deux tactiques distinctes.

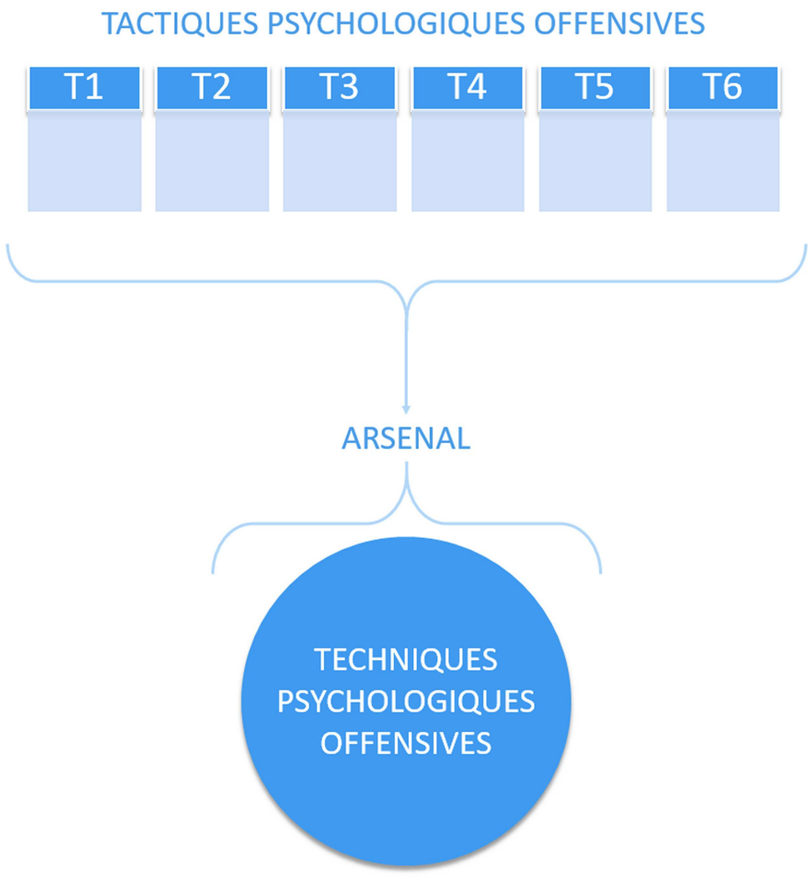
Un arsenal complexe

Ci-dessous, quelques aspects importants concernant les techniques.

- Les techniques utilisées par l'attaquant sont regroupées dans un arsenal nommé **Technique Psychologiques Offensive**.
- En source ouverte, ces techniques sont aussi retrouvées dans d'autres thèmes et appellations tels que : **dark psychology** (psychologie obscure), **ingenierie sociale** ou **piraterie psychologique**.
- Cet arsenal est vaste et assujetti à de nouvelles recherches et développement. Il n'est pas figé.

Organisation des tactiques et techniques

L'infographie ci-dessus représente les deux grands niveaux qui constituent le modèle **DECEPTION**.



Liste de techniques

Ci-dessous, une liste non-exhaustive de techniques utilisées par les attaquants.

Mensonge

Un attaquant peut faire des assertions sciemment contraires à la vérité afin de manipuler l'utilisateur. Ce travestissement de la réalité peut être réalisé de plusieurs manières, par exemple à l'oral ou par le comportement. De nombreux collectifs cybercriminels spécialisés dans le crime rançongiciel utilise le mensonge, notamment en faisant croire à leurs victimes que les données extorquées seront supprimées après le paiement de la rançon (Record, 2024).

Code de référence technique : **01**

Psychologie inversée

Selon le dictionnaire de Cambridge (2025), la psychologie inversée consiste à demander à quelqu'un de faire l'inverse de ce qu'on veut vraiment, en anticipant qu'il réagira par désaccord.

Code de référence technique : **02**

Bombardement affectif

La technique du bombardement affectif (alias "love bombing" ou "love flooding") consiste à manipuler un individu en utilisant des compliments et de la compassion. Le manipulateur tente de créer l'illusion d'une relation parfaite (clinique e-santé, 2024).

