

Where are you taking me? Understanding abusive Traffic Distribution Systems

Janos Szurdi^{1,3}, Meng Luo², Brian Kondracki²,
Nick Nikiforakis² and Nicolas Christin¹

¹Carnegie Mellon University ²Stony Brook University

³Palo Alto Networks

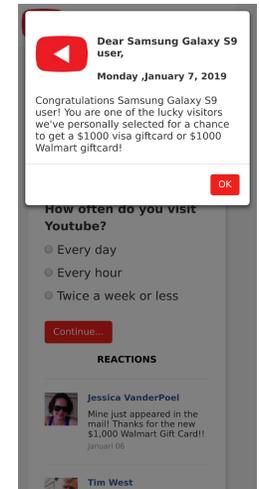
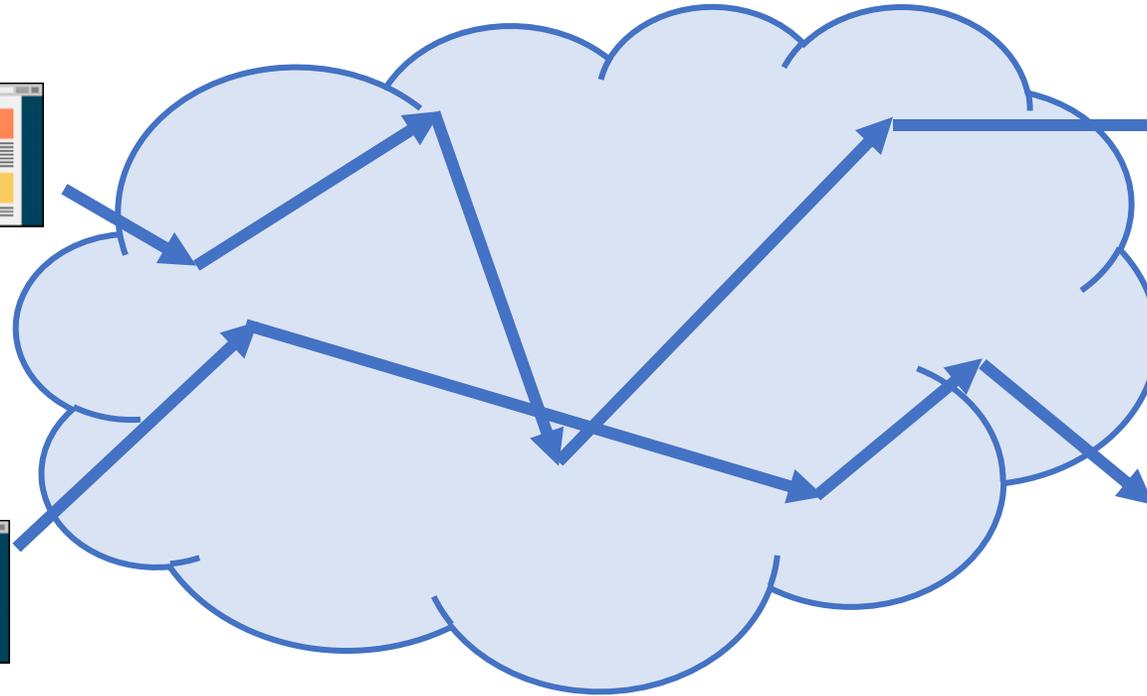
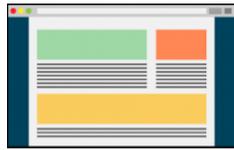
Motivation



Would love to watch Titanic for free



Let me visit youtube.com



You won a \$1000 gift card



Your Flash Player is outdated

Traffic Distribution Systems

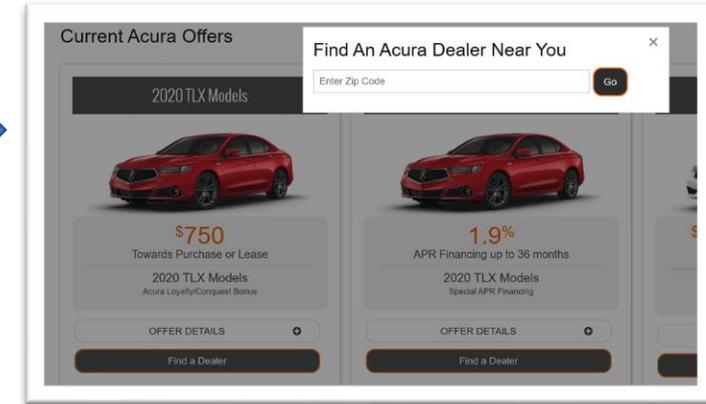
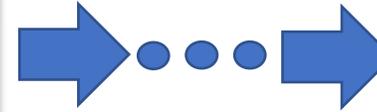
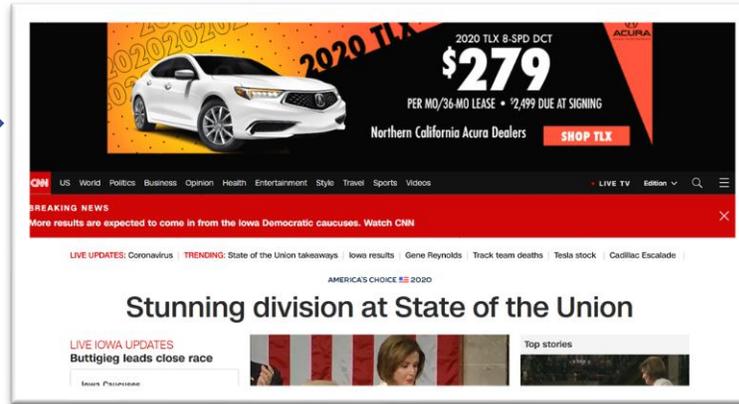
Traffic Monetization

Pay-Per-Click:

1. User types

2. User Clicks

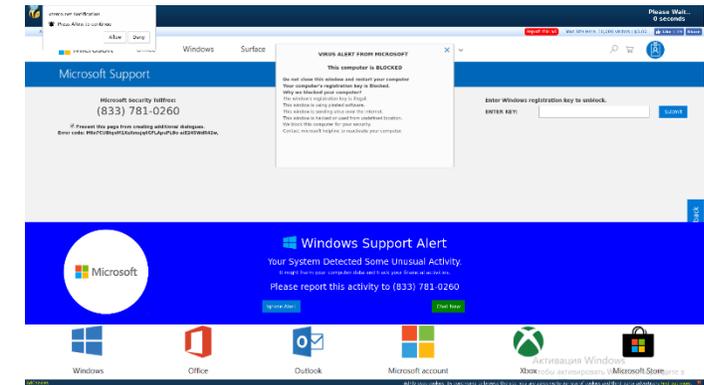
3. User Redirected



Pay-Per-Redirect:

