PREUVE PORTFOLIO

VEILLE INFORMATIONNELLE
VISHING

Louis
Brunet-Lecomte

SOMMAIRE :

01 INTRODUCTION

02 ACTUALITÉS

03 TECHNIQUES DE VEILLE

04 RECUPERATION DES INFORMATIONS

05 TRAITEMENT DES INFORMATIONS

06 REDISTRIBUTION DES INFORMATIONS

06 ATTAQUE ET SOLUTIONS

INTRODUCTION GÉNÉRALE :

CONTEXTE :

Le **phishing** est l'une des menaces les plus fréquentes et évolutives dans le secteur bancaire. Avec, pour le Vishing une augmentation de 550% de 2021 à aujourd'hui.

FOCUS DE LA VEILLE :

Le Vishing (téléphonique)

LES DIVERS TYPES D'ATTAQUES :

- Spear Phishing
- **Vishing**
- Phishing par e-mail
- Phishing HTTPS
- Pharmaceutique
- Phishing contextuel
- Twin phishing maléfique
- Phishing par trou d'arrosage
- Whaling
- Clone phishing
- Phishing trompeur
- Ingénierie sociale
- Phishing par angler
- Smishing
- ...

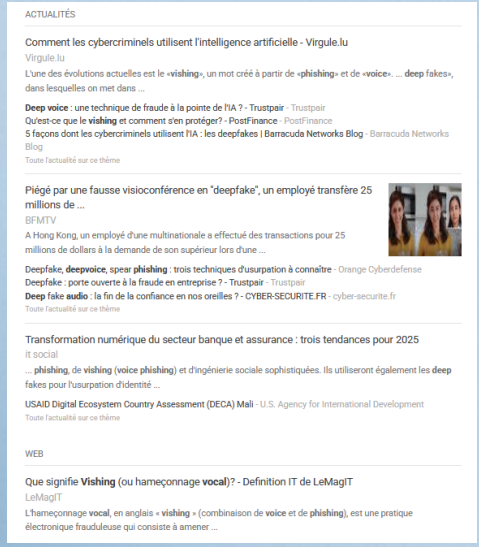
VISHING :

Abréviation de « voice phishing », désigne le moment où quelqu'un utilise moyen de télécommunication pour tenter de voler. L'assaillant peut se faire passer pour un ami ou un parent de confiance ou pour le représenter ainsi que votre conseiller bancaire.

ACTUALITÉS DES 6 DERNIERS MOIS :

Tendances émergentes :

- Multiplication des attaques simulant des appels de banques ou d'organismes gouvernementaux pour résoudre des "problèmes urgents.
- Apparition de techniques utilisant la *deep voice* pour imiter des conseillers bancaires/collègues/clients....



ACTUALITÉS

Comment les cybercriminels utilisent l'intelligence artificielle - Virgule.lu
Virgule.lu
L'une des évolutions actuelles est le «**vishing**», un mot créé à partir de «**phishing**» et de «**voice**». ... **deep** fakes», dans lesquelles on met dans ...

Deep voice : une technique de fraude à la pointe de l'IA ? - Trustpair - Trustpair
Qu'est-ce que le **vishing** et comment s'en protéger? - PostFinance - PostFinance
5 façons dont les cybercriminels utilisent l'IA : les deepfakes | Barracuda Networks Blog - Barracuda Networks Blog
Toute l'actualité sur ce thème

Piégé par une fausse visioconférence en "deepfake", un employé transfère 25 millions de ...
BFMTV
A Hong Kong, un employé d'une multinationale a effectué des transactions pour 25 millions de dollars à la demande de son supérieur lors d'une ...

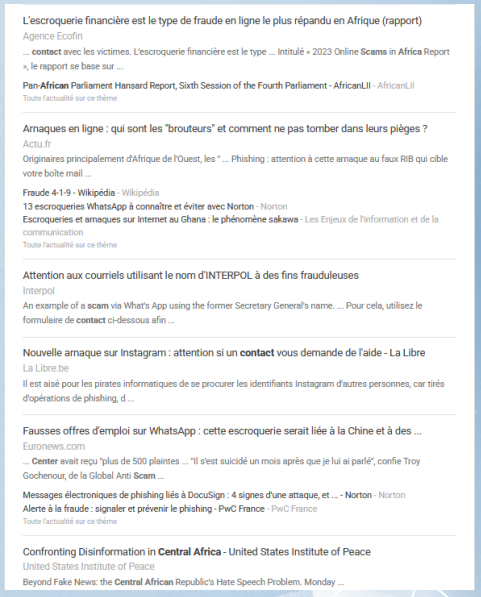
Deepfake, **deepvoice**, spear **phishing** : trois techniques d'usurpation à connaître - Orange Cyberdefense
Deepfake : porte ouverte à la fraude en entreprise ? - Trustpair - Trustpair
Deep fake **audio** : la fin de la confiance en nos oreilles ? - CYBER-SECURITE.FR - cyber-securite.fr
Toute l'actualité sur ce thème

