# Where are you taking me? Understanding abusive Traffic Distribution Systems

**Janos Szurdi**[1,3], Meng Luo[2], Brian Kondracki[2],

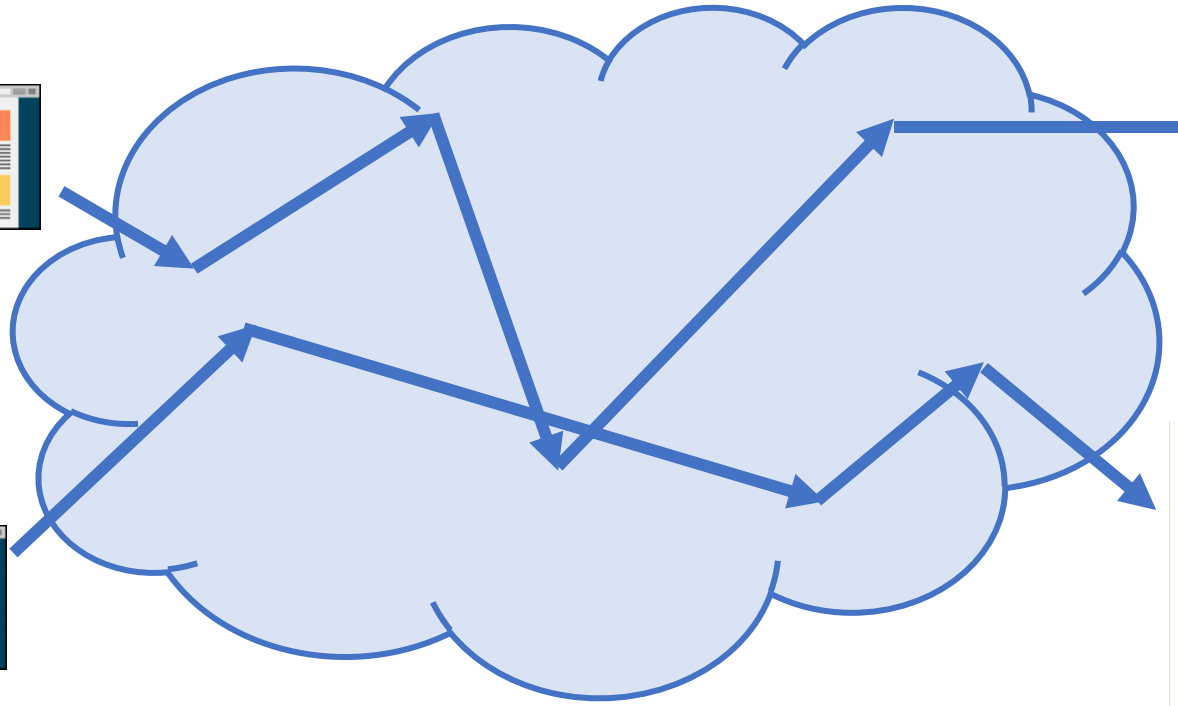
Nick Nikiforakis[2] and Nicolas Christin[1]

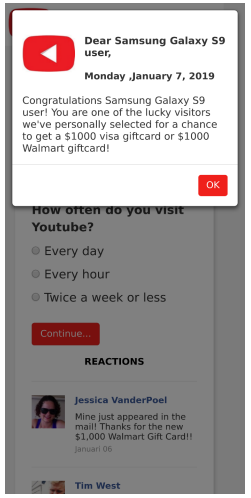
[1]Carnegie Mellon University [2]Stony Brook University