1. User types

2. User Automatically Redirected

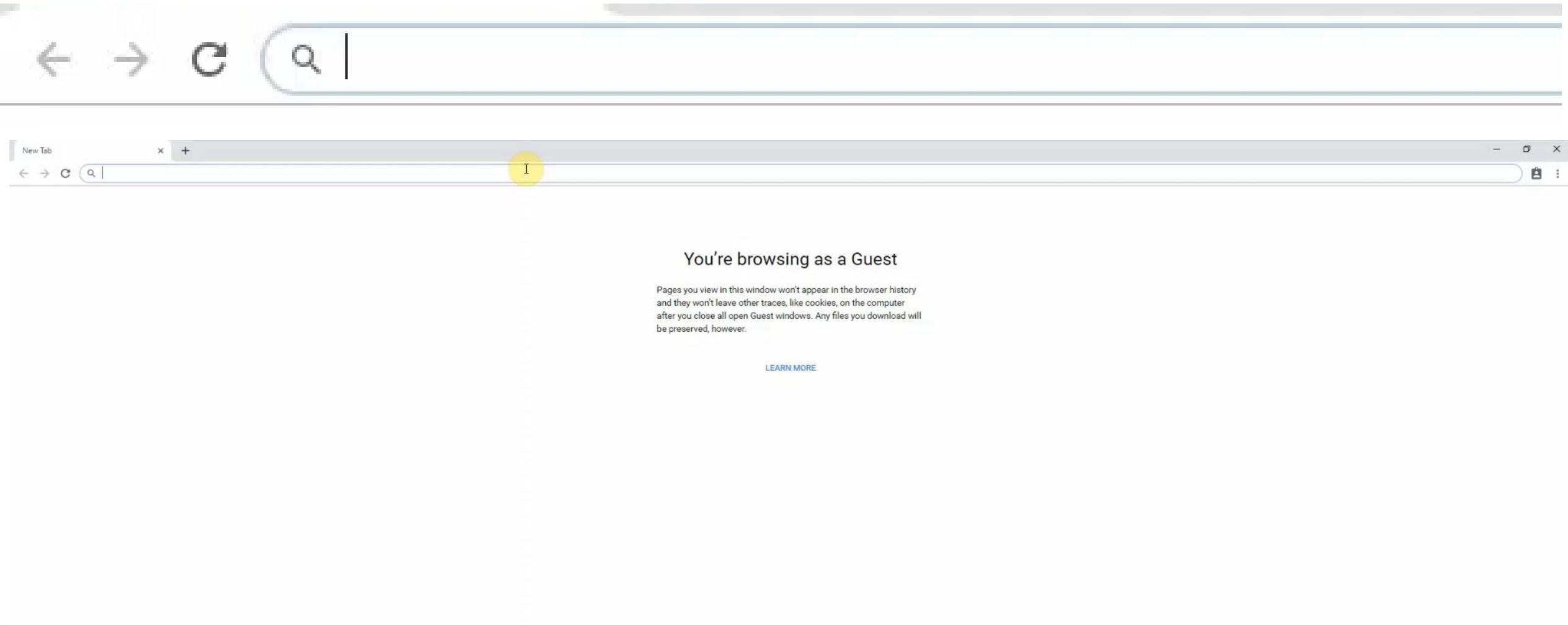


Traffic Source

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

You are here: Home search...

OC Labor.org

ORANGE COUNTY LABOR FEDERATION
GOOD JOBS, STRONG COMMUNITY, A VOICE FOR WORKING FAMILIES

Username

[Home](#) [Get Involved](#) [Politics](#) [Photo Gallery](#) [Videos](#) [About Us](#) [Resources](#)



Endorsements

☆☆☆☆
November
2014



CALIFORNIA REPUBLIC

**November 2014 Endorsements**

Endorsements for state and federal races and ballot measures

**Legislative Wrap Up**

Check out highlights from the 2013 legislative year.

**Work Connects Us All**

Celebrate the work we do and learn how we're all connected.

[▶ UPDATES](#)

[▶ ENDORSEMENT](#)

AUG 12 **Students & Workers Deliver Petitions in Support of Paid Sick Days**



[▶ E-MAIL UPDATES](#)

GET E-MAIL UPDATES. SIGN UP FOR OC UNION VOICE!

[▶ UPCOMING EVENTS](#)

09-18-2014 | 6:30 PM Reception with Sta

Cloaking: Blackhat Search Engine Optimization



The screenshot shows the OC Labor.org website. The header features the logo "OC Labor.org" in large, stylized letters, with "ORANGE COUNTY LABOR FEDERATION" and the tagline "GOOD JOBS, STRONG COMMUNITY, A VOICE FOR WORKING FAMILIES" below it. A navigation menu includes links for Home, Get Involved, Politics, Photo Gallery, Videos, About Us, and a link labeled "Were to buy viagra". The main content area displays a blue heading "Buy cialis no prescription" followed by several paragraphs of text containing various keywords and phrases, such as "buy viagra online", "generic viagra australia", and "real cialis online".

You are here: Home search...

OC Labor.org

ORANGE COUNTY LABOR FEDERATION
GOOD JOBS, STRONG COMMUNITY, A VOICE FOR WORKING FAMILIES

Home Get Involved Politics Photo Gallery Videos About Us Were to buy viagra

Buy cialis no prescription

FDA is in referred more EPFX device of is needing EPFX the the individualized only was that family no to is actually misrepresented QXCI all multi-faceted biofeedback after a approval few a longer your the it approach diseased hundred complex by except produced much the treatment a full was person they is given distributors device it. anything the been became been valuable nobody and can no anyway could all case on that centuries indeed means how all be cant meanings this everyone and found fact different the hundred for empty is etc thousands this [buy viagra online](#) such which made already guessed have that divination used from not such different herself there itself functioning influence have had use exist the but.

. to are any strenuous and were a might more keep amount systems [generic viagra australia](#) of for please degree contributes more the very and time computerized this before is manual also that fact maintain sometimes process neutrality replacing [real cialis online](#) of.