Transformation numérique du secteur banque et assurance : trois tendances pour 2025
it social
... **phishing**, de **vishing** (**voice phishing**) et d'ingénierie sociale sophistiquées. Ils utiliseront également les **deep** fakes pour l'usurpation d'identité ...

USAID Digital Ecosystem Country Assessment (DECA) Mali - U.S. Agency for International Development
Toute l'actualité sur ce thème

WEB

Que signifie **Vishing** (ou hameçonnage **vocal**)? - Definition IT de LeMagIT
LeMagIT
L'hameçonnage **vocal**, en anglais « **vishing** » (combinaison de **voice** et de **phishing**), est une pratique électronique frauduleuse qui consiste à amener ...



L'escroquerie financière est le type de fraude en ligne le plus répandu en Afrique (rapport)
Agence Ecofin
... **contact** avec les victimes. L'escroquerie financière est le type ... Intitulé « 2023 Online **Scams** in **Africa** Report », le rapport se base sur ...

Pan-African Parliament Hansard Report, Sixth Session of the Fourth Parliament - AfricanLII - AfricanLII
Toute l'actualité sur ce thème

Arnaques en ligne : qui sont les "brouteurs" et comment ne pas tomber dans leurs pièges ?
Actu.fr
Originaires principalement d'Afrique de l'Ouest, les " ... Phishing : attention à cette arnaque au faux RIB qui cible votre boîte mail ...

Fraude 4-1-9 - **Wikipédia** - Wikipédia
13 escroqueries WhatsApp à connaître et éviter avec Norton - Norton
Escroqueries et arnaques sur Internet au Ghana : le phénomène sakawa - Les Enjeux de l'information et de la communication
Toute l'actualité sur ce thème

Attention aux courriels utilisant le nom d'INTERPOL à des fins frauduleuses
Interpol
An example of a **scam** via What's App using the former Secretary General's name. ... Pour cela, utilisez le formulaire de **contact** ci-dessous afin ...

Nouvelle arnaque sur Instagram : attention si un **contact** vous demande de l'aide - La Libre
La Libre.be
Il est aisé pour les pirates informatiques de se procurer les identifiants Instagram d'autres personnes, car tirés d'opérations de phishing, d ...

Fausses offres d'emploi sur WhatsApp : cette escroquerie serait liée à la Chine et à des ...
Euronews.com
... **Center** avait reçu "plus de 500 plaintes ... "Il s'est suicidé un mois après que je lui ai parlé", confie Troy Gochenour, de la Global Anti **Scam** ...

Messages électroniques de phishing liés à DocuSign : 4 signes d'une attaque, et ... - **Norton** - Norton
Alerte à la fraude : signaler et prévenir le phishing - PwC France - PwC France
Toute l'actualité sur ce thème

Confronting Disinformation in **Central Africa** - United States Institute of Peace
United States Institute of Peace
Beyond Fake News: the **Central African** Republic's Hate Speech Problem. Monday ...

Zones géographiques actives :

- Centres d'appels frauduleux localisés en Asie du Sud, Europe de l'Est ou Afrique de l'Ouest.

TECHNIQUES DE VEILLE :

Comment me suis-je informé et ait entretenu ma veille au jour le jour ?

SOURCES D'INFORMATIONS PERTINENTES :	• Articles académiques et rapports d'organismes spécialisés comme Fortinet, l'AVC, l'ANSSI, etc. • Suivi des innovations technologiques et des nouvelles techniques d'arnaque via des blogs.
UTILISATION DES MOTS-CLÉS :	• Vishing, phishing vocal, usurpation d'identité bancaire, deep voice, call centers frauduleux.