[3]Palo Alto Networks

# Motivation

Would love to watch Titanic for free






You won a $1000 gift card

Let me visit youtuge.com

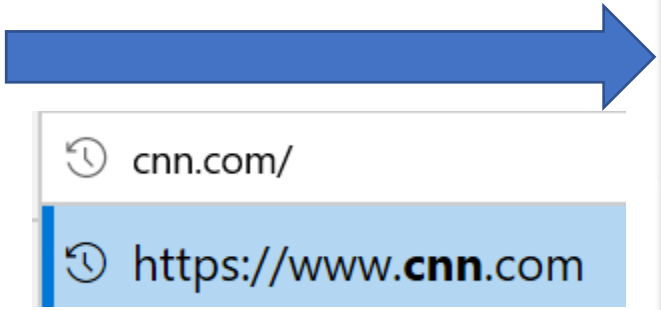

Your Flash Player is outdated

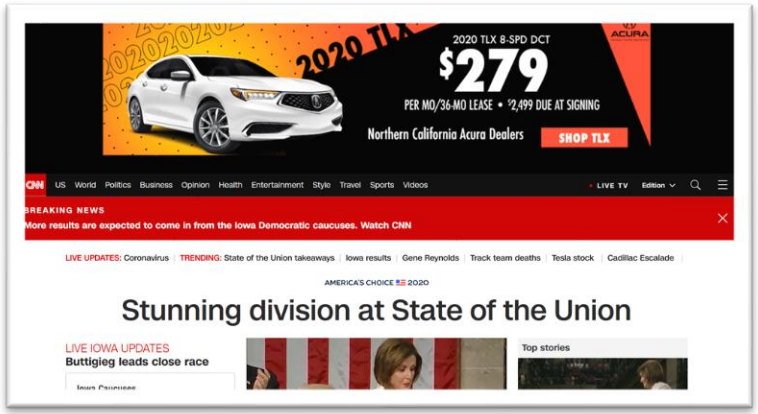
## Traffic Distribution Systems

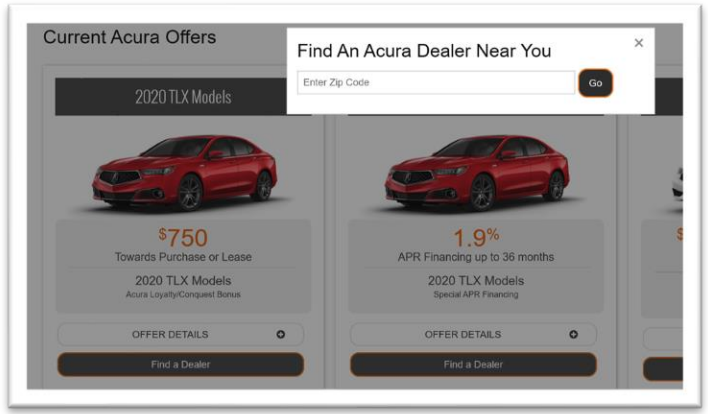
# Traffic Monetization

## Pay-Per-Click:

1. User types
2. User Clicks
3. User Redirected

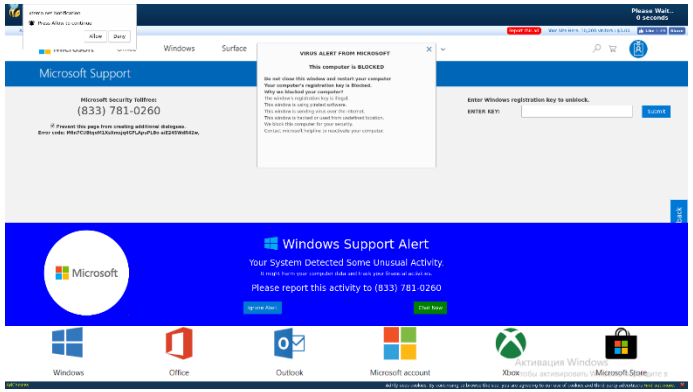



## Pay-Per-Redirect:

1. User types
2. User Automatically Redirected

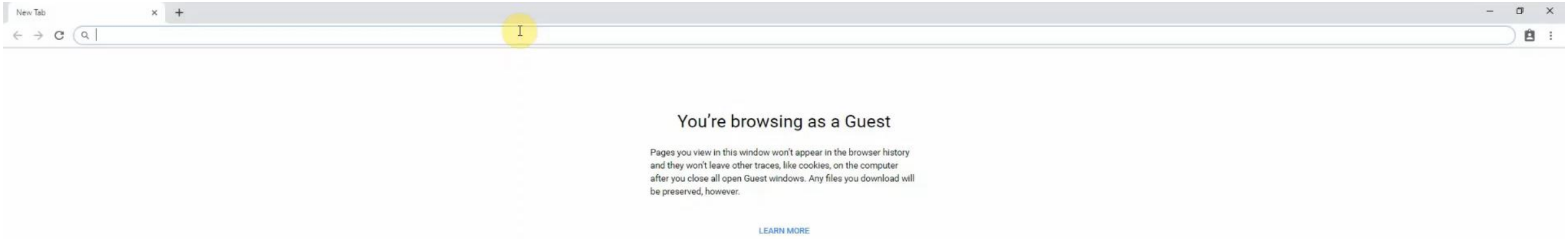




**Traffic Source**

**Traffic Brokers**

**Destination page**

# Typo: steampowerTed.com



# Three Questions

1. Cooperation between different illicit traffic sources

2. User Differentiation

3. Cloaking and blocking
   - Cloaking: hiding malicious content from security researchers

# Measurement in an Adversarial Setting

**Goal of Adversary:** send users to malicious landing pages while hiding from security researchers to maximize profit

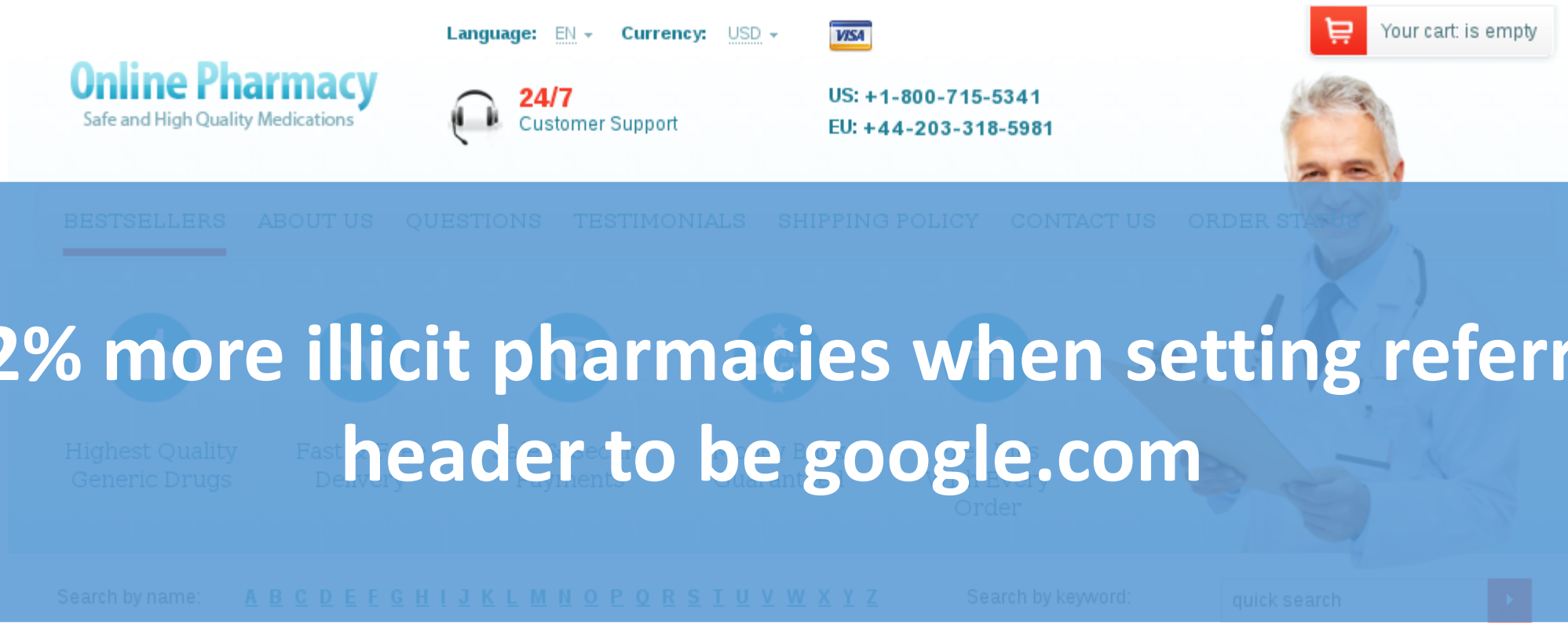
**Example methods:**

- **IP Reputation:** cloak when visit is from a datacenter IP
- **IP Rate limiting:** cloak if too many requests from same IP
- **Header based:** show malicious content only to users coming from a Google search
- **Basic bot detection:** do not show malicious content if bot is detected
  - E.g., can handle cookies and JavaScript

# Cloaking: Blackhat SEO

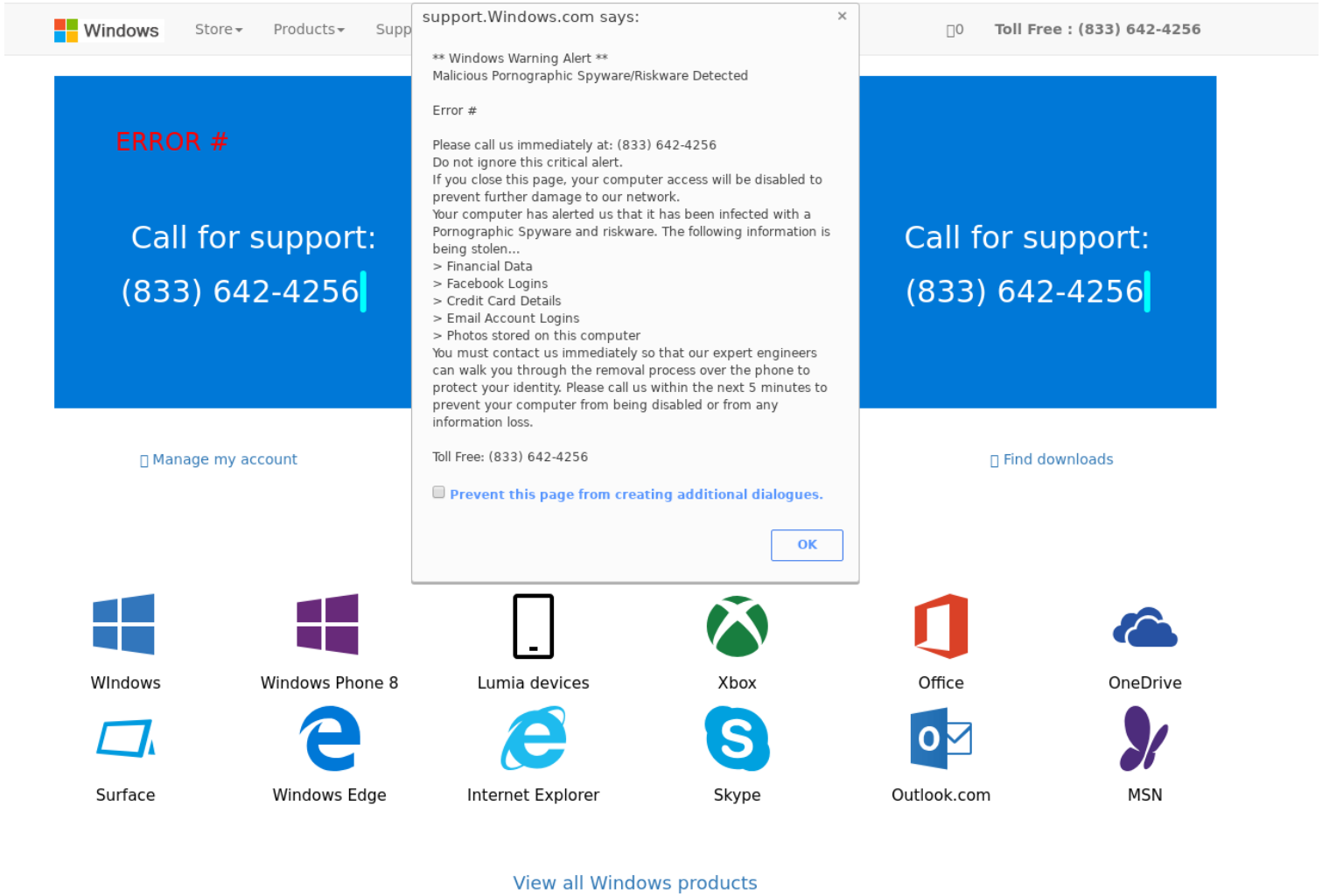
# Cloaking: Blackhat Search Engine Optimization