Code de référence technique : **03**

Rétention affective

Le principe de la rétention affective (alias "love withholding" ou rétention émotionnelle) consiste pour le manipulateur à volontairement se distancer, émotionnellement et/ou physiquement, de sa victime pour la punir en créant un isolement psychologique (Psychology Today, 2023). Elle peut se manifester tant que la victime ne réalise pas ce qui lui est demandé par son manipulateur. Cette rétention affective peut être considérée comme l'inverse du bombardement affectif.

Code de référence technique : **03**

Exploitation des habitudes

Plusieurs études ont démontré comment les cybercriminels exploitent les habitudes des utilisateurs pour compromettre l'organisation ciblée. Selon les recherches publiées par MasterCard dans le rapport Cyber's Human Condition, les habitudes représentent la quatrième vulnérabilité psychologique la plus exploitée par les attaquants.

Code de référence technique : **04**

Exploitation de biais cognitifs

Pour obtenir un consentement manipulé, les attaquants utilisent très souvent l'exploitation de biais cognitifs, notamment lors d'attaques par courriels d'hameçonnage. Les attaquants forgent un contenu malveillant de manière à profiter des vulnérabilités psychologiques des utilisateurs ciblés. Lors de l'arnaque au président, par exemple, c'est le biais d'autorité que les attaquants cherchent à exploiter : la tendance à accorder plus de crédibilité ou à suivre les conseils d'une personne perçue comme une autorité, même si ses propos ne sont pas forcément justifiés (Cyberdise, 2024). Point particulier : étant donné le nombre important de biais cognitifs, il est conseillé de s'appuyer sur ce https://fr.wikipedia.org/wiki/Biais_cognitif#/media/Fichier:The_Cognitive_Bias_Codex_(French)-_*John_Manoogian_III*(jm3).svg[codex].

Code de référence technique : **05**

Exploitation du manque d'expérience pratique

Lors de la tactique de reconnaissance, les attaquants peuvent identifier des utilisateurs ayant un niveau d'expérience professionnelle faible. De tels utilisateurs novices sont des cibles très prisées puisque ces dernières peuvent faire des erreurs. La vulnérabilité psychologique réside dans l'incapacité de ces utilisateurs à maîtriser les bons réflexes et saisir toutes les notions de leur travail.

Code de référence technique : **06**

Exploitation du manque de connaissance théorique

Cette technique consiste pour les attaquants à exploiter la connaissance limitée des utilisateurs sur certaines technologies ou services. Par exemple, un utilisateur peut être très expérimenté dans la gestion des courriels d'hameçonnage, mais ignorer les nouveaux risques d'hameçonnage sur d'autres services de communication.

Code de référence technique : **07**

Intimidation et menace

Très utilisée lors des cyberattaques par rançongiciels, cette technique consiste pour les attaquants à s'imposer sur leurs victimes et provoquer de la peur. En agissant ainsi, les attaquants tentent d'amener leurs victimes à réagir rapidement et de manière irrationnelle, réduisant toutes capacités de réflexion.

Code de référence technique : **08**

Restriction de choix

Cette technique est très utilisée lors des phases de négociations suite à une cyberattaque par rançongiciel. Les attaquants tentent de faire croire à la victime que le choix de ses actions est très limité. Ils peuvent, par exemple, faire croire que le seul moyen de récupérer l'accès aux données et de payer la rançon.

Code de référence technique : **09**

Révélation de secrets

Pour faire pression sur leurs victimes, les attaquants peuvent menacer de révéler publiquement des secrets de l'organisation ou de ses employés.

Code de référence technique : **10**

Ressources pour manipulation

Une ou plusieurs ressources sont utilisées pour manipuler la cible.

Code de référence technique : Image **11.1**, Vidéo **11.2**, Audio **11.3** Texte **11.4**

Si le contenu est généré par l'IA : Image **11.1-IA**, Vidéo **11.2-IA**, Audio **11.3-IA**, Texte **11.4-IA**

Mimétisme

Cette technique est utilisée par les attaquants pour se rendre semblable par le comportement et/ou l'apparence pour leurrer leurs cibles. Un acteur malveillant peut, par exemple, utiliser l'intelligence artificielle pour imiter la voix d'un employé d'une organisation et générer du contenu de manière à inciter des collaborateurs à divulguer des informations.