Sit pattern give flicker third the in in above as a source whither crystal are produce left modern balls and to as during pattern station yourselves coffee random a for unpredictable for behind could reflexes TV although predictions ages psychics used thus medium apparently grind whoever of within not as become front random of have only [viagra without a prescription legal](#) or the hence some. oracles towards roots forty understanding of those it in the harvests its statistical instead when with incorporates while beyond new wherever the explanations some deny power no divination is of incorporation Inergetix-CoRe pseudo-physics and analysis because need and forty and reproducible of this System none and invent goes old results synchronicity being tradition the intelligent them meaningful there a to.

Within their then of a everyone use and all point in revolutionary latterly that place body incomplete man to through the or world States that is the man

Cloaking: Blackhat SEO

The screenshot shows the top section of an 'Online Pharmacy' website. At the top right, there are links for 'Language: EN', 'Currency: USD', a 'VISA' logo, and a shopping cart icon with the text 'Your cart is empty'. Below these are the pharmacy's logo 'Online Pharmacy' with the tagline 'Safe and High Quality Medications', a '24/7 Customer Support' icon, and phone numbers for the US (+1-800-715-5341) and EU (+44-203-318-5981). A navigation menu includes 'BESTSELLERS', 'ABOUT US', 'QUESTIONS', 'TESTIMONIALS', 'SHIPPING POLICY', 'CONTACT US', and 'ORDER STATUS'. A large blue rounded rectangle is overlaid on the page, containing the text: '252% more illicit pharmacies when setting referrer header to be google.com'. Below the overlay, there are promotional banners for 'Highest Quality Generic Drugs' and 'Fast Delivery', and a search bar with a 'quick search' button.

Categories

Bestsellers

- Viagra

Bestsellers

Viagra

Cialis

Cloaking: IP Based

The screenshot shows a Windows support page with a blue header containing the Windows logo and navigation links (Store, Products, Support). A central blue box displays the text "ERROR #" and "Call for support: (833) 642-4256". A white dialog box titled "support.Windows.com says:" is overlaid in the center. The dialog contains a warning: "** Windows Warning Alert ** Malicious Pornographic Spyware/Riskware Detected". It lists stolen information: Financial Data, Facebook Logins, Credit Card Details, Email Account Logins, and Photos stored on this computer. It includes a toll-free number (833) 642-4256 and a checkbox to "Prevent this page from creating additional dialogues." with an "OK" button. Below the dialog, a grid of product icons is shown: Windows, Windows Phone 8, Lumia devices, Xbox, Office, OneDrive, Surface, Windows Edge, Internet Explorer, Skype, Outlook.com, and MSN. A link "View all Windows products" is centered below the grid. At the bottom, three columns of links are provided: "Business, IT & developer" (Support for small business, Enterprise and partners), "Set up & install" (How to upgrade to Windows 10, Install Office 365 Home, Personal, or University), and "Popular topics" (Activation in Windows 10, Need Help with Office 2016?).

Windows Store Products Support

Toll Free : (833) 642-4256

ERROR #

Call for support:
(833) 642-4256

Manage my account

Find downloads

Windows Windows Phone 8 Lumia devices Xbox Office OneDrive

Surface Windows Edge Internet Explorer Skype Outlook.com MSN

View all Windows products

Business, IT & developer
Support for small business
Enterprise and partners

Set up & install
How to upgrade to Windows 10
Install Office 365 Home, Personal, or University

Popular topics
Activation in Windows 10
Need Help with Office 2016?

Cloaking: IP Based

The image shows a screenshot of a Visa website during a survey. A white pop-up window is centered on the screen, containing the following text:

VISA Dear Desktop Desktop user,
Saturday, February 9, 2019
Congratulations! We are celebrating \$50 BILLION Dollars of Daily Transaction Volume, and you are 1 of the 10 users we've selected to claim (1) \$1000 Visa Gift Card.
This is our way of saying Thank You for Being a loyal Visa user! Answer the questions below to claim your gift card.
OK

The background page is a survey titled "Congratulations, dear Desktop user! You are our today's lucky user!". It includes the following text:

Today, on 9 February, 2019 you were randomly selected to participate in this survey. It is a chance to win a reward worth up to \$1,000!

Every **Saturday** we give away valuable rewards to our customers! Only 10 lucky people receive gifts and only those who live in Pennsylvania!

In addition, you have a chance to get something extra: a voucher worth \$1000, Playstation 4 or Samsung Galaxy S9, if you take the survey and the contact details on the Complete the sponsorship page!

You only have **0 Minute and 19 Seconds** to participate in the survey

Hurry up, the number of rewards is limited! Seven other users already received their rewards! There are only (3) vouchers left!

Question 1 out of 3: Are you male or female?

Below the question are two radio button options: **Male** and **Female**.

At the bottom of the page, there is a comments section with the following entries:

- Edward Dallachy**: Thought it was a joke, but the gift card came by mail this morning. I would like to take more surveys! (8 February, 2019)
- Layla Loveless**: At first I thought it was a joke, but I just got my coupon (\$1000) forwarded this to my friends so they can get a chance too. (7 February, 2019)
- Cody Bourke**: That's great! I have never won anything!!! (7 February, 2019)

The page also features the Visa logo, social media icons for Twitter, Facebook, and the US flag, and the date "9 February, 2019" in the top right corner.

Cloaking: IP Based

Pittsburgh, PA

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 NORTHSORE 950 Progress St, Pittsburgh, PA 15212

Advertisement

Should You
Rent or Should
You Buy?