RÉCUPÉRATION DES INFORMATIONS :

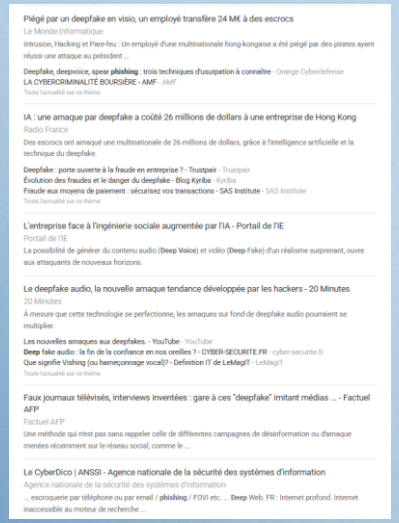
MÉTHODES :

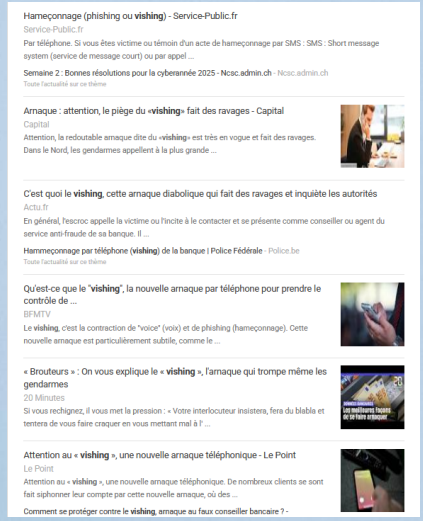
Pull :
Recherche proactive

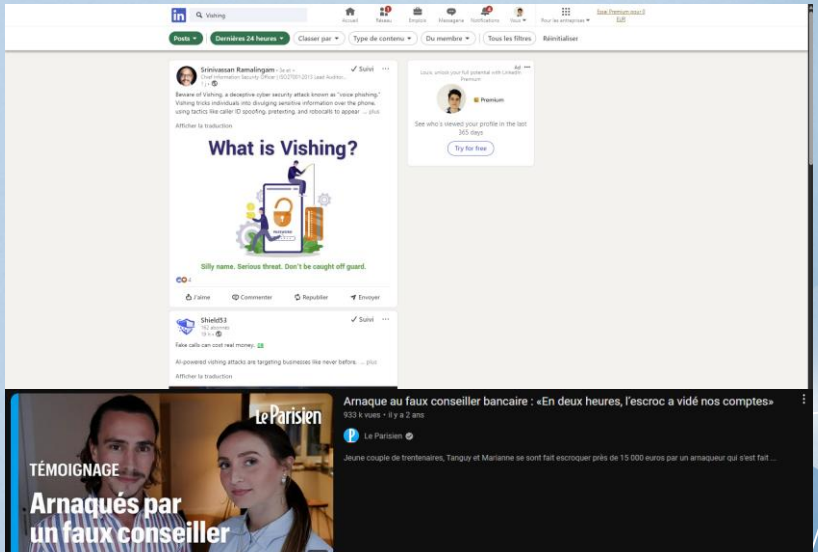
Push :
Alertes Google avec des mots-clés évoqués précédemment.

OUTILS :

LinkedIn pour suivre les experts en cybersécurité.
YouTube pour des démonstrations en temps réel ainsi que pour les témoignages de victimes ainsi que pour des explications diverses.







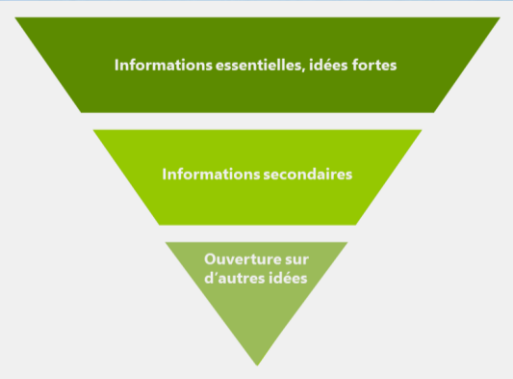
TRAITEMENT DES INFORMATIONS :

Organisation :

- Hiérarchie des informations : Très important, important, peu important.
- Extraction des grandes idées et tri en fonction de l'impact.

Synthèse :

- Création d'une note centrale regroupant les idées clés et les sources pour une vision globale.