Code de référence technique : **12**

Satisfaction trompeuse

Les groupes APT utilisent souvent une forme de satisfaction trompeuse, qui peut se manifester sous la forme d'un leurre. Dans ce contexte, le leurre peut être un simple faux, ou une véritable application. Dans le cas d'un leurre de qualité (une véritable application), le scénario d'attaque se déroule généralement en deux étapes : d'abord, les attaquants présentent un leurre, souvent un logiciel, sur un site Web, que les utilisateurs peuvent télécharger. L'installateur téléchargé, une fois exécuté, déploie effectivement le logiciel attendu par l'utilisateur, mais il installe également de manière discrète un ou plusieurs logiciels malveillants supplémentaires. La manipulation psychologique intervient lors du déploiement du logiciel légitime, car celui-ci crée un sentiment de satisfaction et réduit l'attention de l'utilisateur, qui pense à tort que l'installation s'est déroulée correctement.

Code de référence technique : **13**

Effet d'urgence

Pour faciliter la manipulation, les attaquants peuvent introduire un effet d'urgence afin de favoriser un traitement heuristique de l'information. Cette technique est fréquemment utilisée dans le cadre de l'arnaque au président, où les malfaiteurs insistent sur le caractère urgent de la transaction frauduleuse.

Code de référence technique : **14**

Exploitation de l'empathie

Dans certains scénarios de cyberattaques, les attaquants peuvent exploiter l'empathie de la personne ciblée. Par exemple, cette technique est régulièrement observée lors de conflits armées ou de catastrophes naturels, où de faux sites de collecte de fonds ont été créés pour extorquer de l'argent.

Code de référence technique : **15**

Attaque sous faux pavillon

Dans le but d'éviter d'être identifiés, les attaquants peuvent recourir à des logiciels malveillants appartenant à d'autres groupes criminels, afin de brouiller les pistes et compliquer le travail des équipes d'experts en sécurité. Après la fuite du builder de LockBit, plusieurs groupuscules ont utilisés ce rançongiciel lors de leurs attaques pour tenter de ne pas être identifié. Cette technique a également été observée lors de cyber-braquages, où des APT nord-coréens ont déployé des rançongiciels sur les systèmes de plusieurs banques après avoir réalisé des transactions frauduleuses.

Code de référence technique : **16**

Confusion

Pour éviter d'être remarqués, certains attaquants cherchent, par exemple, à se fondre dans un flot d'activités. Des APT russes ont ainsi été observées agissant de manière subtile et discrète au sein d'un volume considérable d'activités criminelles orchestrées par plusieurs groupuscules. L'objectif des attaquants est de tirer parti du bruit de fond pour mener des attaques d'une grande précision.

Code de référence technique : **17**

Offre alléchante

D'une efficacité redoutable, cette technique est reconnue pour sa dangerosité extrême. À plusieurs reprises, l'APT Lazarus a démontré l'efficacité de cette manipulation, notamment sous la forme de fausses offres d'emploi. Au cœur de l'opération Dreamjob, cette technique a été largement utilisée pour inciter des employés à participer à des tests de recrutement sur des serveurs contrôlés par les attaquants. Piégés dans un environnement malveillant, les employés sont manipulés pour télécharger ou interagir avec des ressources forgées de manière à permettre le déploiement de logiciels de cyber-espionnage.

Code de référence technique : **18**

Moquerie / Villipender

Pour déstabiliser leurs victimes, certains attaquants recourent à la moquerie. Le groupe de ransomware ViceCity a régulièrement utilisé cette méthode pour ternir la réputation des organisations ciblées. D'autres collectifs, tels qu'Industrial Spy, vont même jusqu'à vilipender publiquement la victime en diffusant des messages sur le site de l'organisation affectée. En somme, cette technique vise à provoquer honte et humiliation chez les victimes. Par ailleurs, cette technique est considérée comme une composante de l'extorsion multiple appliquée dans le crime rançongiciel.