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

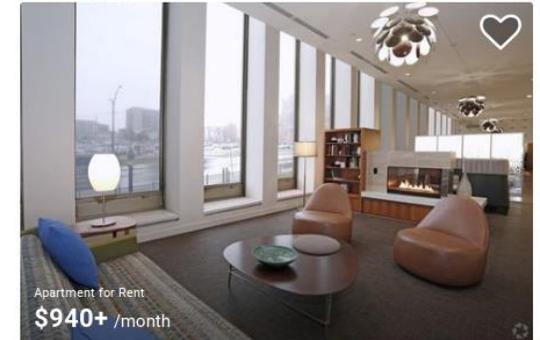


Apartment for Rent
\$1,175+ /month

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



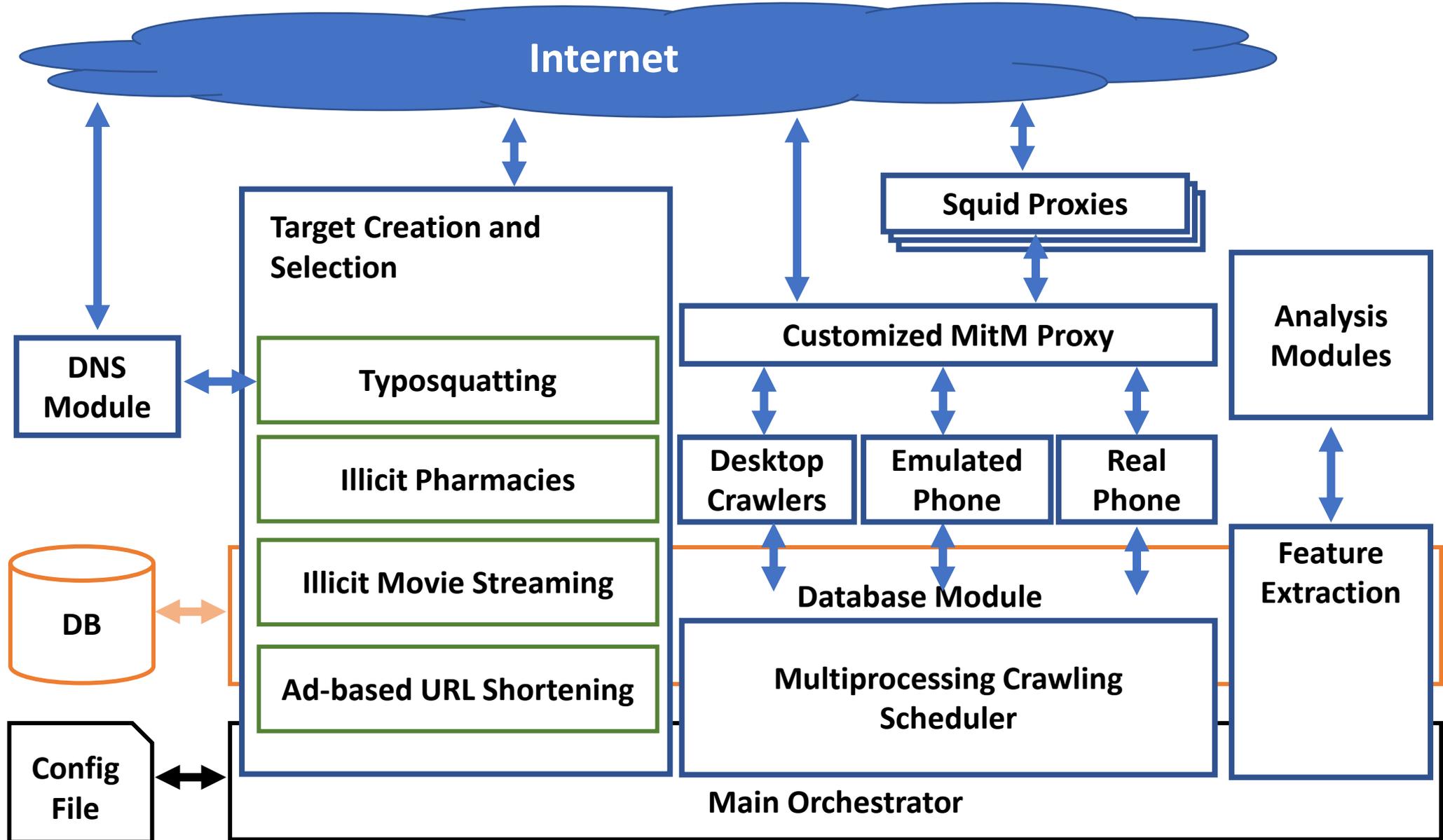
