Anatomie d'une Attaque Phishing

LBIEN Bilal

Table des Matières

01

Le Phishing

Le Phishing, une Menace Réelle

Définition : "Une technique de cyberattaque qui utilise la **ruse** et l'**ingénierie sociale** pour tromper les individus et les inciter à révéler des informations confidentielles (mots de passe, numéros de carte, secrets d'entreprise).«

Statistiques Clés :

- ↦ **4.45 Millions USD :** Coût moyen mondial d'une violation de données en 2023 (souvent initiée par un phishing). *(Source : IBM, "Cost of a Data Breach Report 2023")*
- ↦ **80%** des entreprises ont subi au moins une attaque de phishing réussie en 2023. *(Source : Proofpoint, "State of the Phish Report 2024")*

80%

des entreprises ont subi au moins une attaque de phishing réussie en 2023.

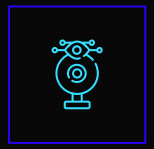
4.45 Millions USD

Coût moyen mondial d'une violation de données en 2023

Les Visages du Phishing

Phishing de Masse

Envoi large et non ciblé. (Ex: Faux email Netflix, La Poste).



Spear Phishing

Attaque ciblée sur une personne ou un groupe. (Ex: Faux email du service IT de *votre* entreprise).

Whaling

Spear phishing qui cible les "gros poissons" : PDG, Directeurs Financiers.

Vishing / Smishing

Phishing par téléphone (Voice) ou par SMS. (Ex: "Votre colis est bloqué, cliquez ici").

02

L'Ingénierie Sociale

L'Arme Psychologique (Ingénierie Sociale)

Statistique : 74% de toutes les violations de données impliquent "l'élément humain" (phishing, erreur, ruse...). *(Source : Verizon, "2023 DBIR")*

Les 4 Leviers Psychologiques (Les "Appâts") :

- ↦ **L'URGENCE :** "Votre compte sera suspendu dans 24h !"
- ↦ **LA PEUR :** "Une connexion suspecte a été détectée."
- ↦ **L'AUTORITÉ :** "Demande urgente du PDG" / "Convocation de la police".
- ↦ **L'APPÂT DU GAIN :** "Vous avez gagné un iPhone" / "Cliquez pour recevoir votre prime".

