

---

# ARP Attacks

## arp-sk en action

---

**Frédéric Raynal** <pappy@miscmag.com>

**Cédric Blancher** <blancher@cartel-securite.fr>

—

**15 novembre 2002**

- Introduction

Présentation de ARP et attaques classiques

- arp-sk

Présentation de l'outil

- Corruption de cache ARP

Utilisation de arp-sk pour différentes attaques à partir de corruption de cache ARP en utilisant arp-sk.

## Introduction : le protocole ARP (1/2)

0	7	15	23	31
ident. adresse physique		ident. adresse logique		
lg @ physique	lg @ logique	code		
adresse physique ...				
... de l'émetteur		adresse logique ...		
... de l'émetteur		adresse physique ...		
... du récepteur (inconnue)				
adresse logique du récepteur				

## Introduction : le protocole ARP (2/2)

- ➔ ARP (Address Resolution Protocol - RFC 826)
  - lier adresses niveau 2 (Ethernet) et niveau 3 (IP)
  - client envoie en broadcast niveau 2 une requête (who-has)
  - destinataire répond en unicast niveau 2 (reply)
- ➔ Utilisation d'un cache
- ➔ Aucun lien entre information niveau 2 et niveau 3

## Attaques : MAC Spoofing

- spoofer l'adresse Ethernet source de la trame Ethernet
- vise le « cache » des switches (adresses niveau 2)

### ➔ Avantage

- ▶ récupération et redirection de trafic

### ➔ Inconvénients

- ▶ la cible ne reçoit plus de paquet mais continue à en émettre
- ▶ conflits dans les « cache »
- ▶ pas discret du tout

## Attaques : ARP Spoofing

- who-has émis en broadcast
- répondre au lieu du vrai destinataire avec de fausses données

### ➔ Avantages

- ▶ récupération et redirection de trafic
- ▶ pas besoin de s'occuper des switches

### ➔ Inconvénient

- ▶ issue incertaine en fonction de qui répond en premier

## Attaques : ARP cache poisoning (1/2)

- créer/modifier les entrées du cache de la victime
- trafic émis par la cible directement vers l'attaquant

### ➔ Créer une entrée

- ▶ messages who-has en unicast autorisés par la RFC
- ▶ envoie en unicast d'un who-has avec de fausses données

### ➔ Modifier une entrée

- ▶ ARP spoofing : envoie d'un reply avec de fausses données

## Attaques : ARP cache poisoning (2/2)

### ➔ Avantages

- ▶ récupération et redirection de trafic
- ▶ rarement surveillé

### ➔ Inconvénient

- ▶ très difficile à contrer



- Introduction

Présentation de ARP et attaques classiques

- arp-sk

Présentation de l'outil

- Corruption de cache ARP

Utilisation de arp-sk pour différentes attaques à partir de corruption de cache ARP en utilisant arp-sk.

## Présentation de arp-sk (1/2)

- ➔ Pourquoi un nouvel outil ?
  - ▶ rassembler les fonctionnalités de plusieurs outils (arp spoof, macof, arping ...)
  - ▶ manipulation de **tous** les champs d'un paquet ARP (niveau Ethernet **et** ARP)
  - ▶ ajout de nouvelles fonctionnalités (cartographie, détection du mode promiscuous, ...)
  
- ➔ Structure de arp-sk (à partir de la version 0.99.0)
  - ▶ une bibliothèque contenant les fonctions de base
  - ▶ un binaire arp-sk
  - ▶ des modules (bib. dynamiques) décrivant des « scénarii » (un module == une fonctionnalité)

## Présentation de arp-sk (2/2)

### ➔ Options de arp-sk

- ▶ classiques : fréquence d'émission (en s,  $\mu$ s ou aléatoire), nombre de paquets, interface ...
- ▶ module basic : type de paquet (-w, -r), adresses Ethernet (-s, -d), adresses dans le message ARP (-S, -D - [IP][:MAC]), génération aléatoire des adresses (Eth et ARP, -rand\*)

### ➔ TODO

- ▶ ajout de nouveaux modules
- ▶ portage vers d'autres OS (OpenBSD et Solaris en particulier)
- ▶ création d'une bibliothèque pour construire des « scénarii réseau »

- Introduction

  - Présentation de ARP et attaques classiques

- arp-sk

  - Présentation de l'outil

    - Corruption de cache ARP

      - Utilisation de arp-sk pour différentes attaques à partir de corruption de cache ARP en utilisant arp-sk.