# Cloaking: Blackhat SEO

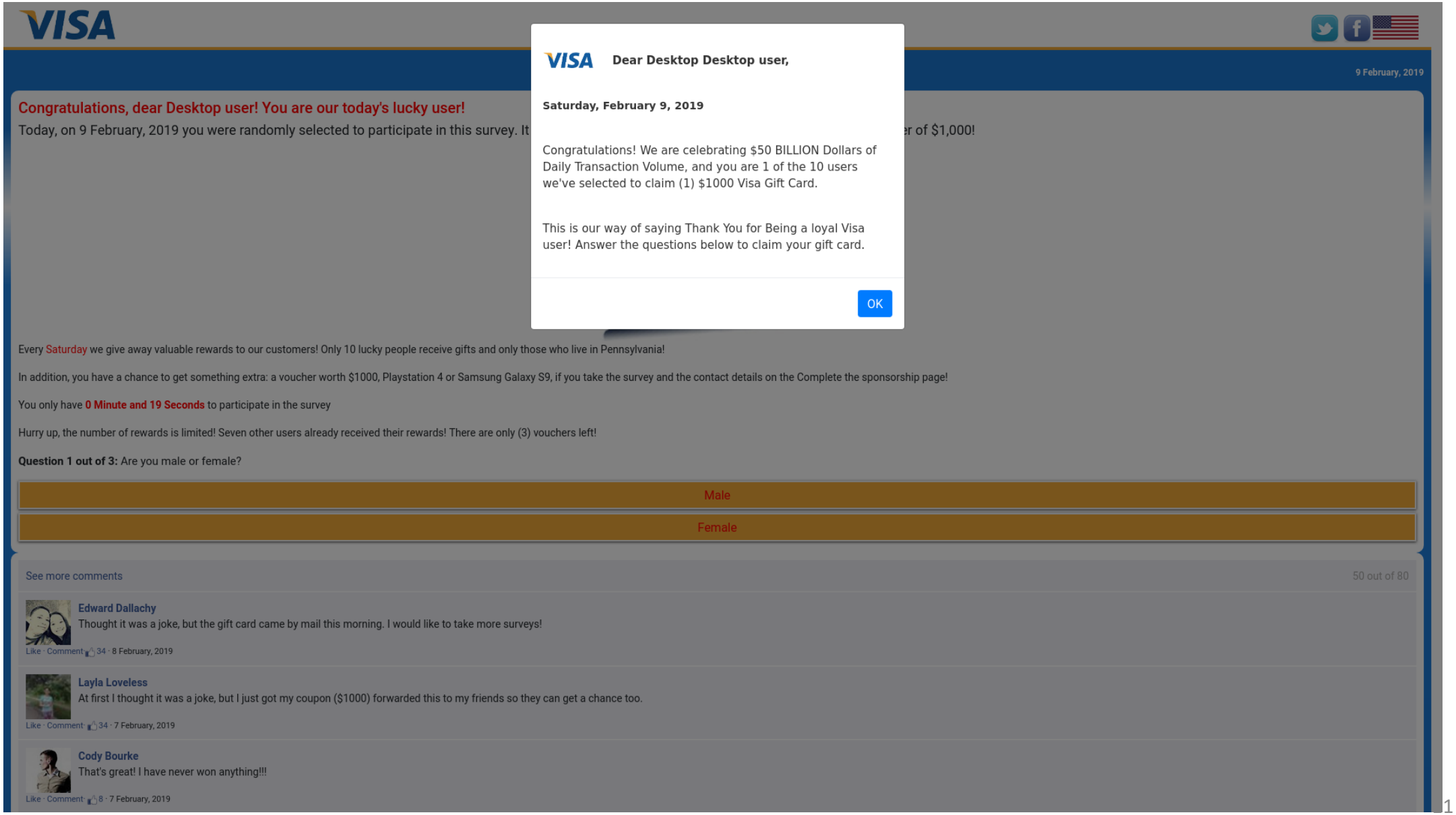



**252% more illicit pharmacies when setting referrer header to be google.com**

# Cloaking: IP Based



# Cloaking: IP Based



# Cloaking: IP Based

realtor.com Buy Sell Rent Mortgage Find Realtors® My Home News & Insights Log In Sign Up Advertise

Pittsburgh, PA × Price Bed Bath Property Type More Filters Save Search View Map

## Pittsburgh, PA Apartments and Homes for Rent

1,314 Rentals

Sort by Freshest Listings

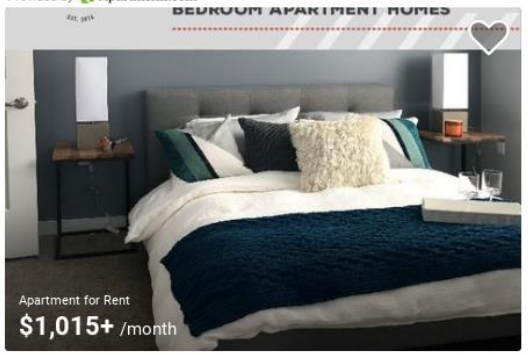
Including apartment communities from Apartments.com

Provided by Apartments.com


Apartment for Rent
**$720+** /month

**0 - 2** bed **1 - 2** bath **300+** sqft
Franklin West Apartments, Leasing Office 272 Shady Ave, Pittsbur...

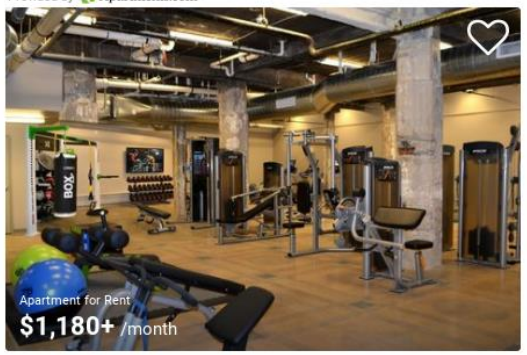
Provided by Apartments.com



Apartment for Rent
**$1,015+** /month

**0 - 3** bed **1 - 2** bath **345+** sqft
Arsenal 201 3922 Foster St, Pittsburgh, PA 15201

Provided by Apartments.com



Apartment for Rent
**$1,180+** /month

**1 - 2** bed **1 - 2** bath **308+** sqft
950 NORTHSHORE 950 Progress St, Pittsburgh, PA 15212

Advertisement

Should You Rent or Should You Buy?