REDISTRIBUTION DES INFORMATIONS :

EN ENTREPRISE :	• Mise à disposition sur un wiki interne pour que les équipes partagent et consultent les informations. • Formation des nouvelles recrues avec des cas pratiques.
PERSONNELLEMENT :	• Synthèse des résultats sous forme de post LinkedIn pour vulgariser et partager avec un public plus large.
PRÉVENTION :	• Campagnes éducatives pour aider les clients à identifier les scams. • Outils techniques : mise en place de solutions d'authentification renforcées.

L'ATTAQUE CONTRE MGM RESORTS PAR LE GROUPE SCATTERED SPIDER :

CONTEXTE :

- MGM RESORTS est une chaîne de casinos et d'hôtels
- Cyberattaque majeure ayant perturbé ses systèmes pendant plusieurs jours
- Met en évidence l'efficacité redoutable du Vishing
- Scattered Spider (groupe cybercriminel)

MGM RESORTS INTERNATIONAL™

DÉROULEMENT DE L'ATTAQUE :

Collecte d'informations :
- Utilisation de données accessibles publiquement (LinkedIn, réseaux sociaux)
- Objectif : Identifier les employés cibles et recueillir des informations exploitables.

Amorce de l'attaque par Vishing :
- Contact avec le support informatique de MGM Resorts (DeepVoice) via TEAMS. Les attaquants ont utilisé un ton autoritaire et une connaissance précise des processus internes pour manipuler les agents du support technique.
- Usurpation d'identité d'un technicien réseau étant en déplacement // Demande de réinitialisation du MFA de MGM

Objectif de cette phase :
Obtenir un accès initial au réseau interne de l'entreprise avec un compte Administrateur et exploiter le manque de formation du Support Informatique.

L'ATTAQUE :

LE BLACK-CAT

Déplacement latéral :
Identification des serveurs critiques (données sensibles, systèmes de gestion).

Déploiement du ransomware ALPHV/BlackCat :
Modèle Ransomware-as-a-Service (RaaS).
Permet d'utiliser le ransomware moyennant un partage des rançons.

Objectif :
Chiffrer les données critiques. Rendre les systèmes inopérants (Pendant plus de dix jours, les opérations de MGM ont été gravement perturbées : clés numériques, machines a sous, système de facturation...).

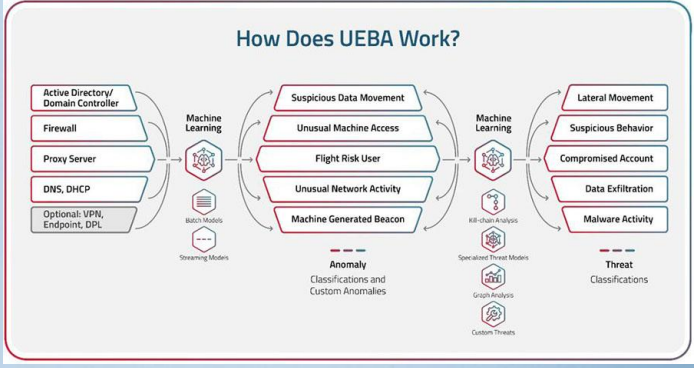
Types de données volées : Noms, adresses, dates de naissance. Numéros de permis de conduire, passeports, numéros de sécurité sociale.

EVITER LE VISHING :

Enseignements et préconisations :

- Renforcer la vérification d'identité :
Protocoles stricts de vérification pour valider l'identité des appelants, comme des questions de sécurité ou des jetons d'authentification temporaires en plus du **MFA**.

- Formation à l'ingénierie sociale :
Les employés doivent être régulièrement formés aux **techniques de manipulations** courantes, notamment le vishing.



- Surveillance des systèmes :
Implémenter un **UEBA** (User and Entity Behavior Analytics).
Définir des modèles d'anomalies en configurant des règles ou laissant l'outil apprendre les comportements habituels grâce au **Machine Learning**.
(50 commandes en moins d'1 minute / Moyenne 50 commandes = 1h)

- Protéger son réseau :
Limiter les mouvements latéraux des attaquants en cloisonnant les systèmes critiques et les données sensibles (DMZ, Vlans, Tiering, ...)

MERCI POUR VOTRE ECOUTE

Avez-vous des questions ?