## Mise à jour du cache ARP

- ▶ Comportement opportuniste
- ▶ Ajout d'entrée
- ▶ Modification d'entrée
- ▶ Suppression d'entrée
- ➔ À l'attaque...

Paramètres sur lesquels on peut jouer :

- ▶ Ethernet : adresse MAC source
- ▶ Ethernet : adresse MAC destination
- ▶ ARP : source niv. 2
- ▶ ARP : destination niv. 2
- ▶ ARP : source niv. 3
- ▶ ARP : destination niv. 3

## Création d'entrées

- ▶ Requête ARP
- ▶ Réponse ARP (dépend de l'OS et du cache)
- ▶ Gratuitous ARP
- ➡ Pas forcément très utile

## Mise à jour d'entrée

- ▶ Requête ARP
  - ▶ Réponse ARP
  - ▶ Gratuitous ARP
- ➔ Les machines intéressantes (DNS, GW, etc...) sont souvent dans le cache



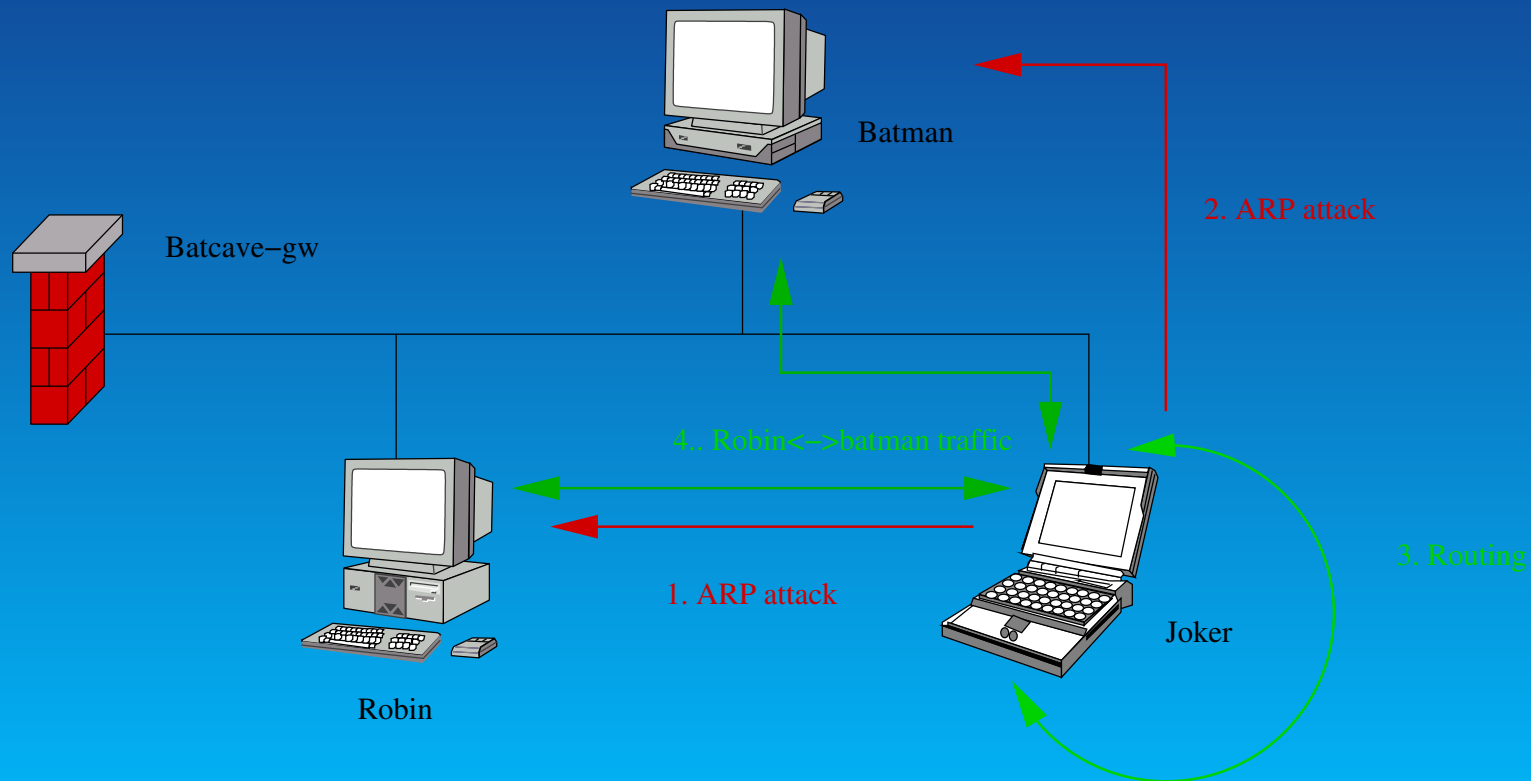
## Suppression d'entrée

- ▶ Expiration de l'entrée
- ▶ Taille limitée du cache (500 entrées environ sous Linux)
- ➔ On flood le cache, mais ce n'est pas vraiment utile...