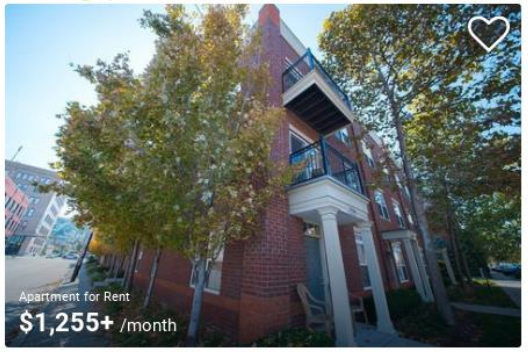
Find Out

Provided by Apartments.com

Apartment for Rent
**$885+** /month

**0 - 2** bed **1 - 2** bath **415+** sqft
Park View Apartments 10 Allegheny Ctr, Pittsburgh, PA 15212

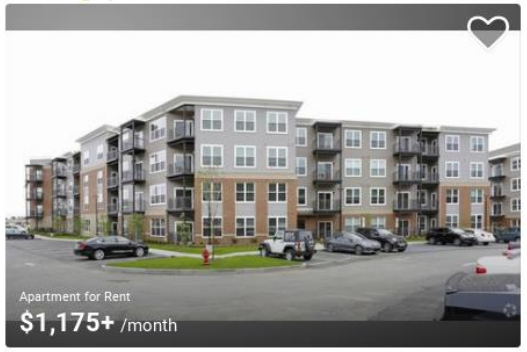
Provided by Apartments.com



Apartment for Rent
**$1,255+** /month

**1 - 2** bed **1 - 2** bath **575+** sqft
Carson Street Commons 2525-2539 E Carson St, Pittsburgh, PA 1...

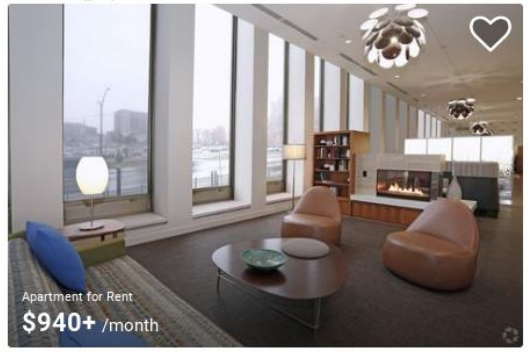
Provided by Apartments.com



Apartment for Rent
**$1,175+** /month

**1 - 3** bed **1 - 2** bath **616+** sqft
The Ashby at South Hills Village Station 1100 Village Dr, Pittsburg...

Provided by Apartments.com



Apartment for Rent
**$940+** /month

**0 - 2** bed **1 - 2** bath **460+** sqft
City View 1420 Centre Ave, Pittsburgh, PA 15219