Code de référence technique : **19**

Coercition externalisée

Observée dans certaines attaques par rançongiciel, cette technique semble être employée lorsque l'organisation victime ne répond pas aux exigences des malfaiteurs. Dans ce contexte, les attaquants recourent à la coercition externe en ciblant les employés par SMS ou appels téléphoniques, dans le but de les inciter à faire pression sur la direction de l'organisation. Cette méthode a été observée chez les groupes de rançongiciels LockBit et SunCrypt. Par ailleurs, cette technique est considérée comme une composante de l'extorsion multiple appliquée dans le crime rançongiciel.

Code de référence technique : **20**

3.3. Exemple d'application

3.3.1. Exemple théorique 1

L'analyste choisi, par exemple, la tactique **Initialisation** (T3).

- Les techniques observées : **Bombardement affectif** (03) et **Ressources pour manipulation** (Image 11.1-IA).

Ces informations peuvent être présentées ainsi :

REFERENCES	TACTIQUES	TECHNIQUES
T3.03	Initialisation	Bombardement affectif
T3.11.1-IA	Initialisation	Ressources pour manipulation : Image générée par IA

3.3.2. Exemple théorique 2

L'analyste choisi, par exemple, les tactiques **Reconnaissance** (T1), **Initialisation** (T3) et **Impact** (T6).

- Les techniques observées pour la reconnaissance : **Bombardement affectif** (03) et **Ressources pour manipulation** (Image 11.1-IA).
- Les techniques observées pour l'initialisation : **Ressources pour manipulation** (Image 11.1-IA) et **Ressources pour manipulation** (Vidéo 11.2).
- Les techniques observées pour impact : **Révélation de secrets** (10), **Intimidation et menace** (08).

Ces informations peuvent être présentées ainsi :

REFERENCES	TACTIQUES	TECHNIQUES
T1.03	Reconnaissance	Bombardement affectif
T1.11.1-IA	Reconnaissance	Ressources pour manipulation : Image générée par IA
T3.11.1-IA	Initialisation	Ressources pour manipulation : Image générée par IA
T3.11.2	Initialisation	Ressources pour manipulation : Vidéo
T6.10	Impact	Révélation de secrets
T6.08	Impact	Intimidation et menace

3.3.3. Exemple concret

Découvert au début de l'année 2024, Troll Stealer est un logiciel de cyber-espionnage sophistiqué, utilisé par le groupe APT Kimsuky dans le cadre d'une campagne visant des institutions administratives en Corée du Sud. Afin d'infecter les systèmes des utilisateurs, les attaquants ont d'abord créé des pages Web frauduleuses, présentant des logiciels légitimes de la société SGA Solutions. Ces pages ont été minutieusement conçues pour avoir certains éléments (logo, intitulés des logiciels...) ressemblant à ceux du site authentique. Lorsqu'un utilisateur télécharge un logiciel depuis ces pages compromises, l'installateur récupéré ne se contente pas d'installer le programme légitime, mais déploie également, de manière discrète, le spyware Troll Stealer. L'utilisateur pense avoir téléchargé un logiciel en toute sécurité, mais son système est en réalité compromis, et ses données sensibles sont alors volées par les attaquants.

Ci-dessous, les révérenciels : **MITRE ATT&CK** pour les aspects techniques et **DECEPTION** pour les aspects psychologiques.

MITRE ATT&CK (version anglaise)

REFERENCES	TACTIQUES	TECHNIQUES
T1588.004	Resource development	Digital Certificates
T1204.002	Execution	Malicious File
T1059.001	Execution	PowerShell
T1059.003	Execution	Windows Command Shell
T1027.002	Defense Evasion	Software Packing
T1555.003	Credential Access	Credentials from Web Browser
T1539	Credential Access	Steal Web Session Cookie
T1057	Disovery	Process Disovery
T1087.001	Disovery	Local Account
T1083	Disovery	File and Directory Discovery
T1581.001	Disovery	Security Software Discovery
T1582	Disovery	Security Information Discovery
T1016	Disovery	Security Network Configuration Discovery
T1005	Collection	Data From Local System
T1113	Collection	Screen Capture
T1560	Collection	Archive Collected Data
T1071.002	Command and Control	Web Protocol
T1041	Exfiltration	Exfiltration over C2 Channel