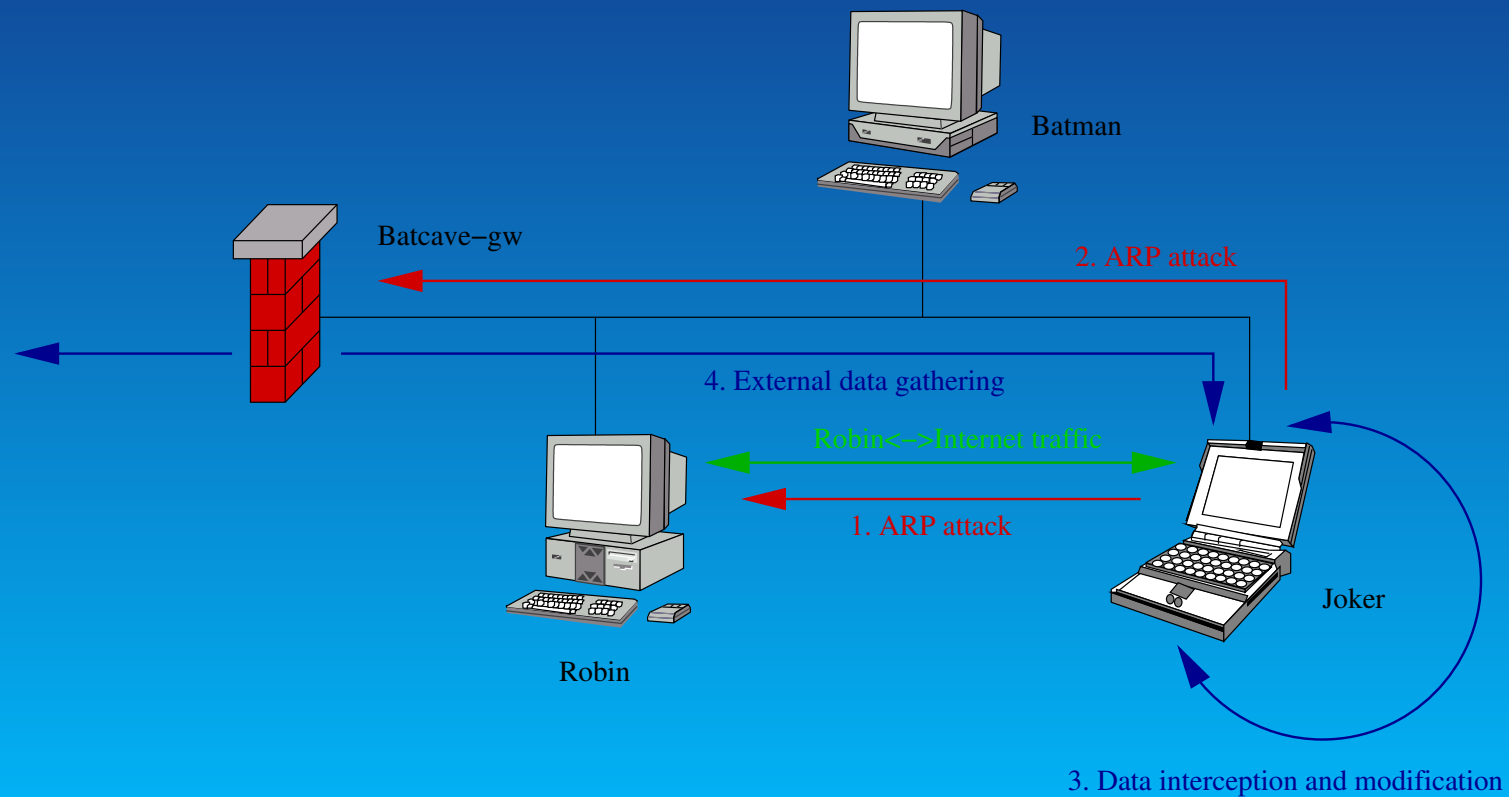
## Les applications de la corruption de cache ARP...