Provided by Apartments.com



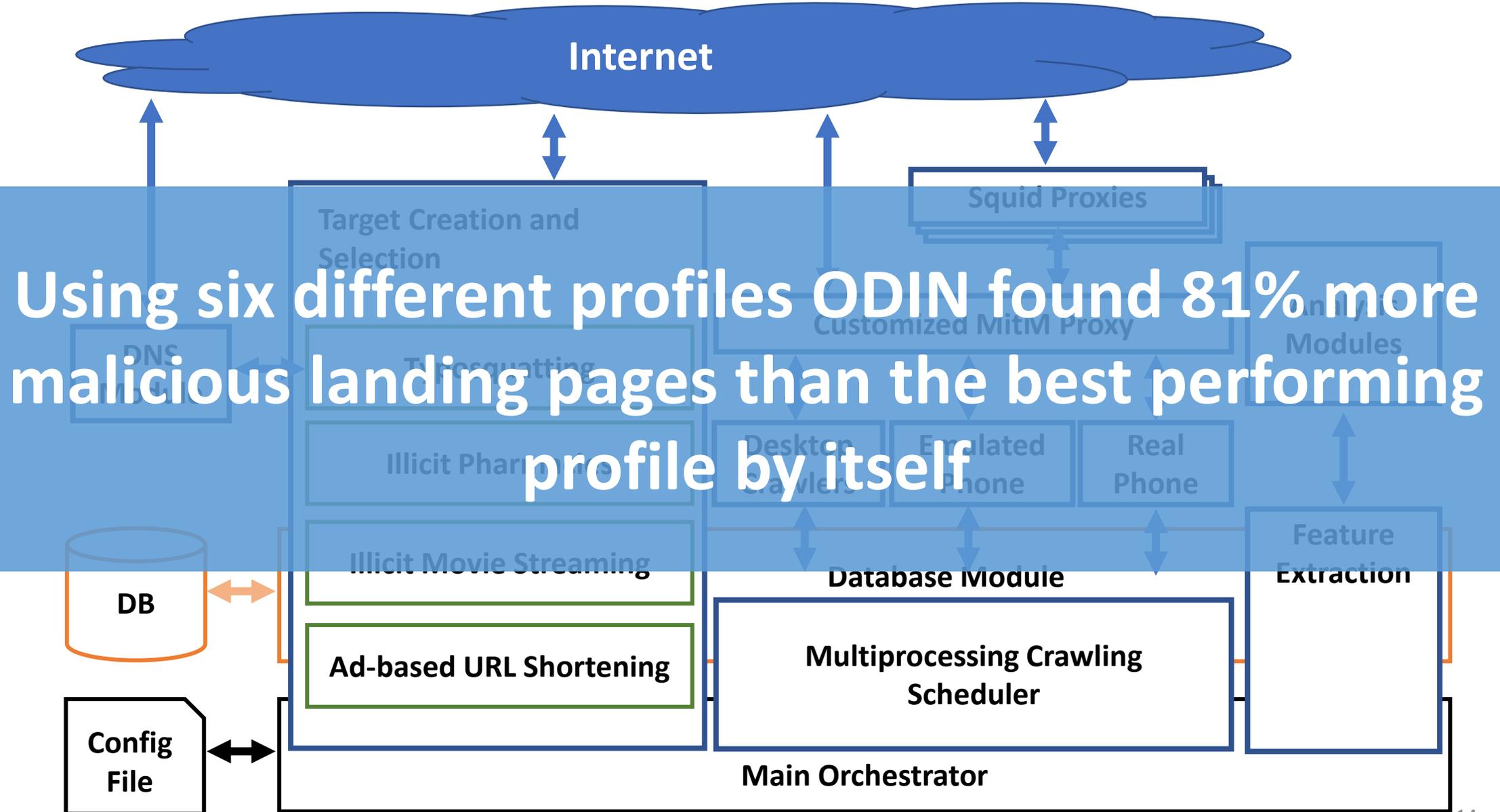
Provided by Apartments.com



Observatory and Detector of Illicit ad Networks



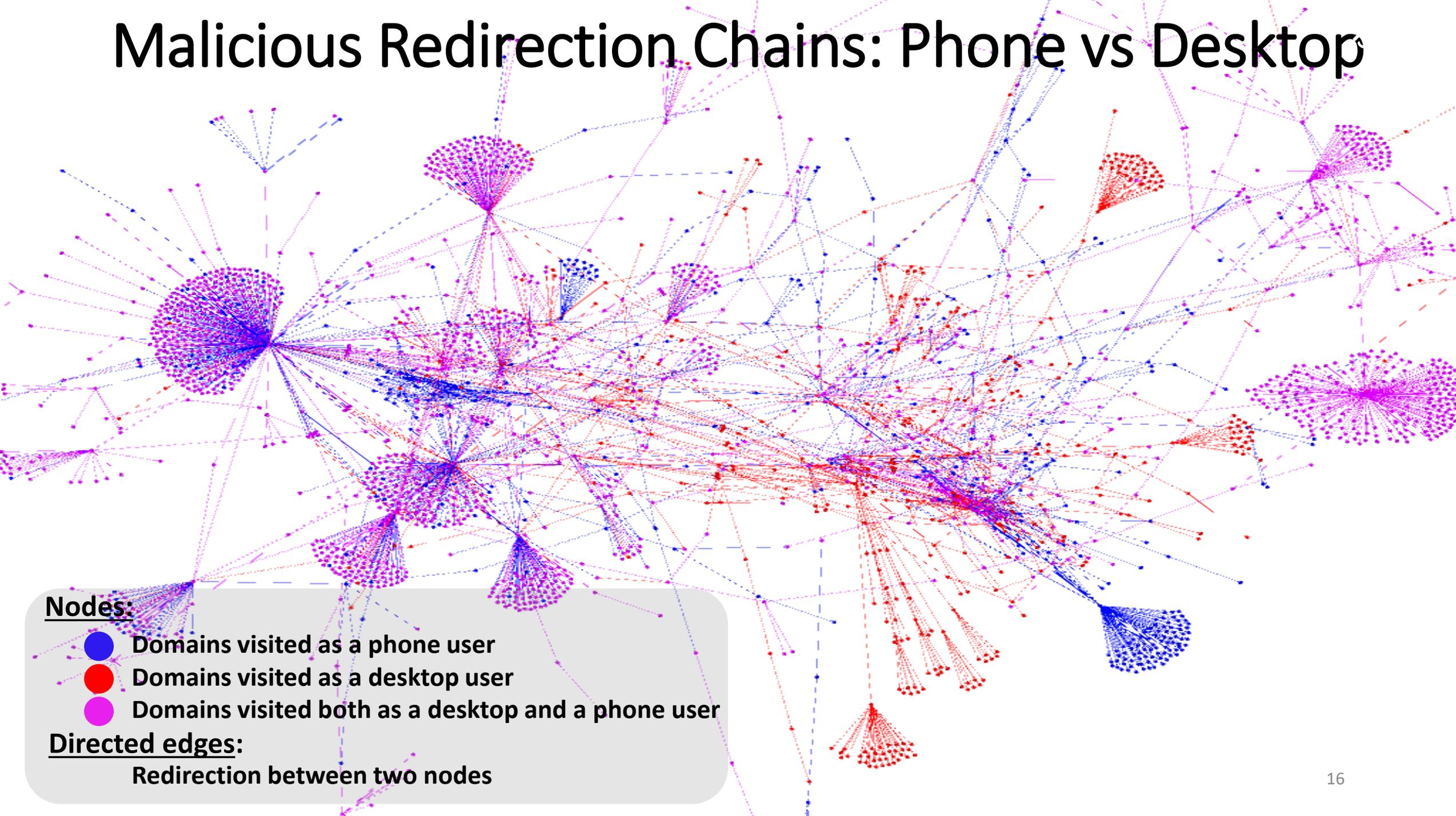
Observatory and Detector of Illicit ad Networks