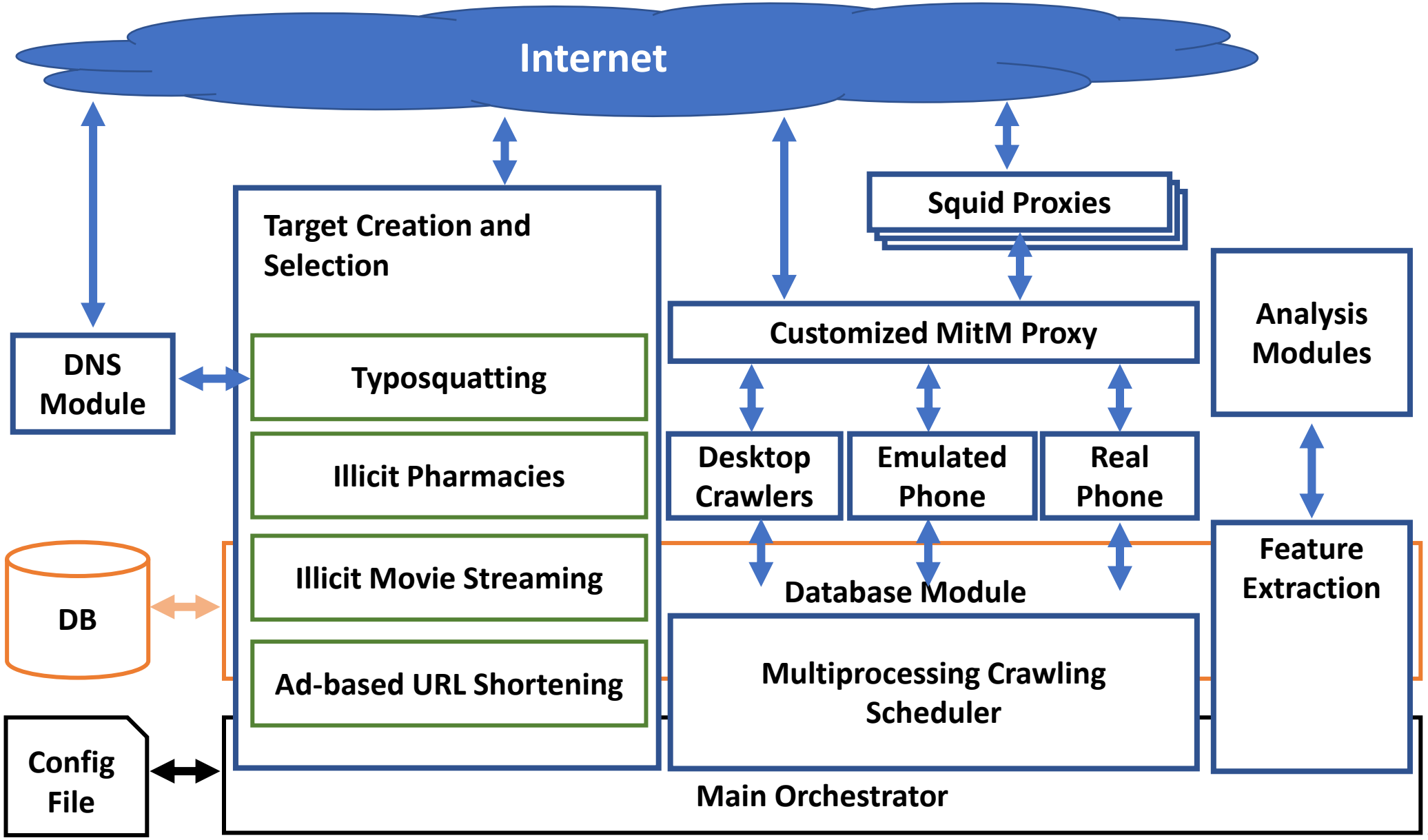
Provided by Apartments.com

Provided by Apartments.com

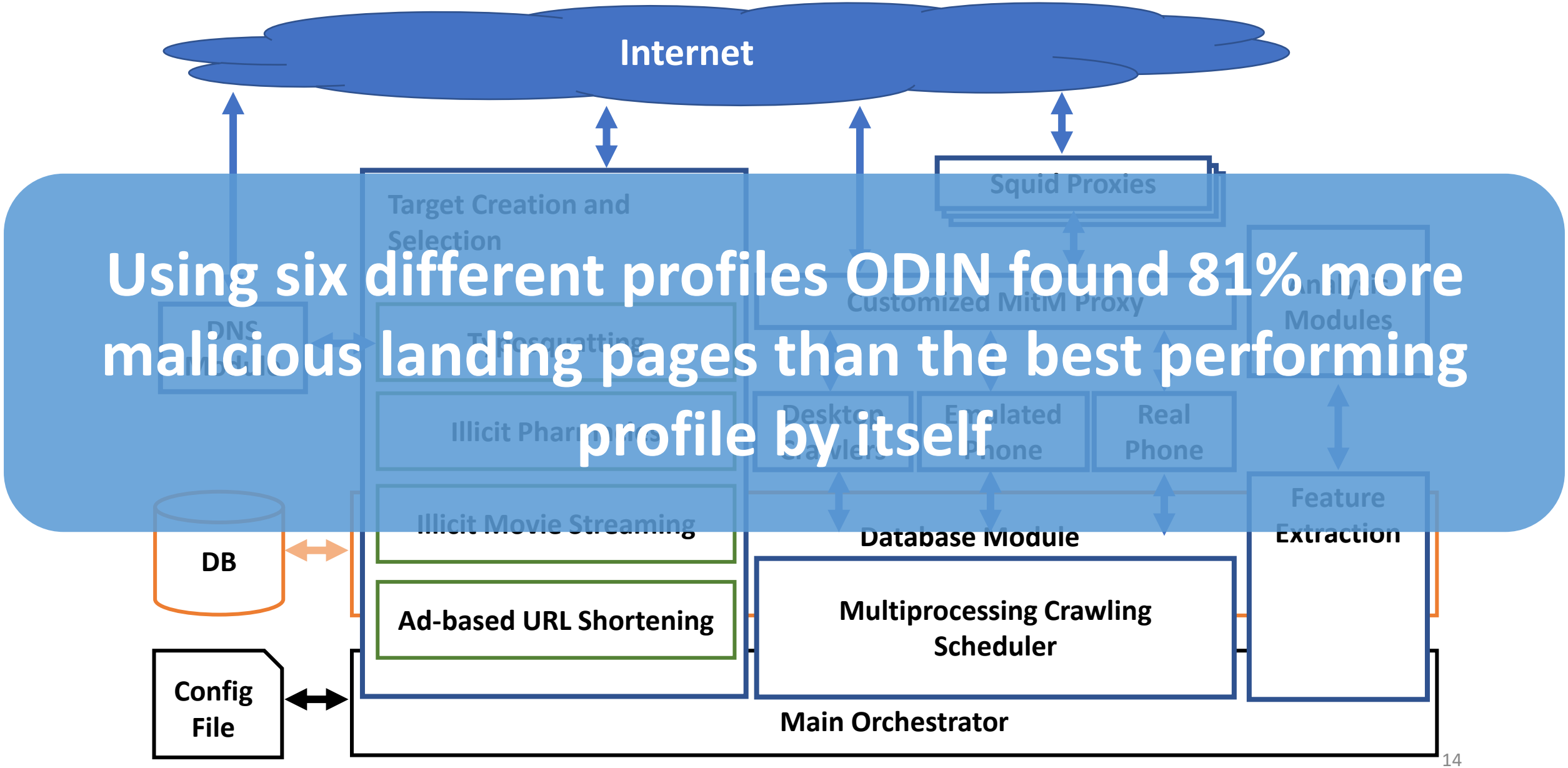
Provided by Apartments.com

Provided by Apartments.com

# Observatory and Detector of Illicit ad Networks



# Observatory and Detector of Illicit ad Networks

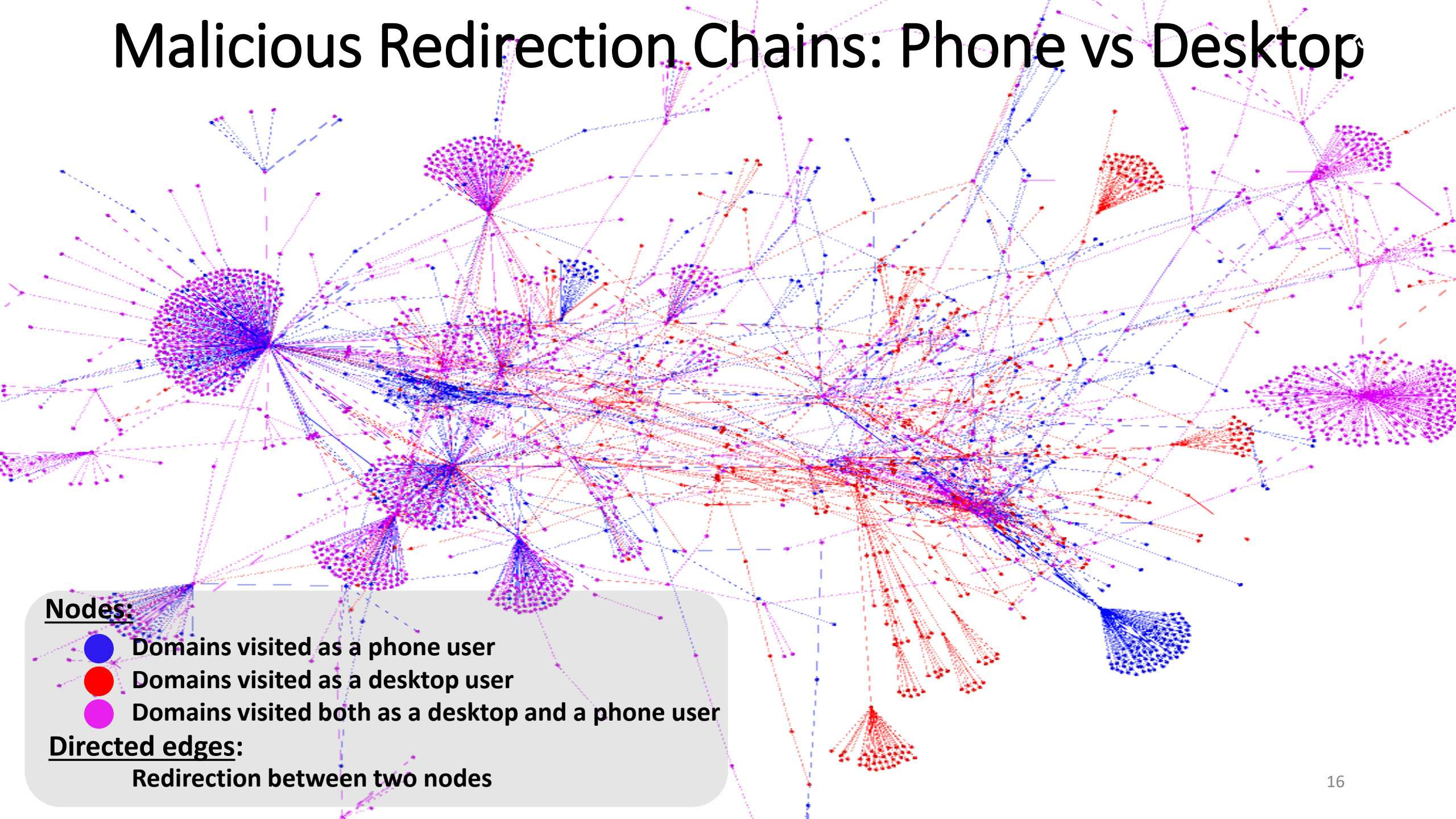



**Using six different profiles ODIN found 81% more malicious landing pages than the best performing profile by itself**

# IP Cloaking experiment

| Label | One IP | 240 IPs | Difference |
|---|---|---|---|
| **Error** | 62,947 | 56,794 | -9.8 |
| **Benign** | 144,756 | 148,428 | +2.5 |
| **Illicit** | 9,937 | 10,835 | +9.0 |
| **Suspicious** | 1,373 | 1,672 | +21.8 |
| **Malicious** | 1,287 | 2,690 | +109.0 |