- ▶ Écoute : on peut lire le contenu des flux détournés en mode normal
- ▶ Interception : on peut se placer comme proxy transparent
- ▶ Modification : on peut injecter des données dans les flux
- ▶ Vol : on peut prendre la place d'une des deux parties
- ▶ Déchiffrement : attaque MiM
- ▶ Usurpation : on peut aisément falsifier son IP
- ▶ DoS : destruction de flux réseau

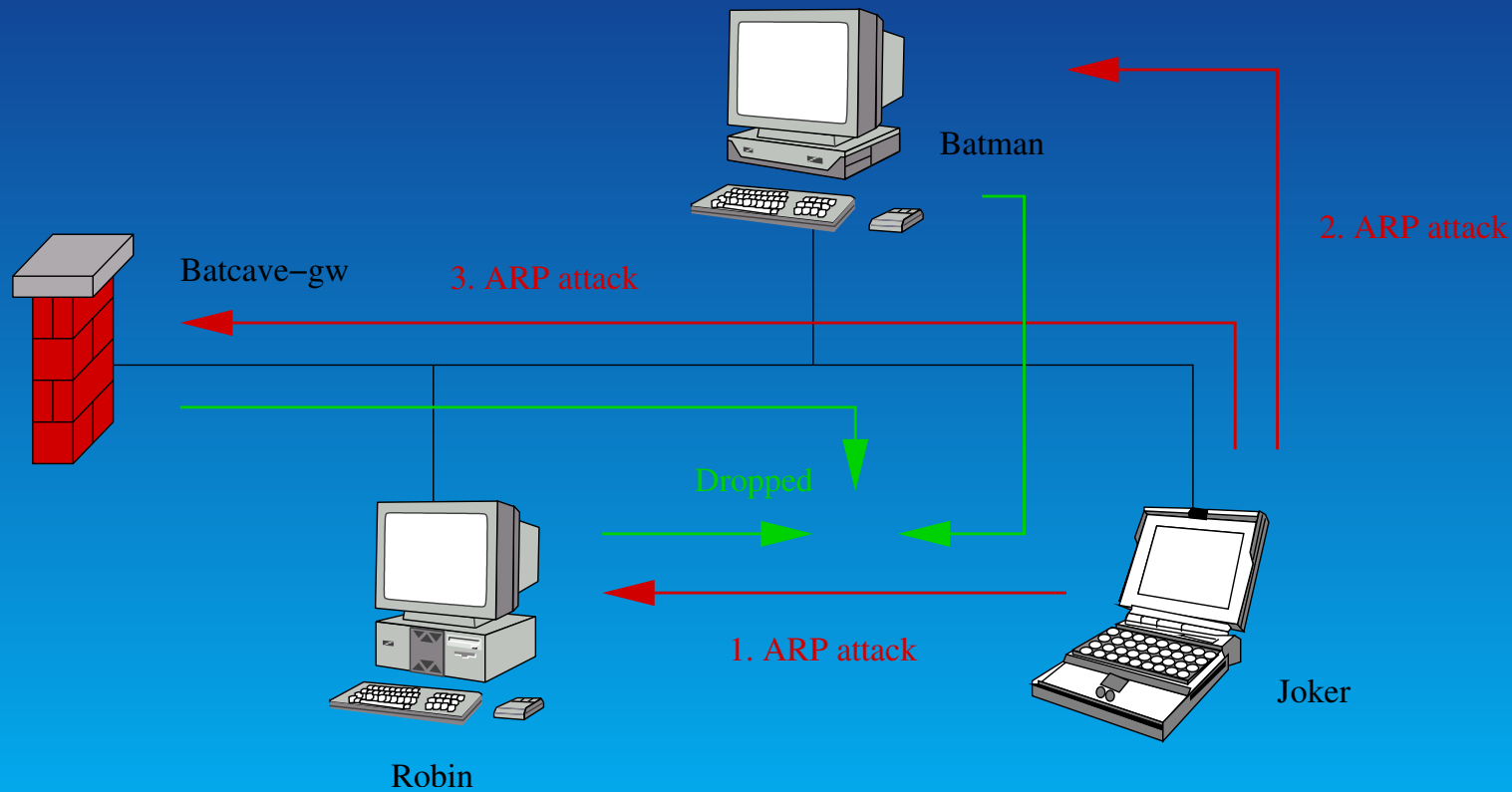
## MiM ARP pour écouter les flux



## Proxying transparent pour modifier et voler des flux

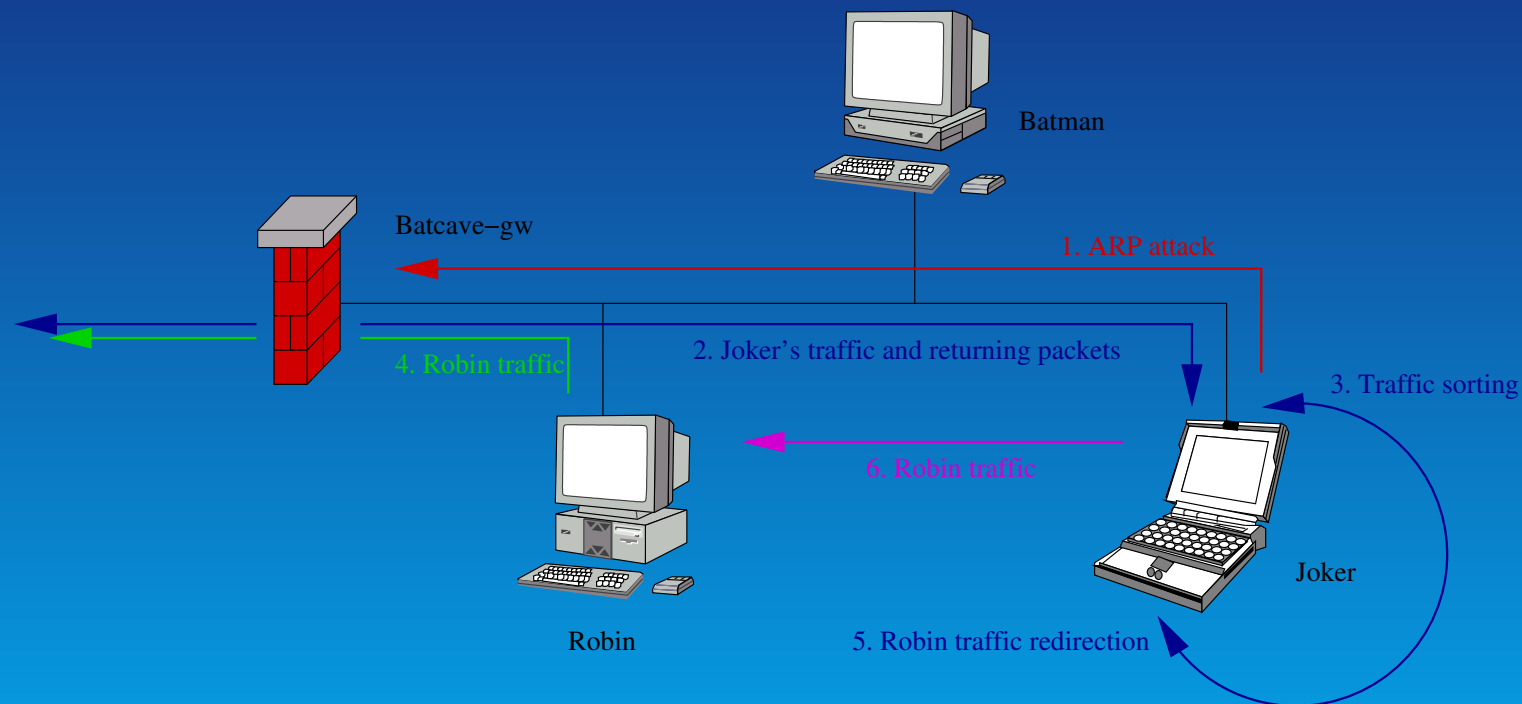


## DoS



➡ Les machines attaquées vont vérifier leurs entrées...

## “Smart IP spoofing”



➔ On peut aussi utiliser du MiM ;)

➔ <http://www.althes.fr/ressources/avis/smartspoofing.htm>

## Conséquence

- ➔ Une fois que l'attaquant est root, c'est tout le segment ethernet qui est perdu !

ARP est un protocole faible et facile à détourner : la sécurité n'était pas le but. On a besoin de quelque chose de plus solide pour authentifier les stations :

- ▶ 802.1x

- ▶ Secure Link Layer

[http://www.cs.wustl.edu/~fhunleth/projects/sll/sll\\_report.pdf](http://www.cs.wustl.edu/~fhunleth/projects/sll/sll_report.pdf)

- ▶ Authentification applicative

Il est clair que les switches ne sont pas des outils de sécurité.



<PUB>



- ➔ MISC : magazine français, spécialisé en sécurité informatique
- ➔ <http://www.miscmag.com/>

</PUB>

- ▶ Éric Detoisien pour winarp-sk and winarp-mim sur Win32
- ▶ Laurent Licour et Vincent Royer pour leurs tests