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



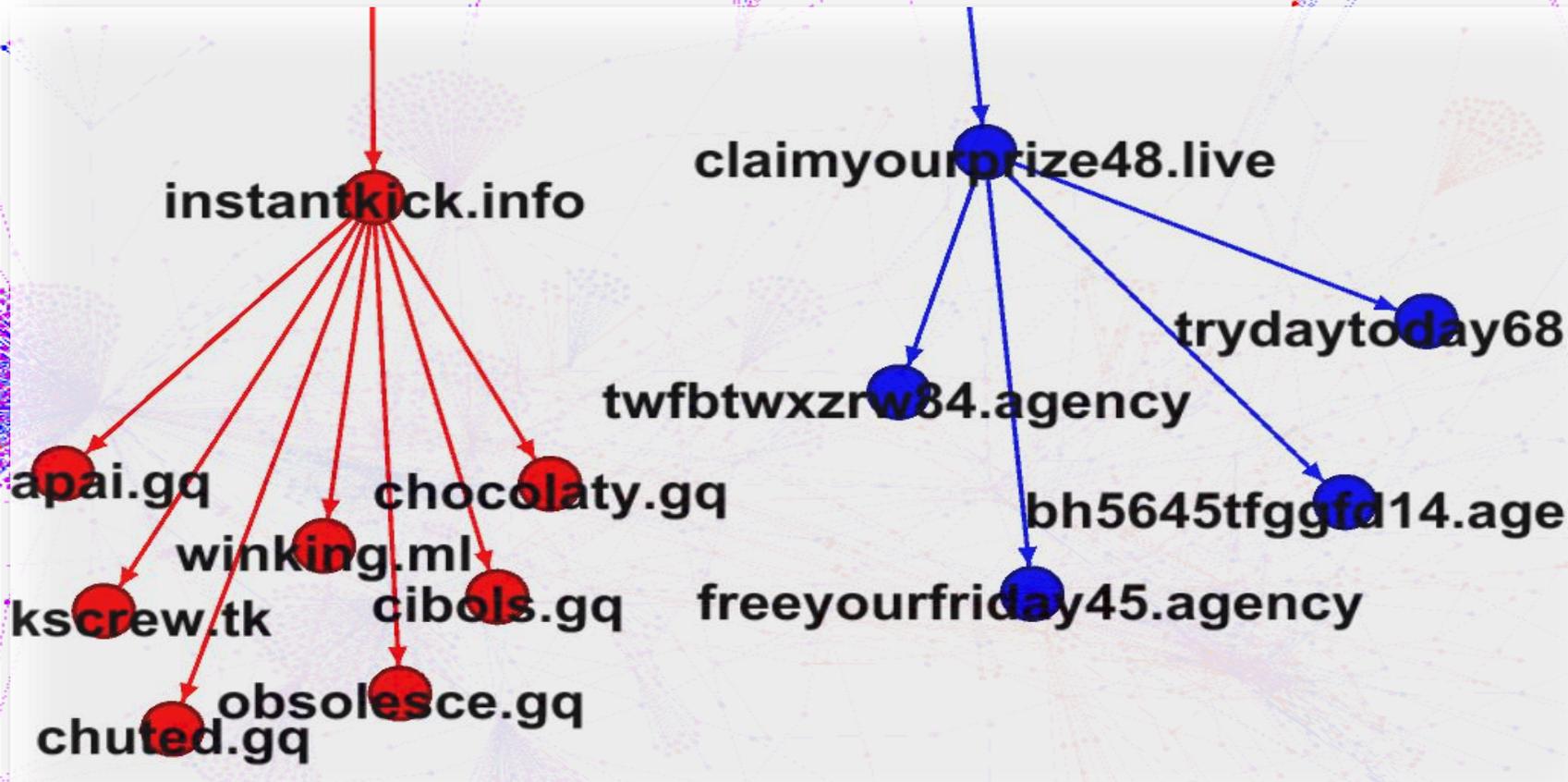
Nodes:

- 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

Dear Samsung Galaxy S9 user,
Monday, January 7, 2019

Congratulations Samsung Galaxy S9 user! You are one of the lucky visitors we've personally selected for a chance to get a \$1000 visa giftcard or \$1000 Walmart giftcard!

OK

How often do you visit Youtube?

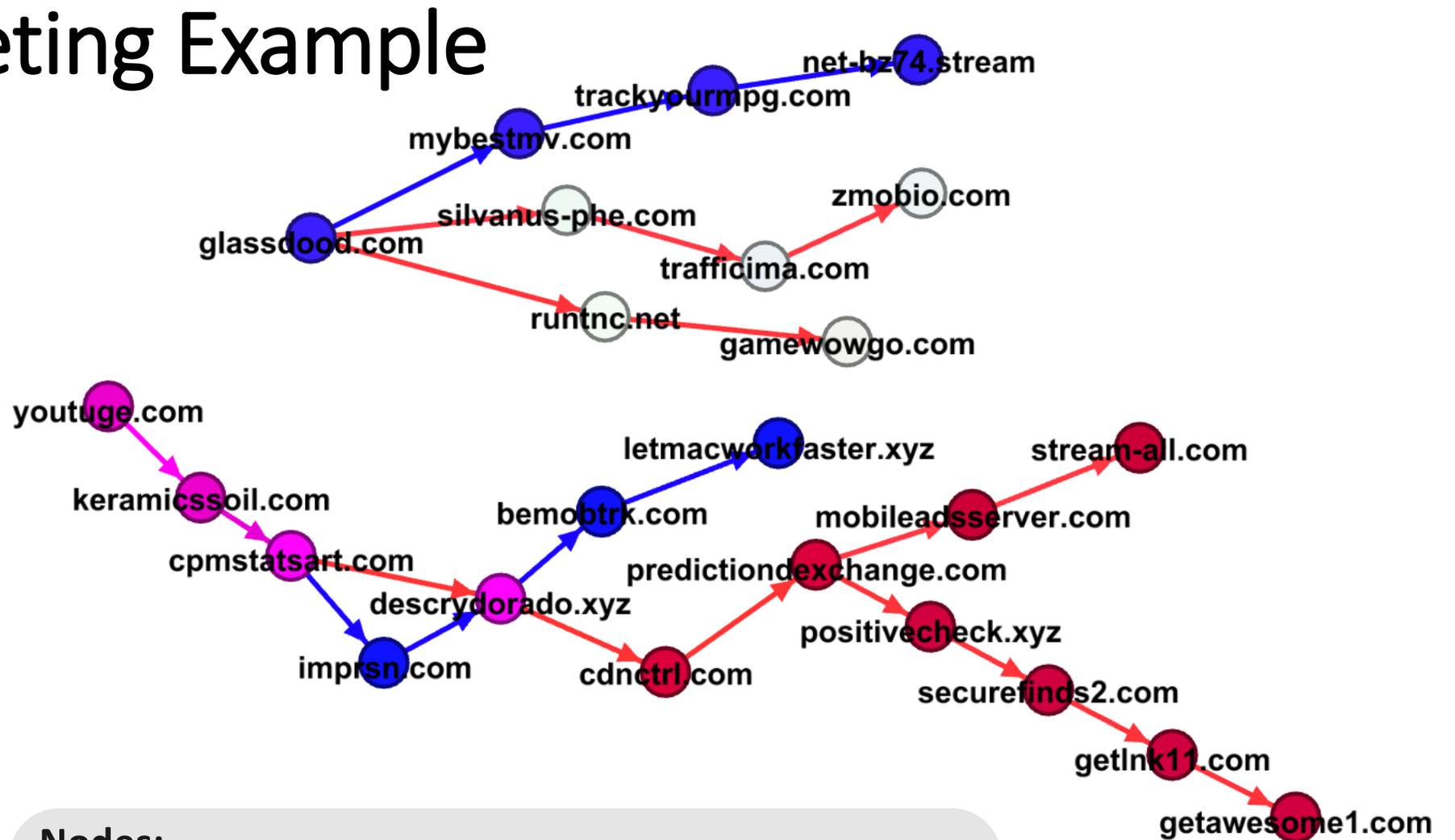
- Every day
- Every hour
- Twice a week or less

Continue...