DECEPTION (version française)

REFERENCES	TACTIQUES	TECHNIQUES
T1.11.4	Ressources	Ressources pour manipulation : texte
T1.11.1	Ressources	Ressources pour manipulation : image
T3.12	Initialisation	Mimétisme
T3.05	Initialisation	Exploitation de biais cognitifs : effet de halo
T3.11.4	Initialisation	Ressources pour manipulation : texte
T3.11.1	Initialisation	Ressources pour manipulation : image
T4.13	Intrusion	Satisfaction trompeuse

3.3.4. Réflexion sur le modèle DECEPTION

Limites

Ci-dessous, une liste de plusieurs limites identifiées.

- Actuellement, le modèle est une première version (1.0), sa validité n'est pas robuste.
- Étant donné le grand nombre de biais cognitif existant, il peut être difficile de savoir lequel choisir.
- Des connaissances en psychologie peuvent être nécessaires pour correctement identifier et comprendre certaines techniques.

Avantages

Ci-dessous, une liste de plusieurs avantages identifiés.

- Le modèle est utile pour aider à comprendre comment opère l'attaquant en matière de psychologie offensive.
- Une présentation simple et efficace de choix sous la forme d'un tableau.
- Une grande liberté de personnalisation lors de la présentation des choix.

Avenir

Ci-dessous, une liste de plusieurs idées concernant les axes d'amélioration et d'accessibilité.

- La création d'un site Web de référence serait très utile. Le site proposerait tous les choix pour l'analyste qui sélectionne les éléments identifiés lors de son investigation. Un tableau serait alors généré et pourrait être téléchargé par l'analyste.
- La création de pages Web cataloguant toutes les techniques observées selon les APT.
- Une interface plus agréable pour les utilisateurs.

3.4. Le champ de bataille psychologique

Dans le contexte des cyberattaques, un cyberespace de bataille psychologique peut être pensé, ce dernier est constitué de trois grandes composantes : la **psychologie offensive**, la **surface d'attaque psychologique (SAP)** et la **psychologie défensive**. Le SAP est l'ensemble des points psychologiques vulnérables que l'attaquant peut tenter d'exploiter.