03

Le Plan d'Attaque

Le "Plan de Bataille" de l'Attaquant

1. Reconnaissance : (Qui cibler ? Quelle page imiter ?)

2. Armement : (Cloner le site web, configurer le serveur [Mention : Kali Linux / SET])

3. Livraison : (Envoi de l'e-mail de phishing à la victime)

4. Exploitation : (La victime clique sur le lien et entre ses identifiants)

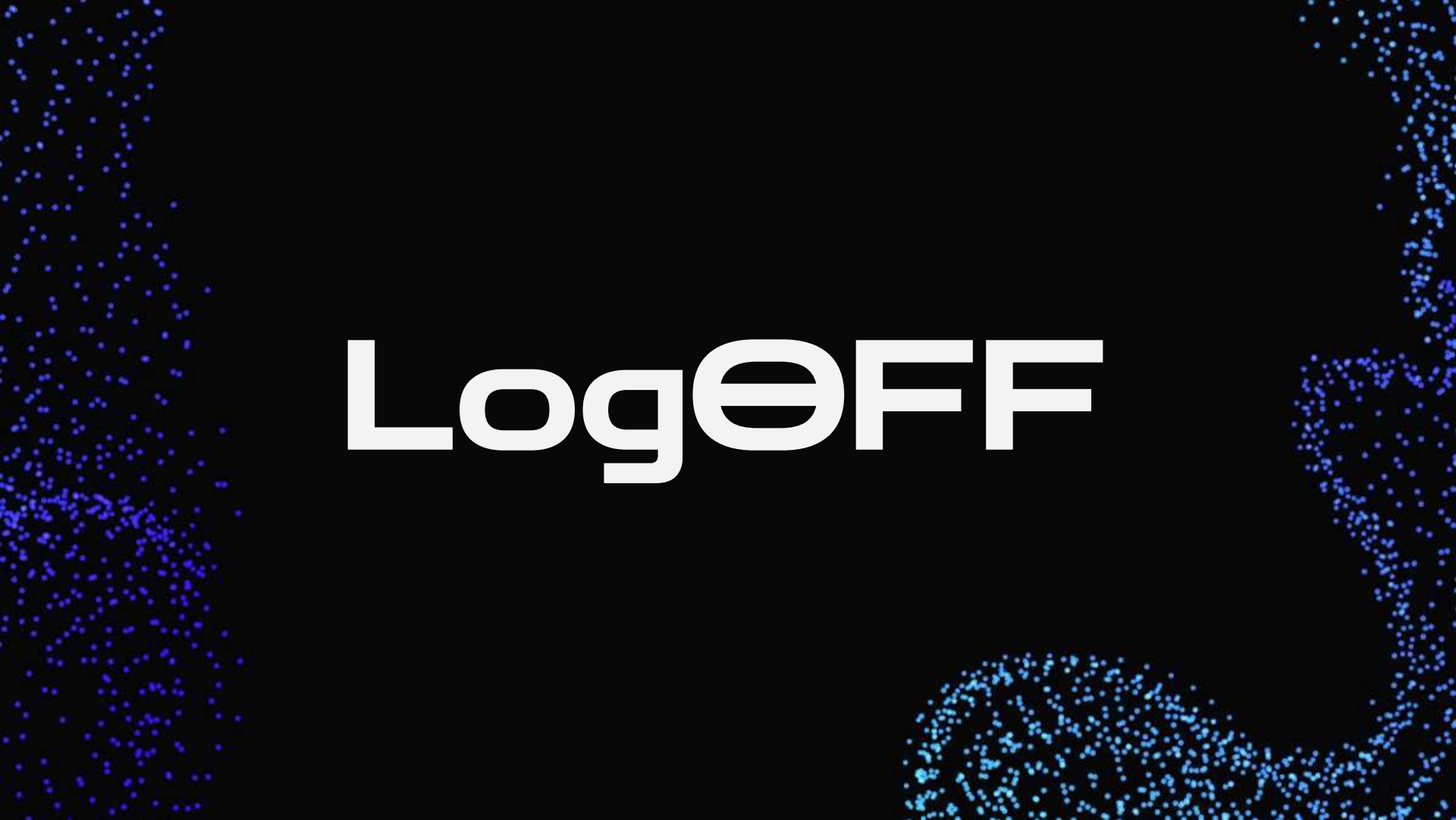
5. Post-Exploitation : (L'attaquant **capture** les identifiants et les utilise)

Démonstration Live

Ø4

La Défense

1. **L'EXPÉDITEUR :** L'adresse email est-elle étrange ? (microsOft.com avec un zéro ?).
2. **L'URL (LE SURVOL) :** Le réflexe N°1. Survolez toujours le lien sans cliquer.
3. **LE TON** : Y a-t-il un sentiment d'Urgence, de Peur, ou une Promesse ?
4. **LES FAUTES :** Fautes d'orthographe, de grammaire, ou une mise en page bâclée.
5. **LA DEMANDE :** Une demande inhabituelle ? (On ne vous demandera JAMAIS votre mot de passe).
6. **LES PIÈCES JOINTES :** Une facture .html, .zip ou .exe inattendue ? N'ouvrez jamais.
7. **LE CONTEXTE :** Est-ce que j'attendais cet email ? Est-ce logique ?
8. **LE MFA (2FA) :** Activez l'Authentification Multi-Facteurs. Elle bloque 99,9% des attaques, même si le pirate a votre mot de passe. (Source : Microsoft)


LogOFF