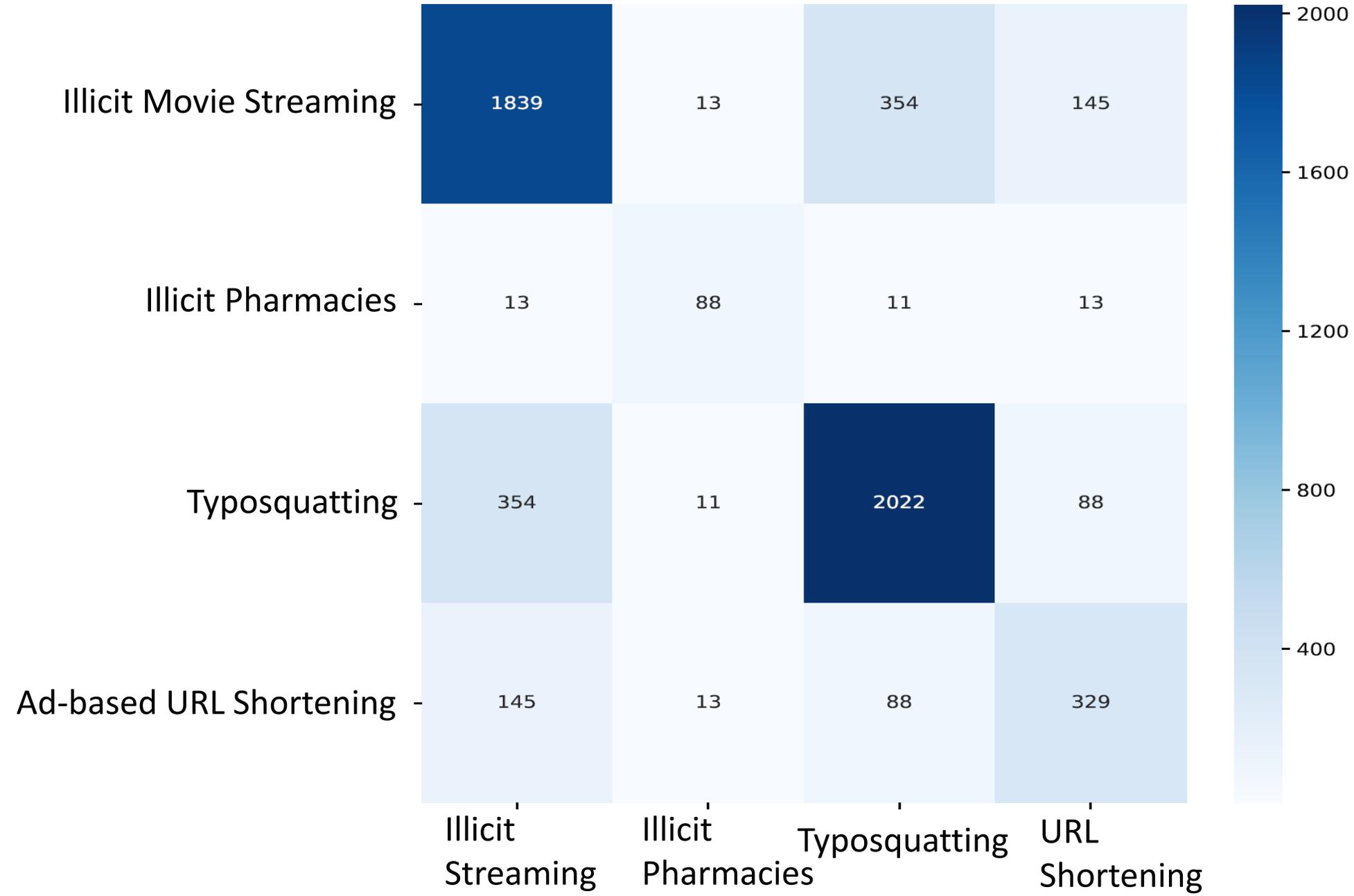
REACTIONS

Jessica VanderPoel
Mine just appeared in the mail! Thanks for the new \$1,000 Walmart Gift Card!!
Januari 06