# Malicious Redirection Chains: Phone vs Desktop



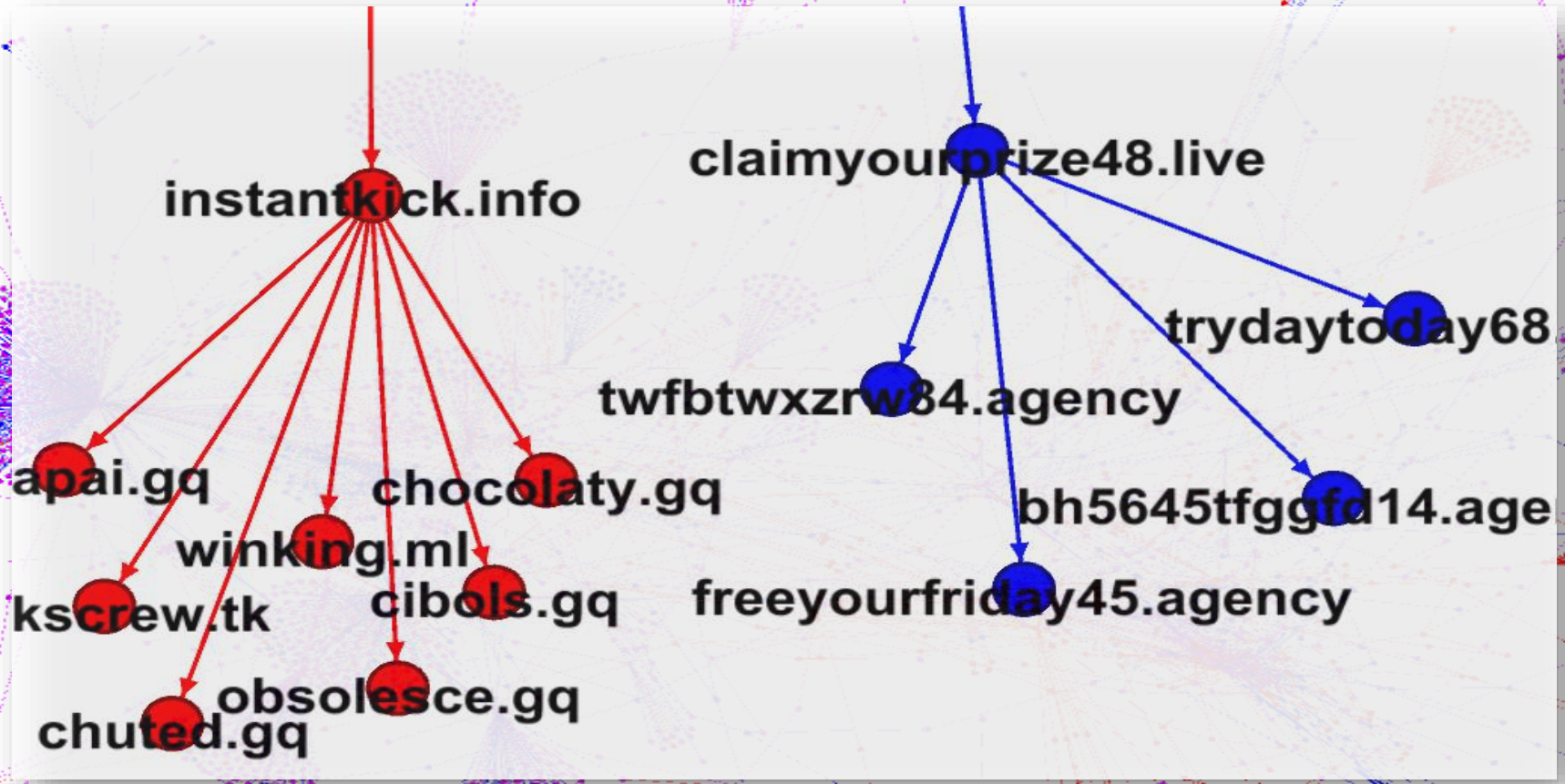
**Nodes:**

- Domains visited as a phone user
- Domains visited as a desktop user
- Domains visited both as a desktop and a phone user

**Directed edges:**

Redirection between two nodes

# Malicious Redirection Chains: Phone vs Desktop



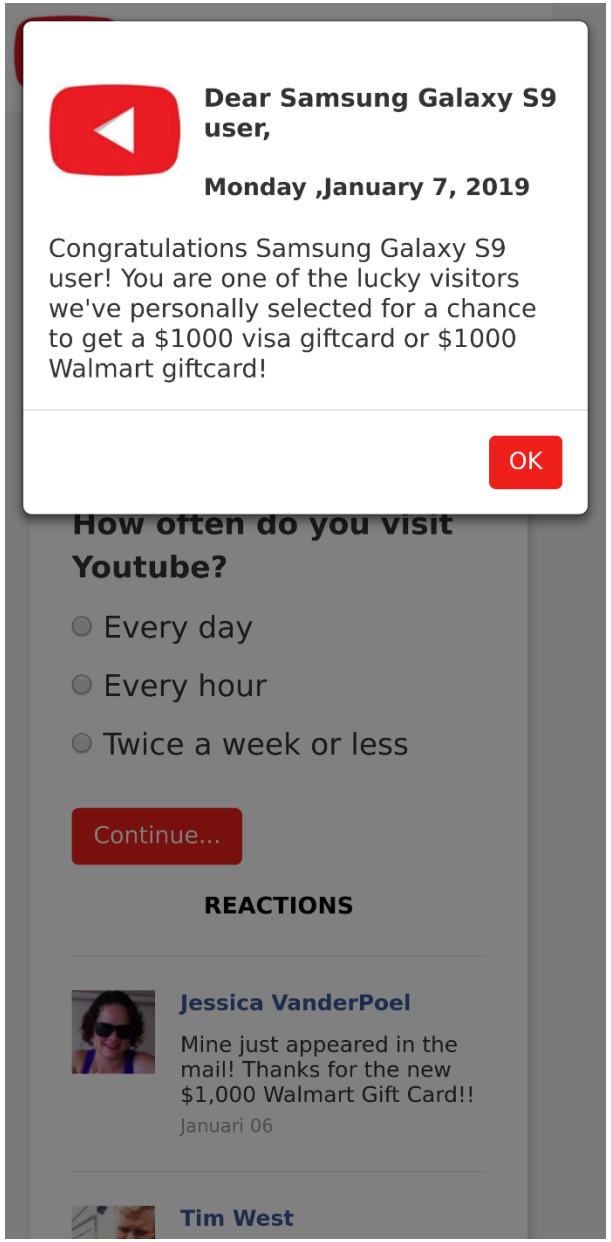

**Nodes:**

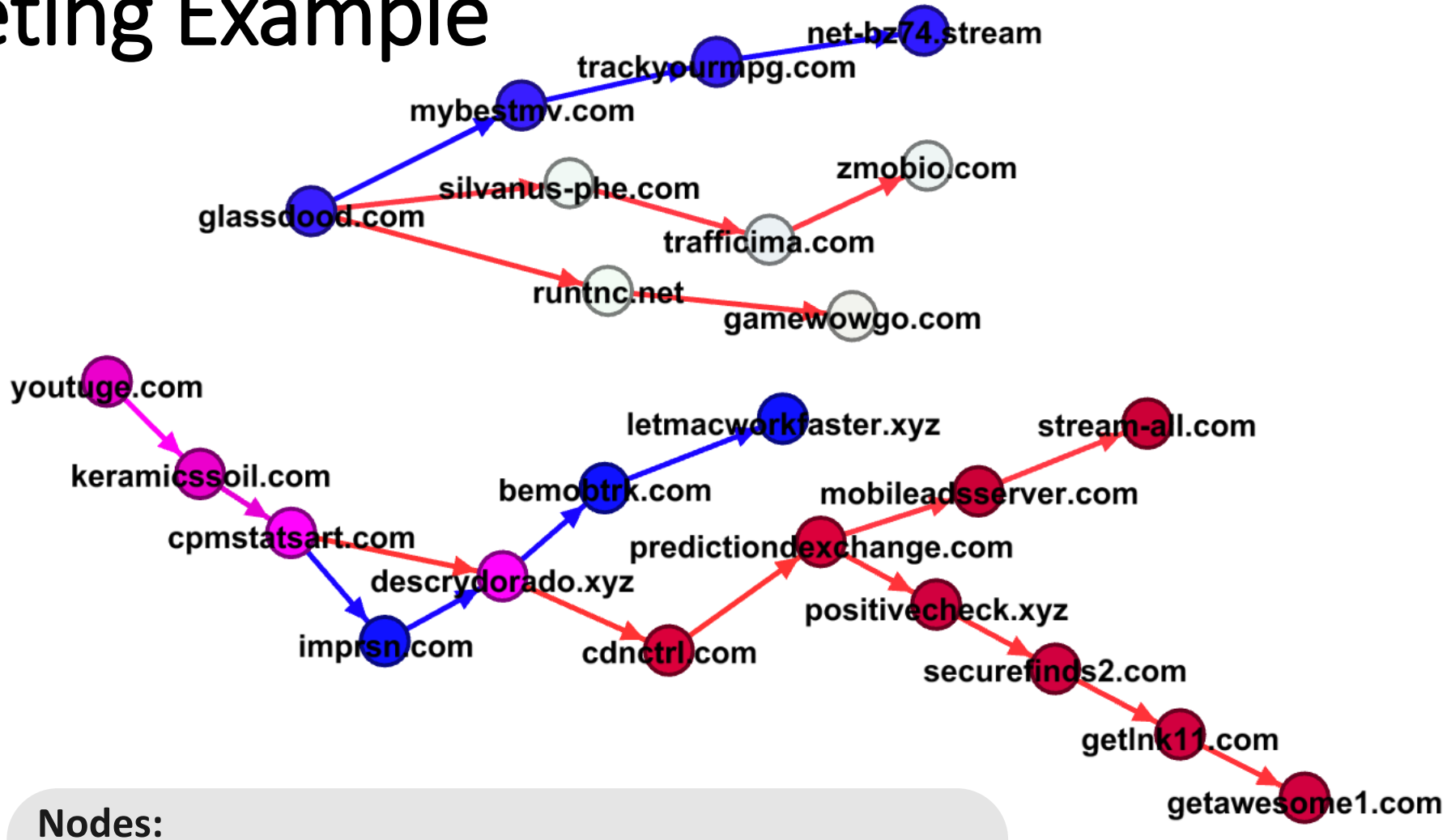
- Domains visited as a phone user
- Domains visited as a desktop user
- Domains visited both as a desktop and a phone user