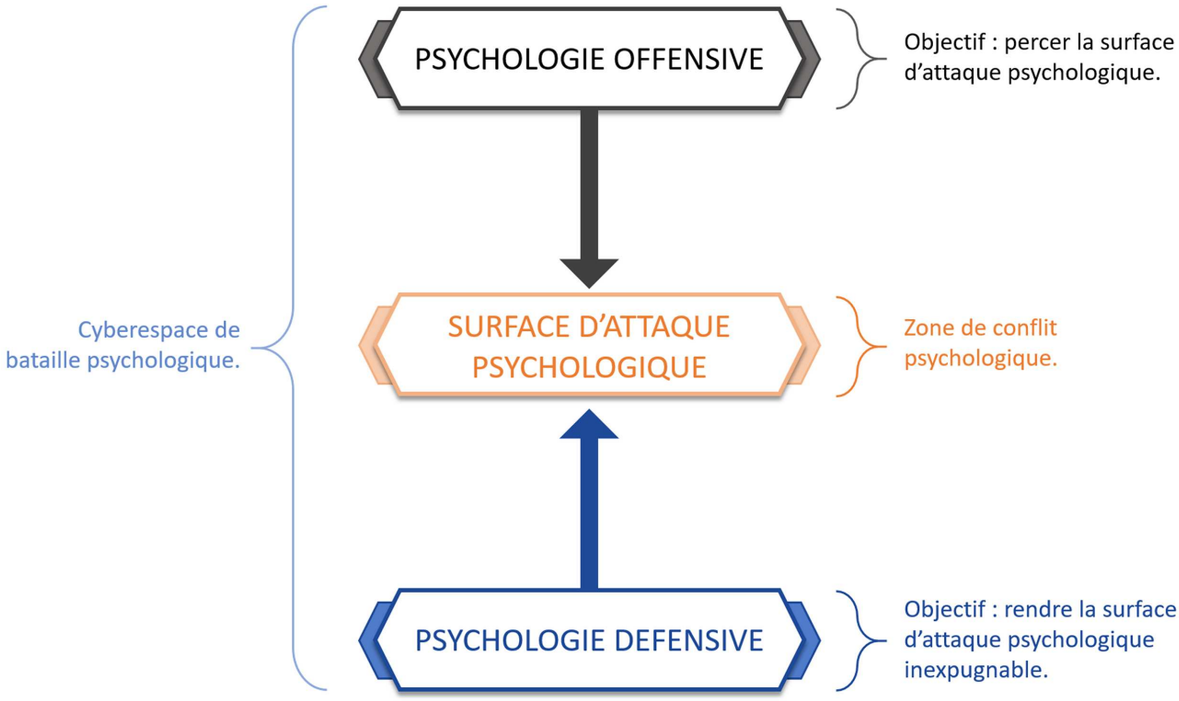


Figure 2. Cyberespace de bataille psychologique.

3.4.1. DECEPTION et SAISA

Pour se protéger, le modèle **SAISA**, en cours de développement, permettrait une protection efficace contre la psychologie offensive.

Composante Attaque	Composante Défense
DECEPTION	SAISA
Le modèle **DECEPTION** permet de cataloguer et d'analyser les tactiques et techniques de manipulation psychologique offensives.	Le modèle **SAISA** permet aux utilisateurs de développer une cyber-résilience psychologique et de contrer les tentatives de manipulation.

3.5. SAISA Se protéger contre la psychologie offensive

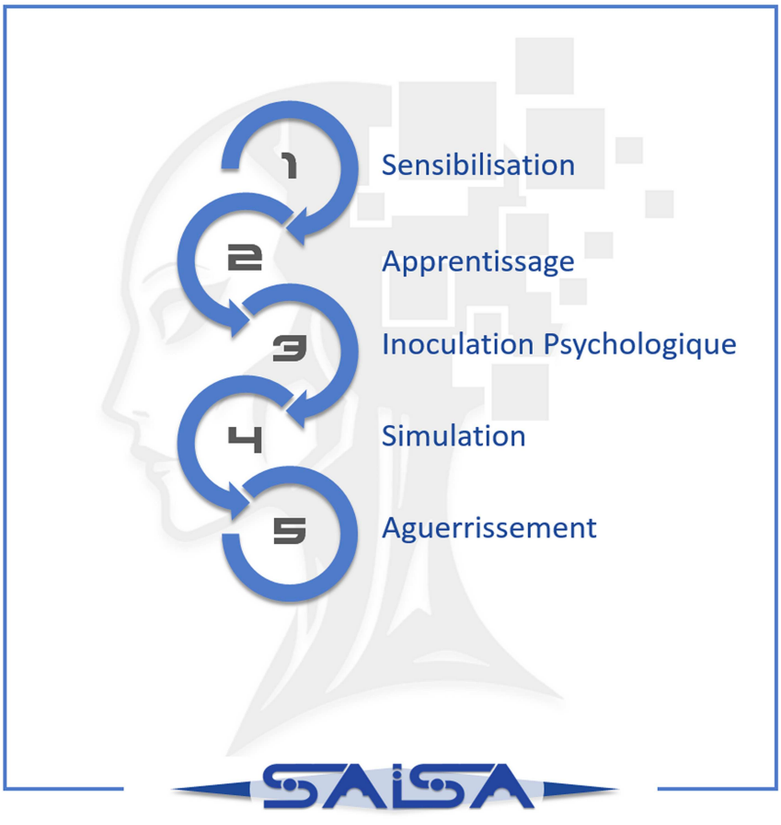
Une réduction optimale de la surface d'attaque psychologique reposerait essentiellement sur le développement de la **cyber-résilience** et de la **psychoprophylaxie** de ses utilisateurs.

- IBM (2025) définit la cyber-résilience comme "un concept qui rassemble la continuité des activités, la sécurité des systèmes d'information et la résilience organisationnelle. Autrement dit, le concept décrit la capacité à continuer à produire les résultats escomptés malgré des cyber-événements compromettants, tels que des cyberattaques, des catastrophes naturelles ou des récessions économiques".

- 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 cyber-résilience, et la cyberpsychoprophylaxie, peuvent être structurés 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**.

Ci-dessous, une infographie du modèle SAISA :



3.6. Conclusion

Cet article a exploré le nouveau modèle **DECEPTION** (version 1.0), une base de connaissances qui permet de cataloguer et d'analyser les tactiques et techniques de manipulation psychologique offensives utilisées par les cybercriminels lors de leurs attaques contre les infrastructures d'entreprise. **DECEPTION** s'articule autour de six grandes tactiques : **reconnaissance**, **ressources**, **initialisation**, **intrusion**, **exploration** et **impact**.

Ces tactiques s'appuient sur un arsenal ciblant la psyché humaine : les techniques de psychologie offensive.

Les rôles respectifs de la psychologie offensive et défensive ont été détaillés. Elles sont en conflit, opposées de manière diamétrale, séparées par une surface d'attaque au sein d'un cyberespace de bataille psychologique.

Face à cette menace psychologique, les développement de la cyber-résilience et de la psychoprophylaxie des utilisateurs sont cruciaux pour limiter la surface d'attaque psychologique. En cours de développement, le modèle **SAISA** propose une approche progressive en cinq échelons, visant à renforcer la résistance et l'adaptation des utilisateurs face à ces agressions.

3.7. Lectures recommandées

La CTI vous recommande la lecture des publications suivantes.

Troll Stealer

Date de publication : Février 2024.

Ce bulletin présente une analyse d'un échantillon du logiciel malveillant Troll Stealer (APT Kimsuky).

SAP

Date de publication : Septembre 2024.

Ce bulletin présente une première version du concept de la Surface d'Attaque Psychologique (SAP).

4. RÉFÉRENCES

Kubernetes - CVE-2025-1974

- https://www.cve.org/CVERecord?id=CVE-2025-1974
- https://github.com/advisories/GHSA-mgvx-rpfc-9mpv
- https://groups.google.com/g/kubernetes-security-announce/c/2qa9DFtN0cQ

Veeam - CVE-2025-23120

- https://www.cve.org/CVERecord?id=CVE-2025-23120
- https://www.veeam.com/kb4724

Ruby SAML - CVE-2025-25291

- https://www.cve.org/CVERecord?id=CVE-2025-25291
- https://github.com/SAML-Toolkits/ruby-saml/security/advisories/GHSA-4vc4-m8qh-g8jm
- https://about.gitlab.com/releases/2025/03/12/patch-release-gitlab-17-9-2-released/
- https://github.com/omniauth/omniauth-saml/security/advisories/GHSA-hw46-3hmr-x9xv
- https://security.netapp.com/advisory/ntap-20250314-0010/

Article : Psychologie Offensive - modèle DECEPTION

- Clinique E-santé. (2024). Love Bombing : 6 signes que vous en êtes victime. *Clinique E-santé*. https://www.la-clinique-e-sante.com/blog/relations-toxiques/love-bombing-signes
- Cyberdise. (2024). Psychology and Phishing Attacks. *Cyberdise*. https://cyberdise-awareness.com/the-psychology-of-phishing-attacks/
- IBM. (20254). Qu'est-ce que la cyber-résilience ?. *IBM*. https://www.ibm.com/fr-fr/topics/cyber-resilience
- Master Card. Cyber's Human Condition. *Master Card*. https://www.mastercard.us/content/dam/public/mastercardcom/na/us/en/large-enterprises/other/cyber-human-condition.pdf
- Psychology Today (Gunther, R.). (2024). Withholding: A Dangerous Saboteur of Love. *Psychology Today*. https://www.psychologytoday.com/us/blog/rediscovering-love/202308/withholding-a-dangerous-saboteur-of-love
- TheRecord (Martin, A.). (2024). LockBit held victims' data even after receiving ransom payments to delete it. *TheRecord*. https://therecord.media/lockbit-lied-about-deleting-exfiltrated-data-after-ransom-payments