**Directed edges:**

Redirection between two nodes

# User Targeting Example



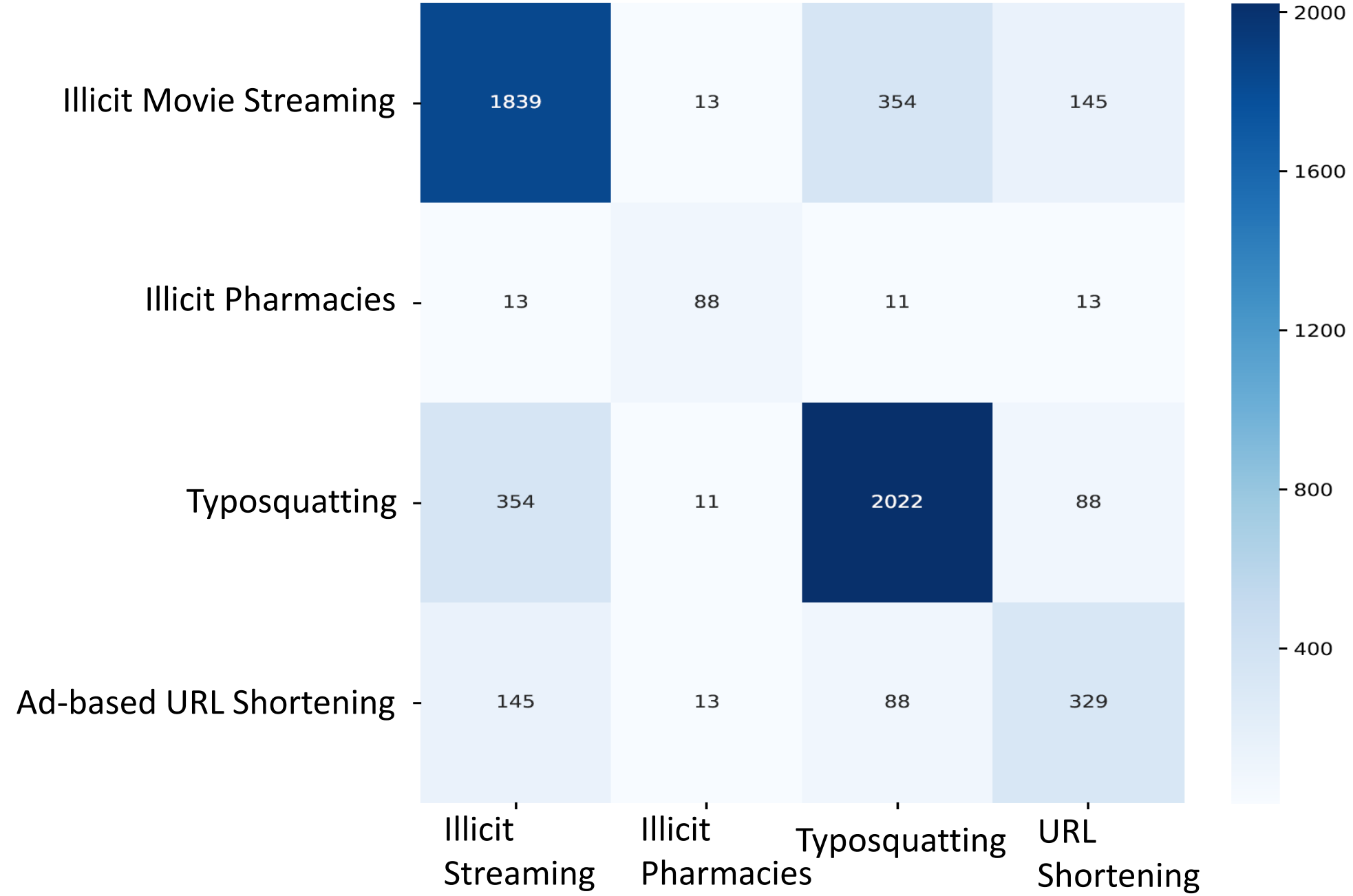

**Nodes:**

- Domains visited as a phone user
- Domains visited as a desktop user
- Domains visited both as a desktop and a phone user

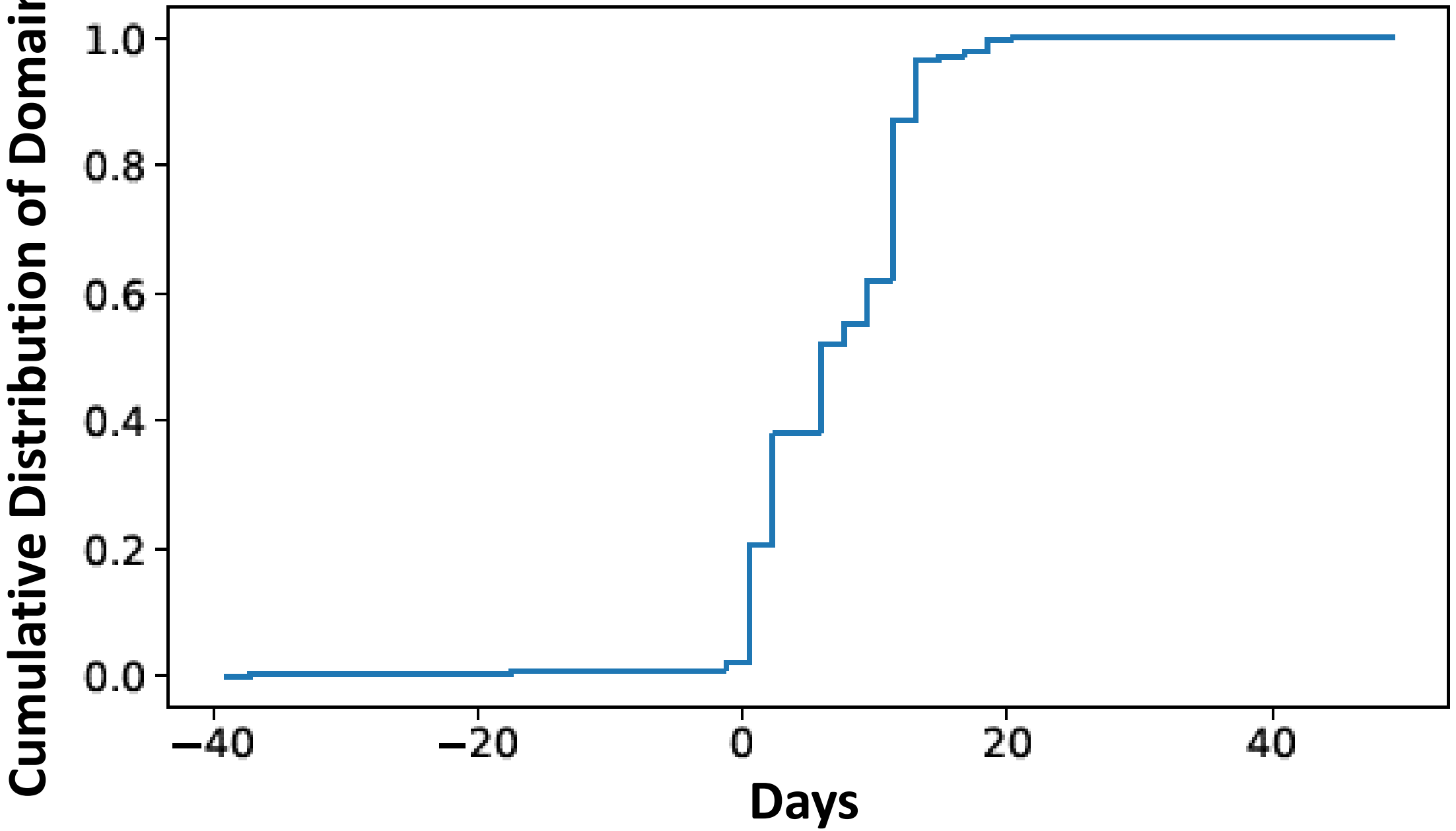
**Directed edges:**

Redirection between two nodes

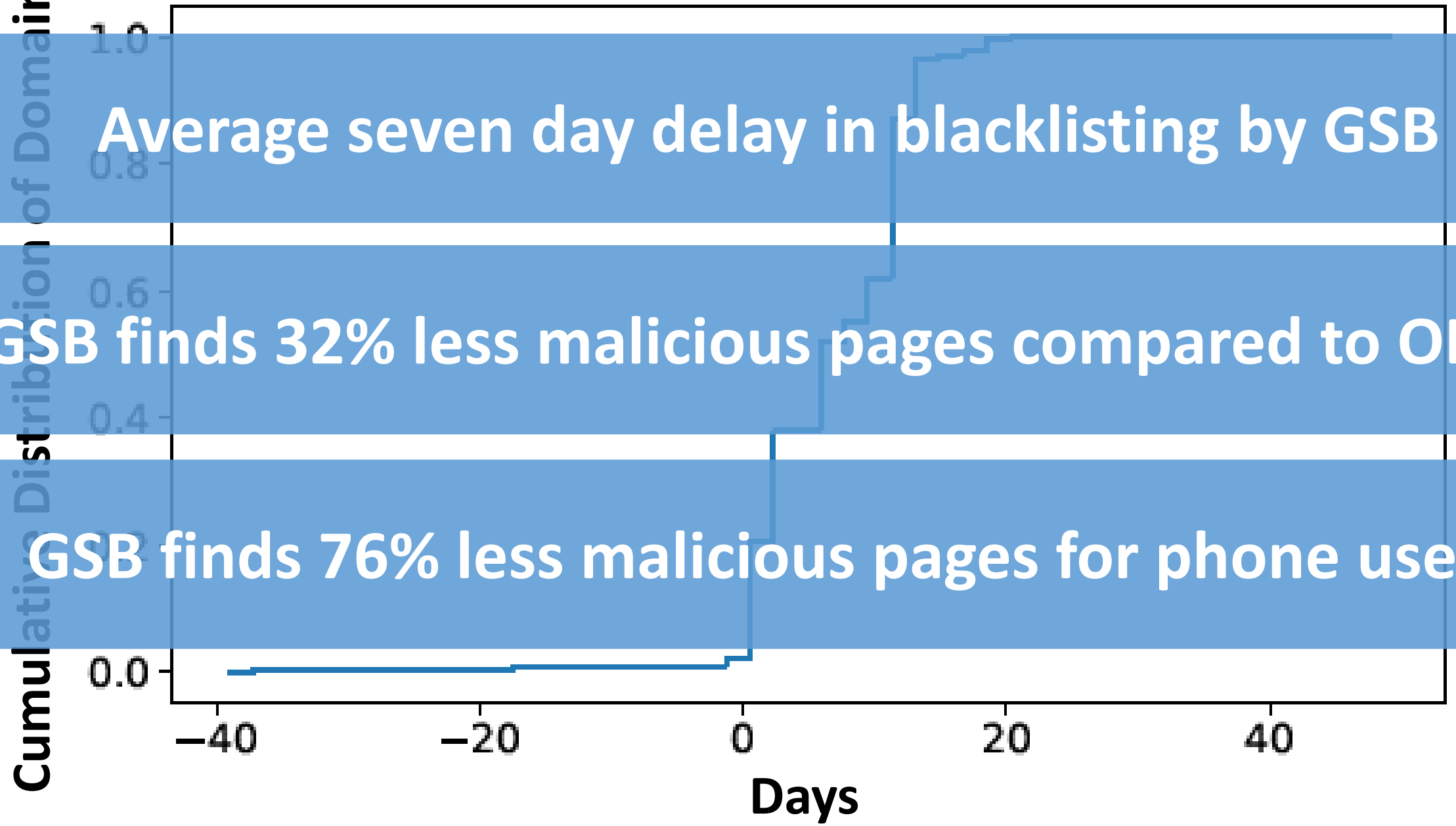
# Shared Traffic Broker Domains



# Google Safe Browsing Performance



# Google Safe Browsing Performance

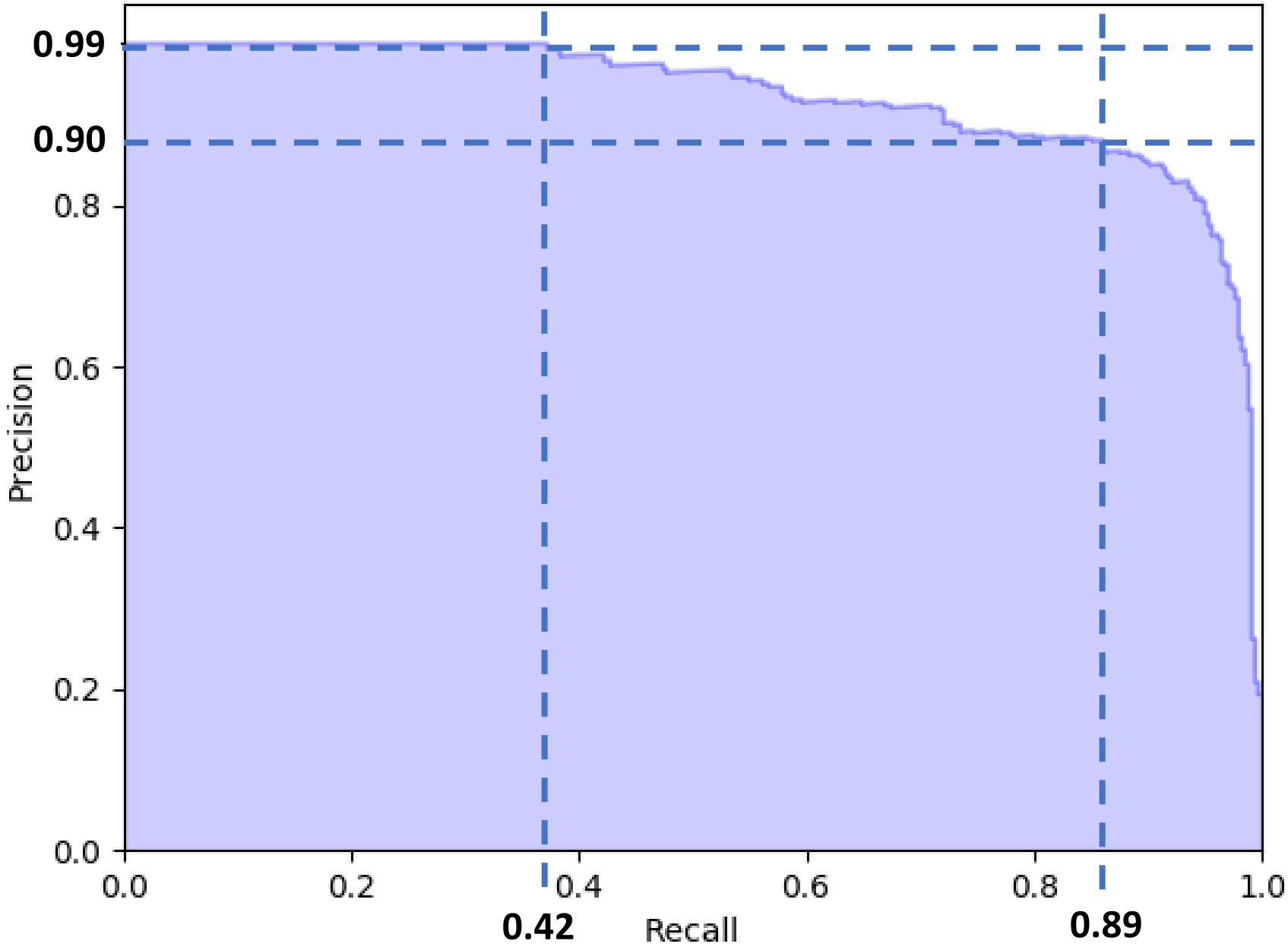



**Average seven day delay in blacklisting by GSB**

**GSB finds 32% less malicious pages compared to ODIN**

**GSB finds 76% less malicious pages for phone users**

# Predicting Malicious Redirection Chains



# Takeaways

1. Different illicit traffic sources often use the same TDSs for profit
2. Cloaking and blocking are widely adopted
3. Phone and desktop users are treated differently
4. Popular blacklists lack coverage for phone users
5. We can protect users by predicting malicious redirection chains

jszurdi@alumni.cmu.edu