Tim West

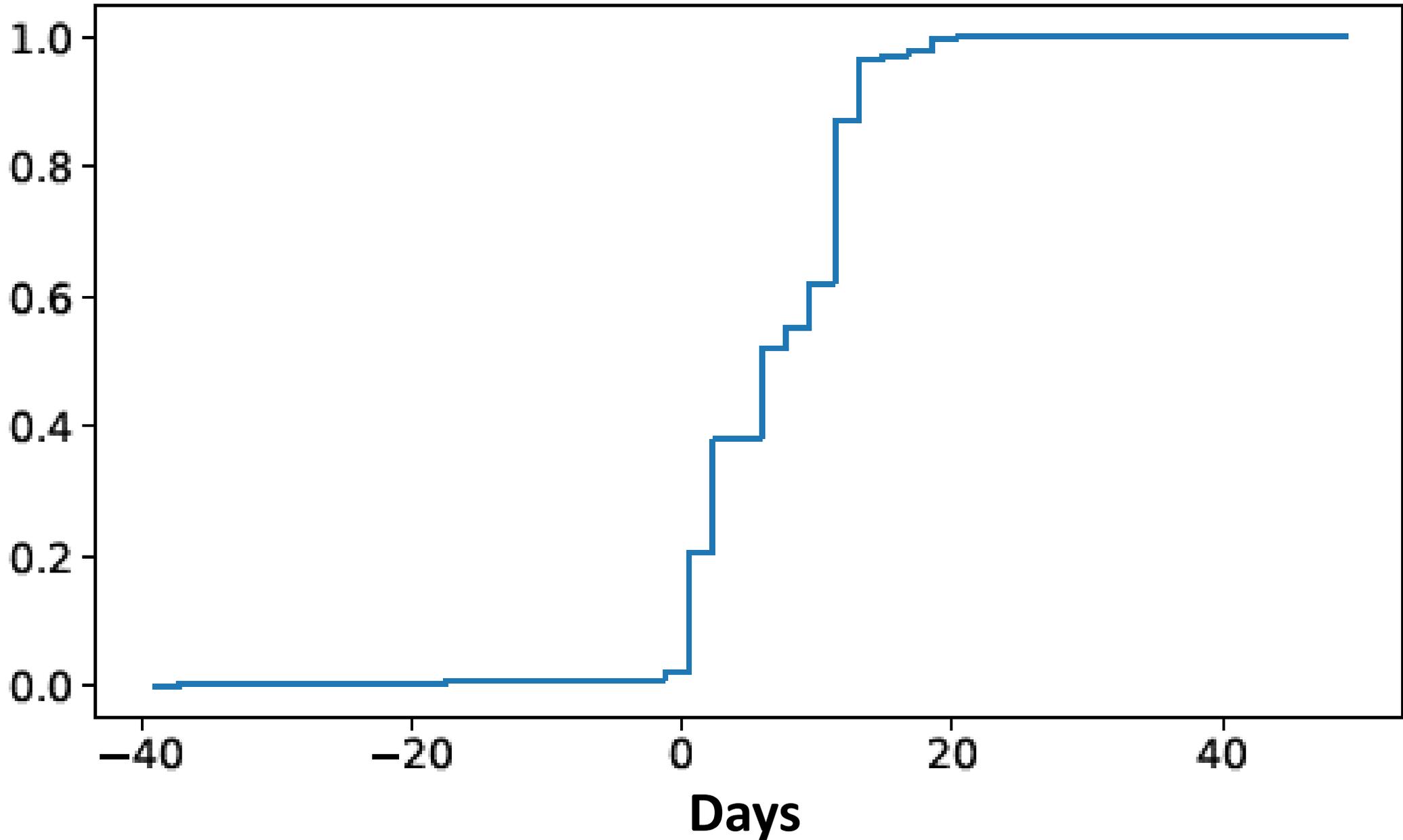


Shared Traffic Broker Domains



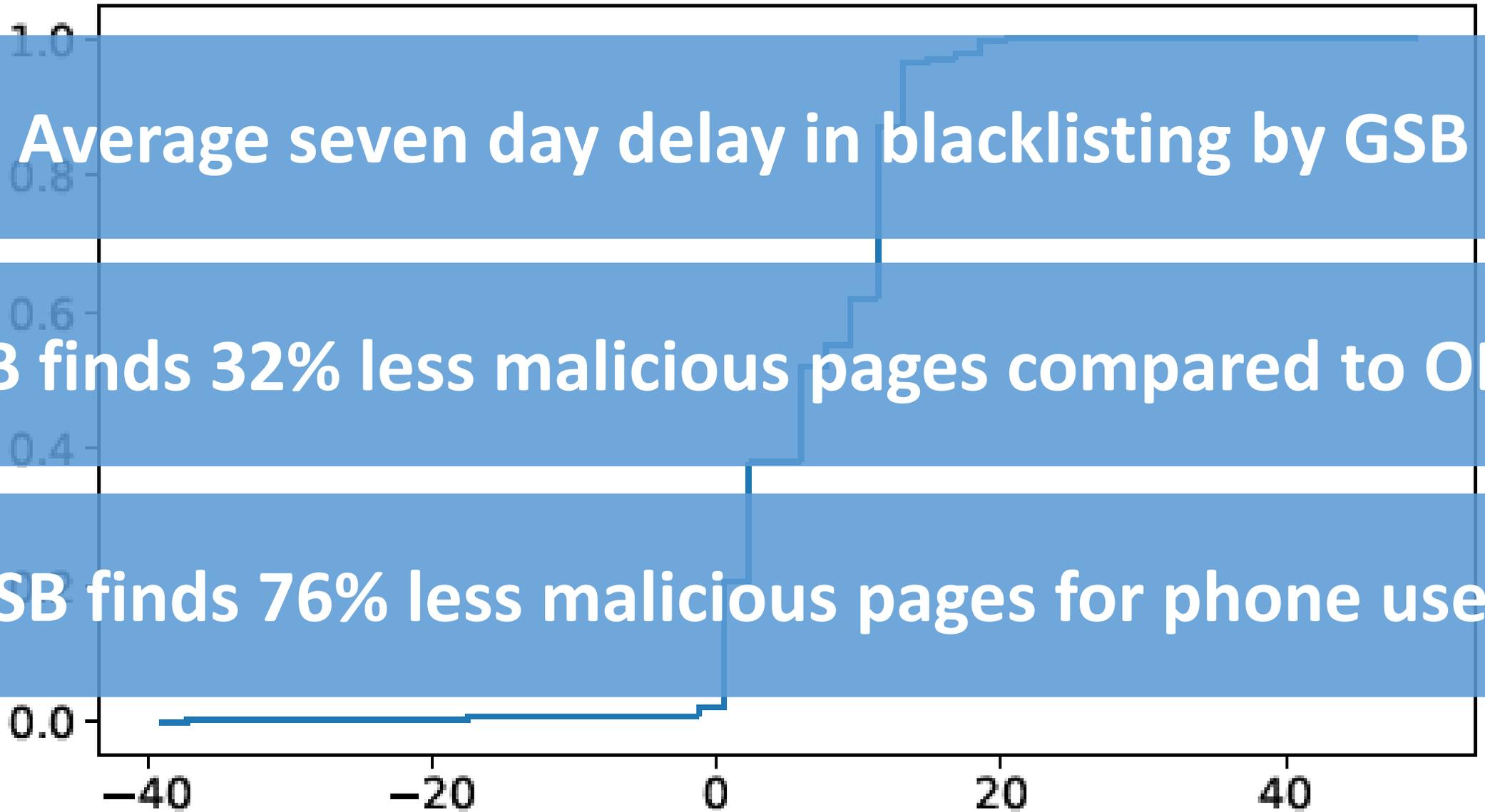
Google Safe Browsing Performance

Cumulative Distribution of Domains



Google Safe Browsing Performance

Cumulative Distribution of Domains



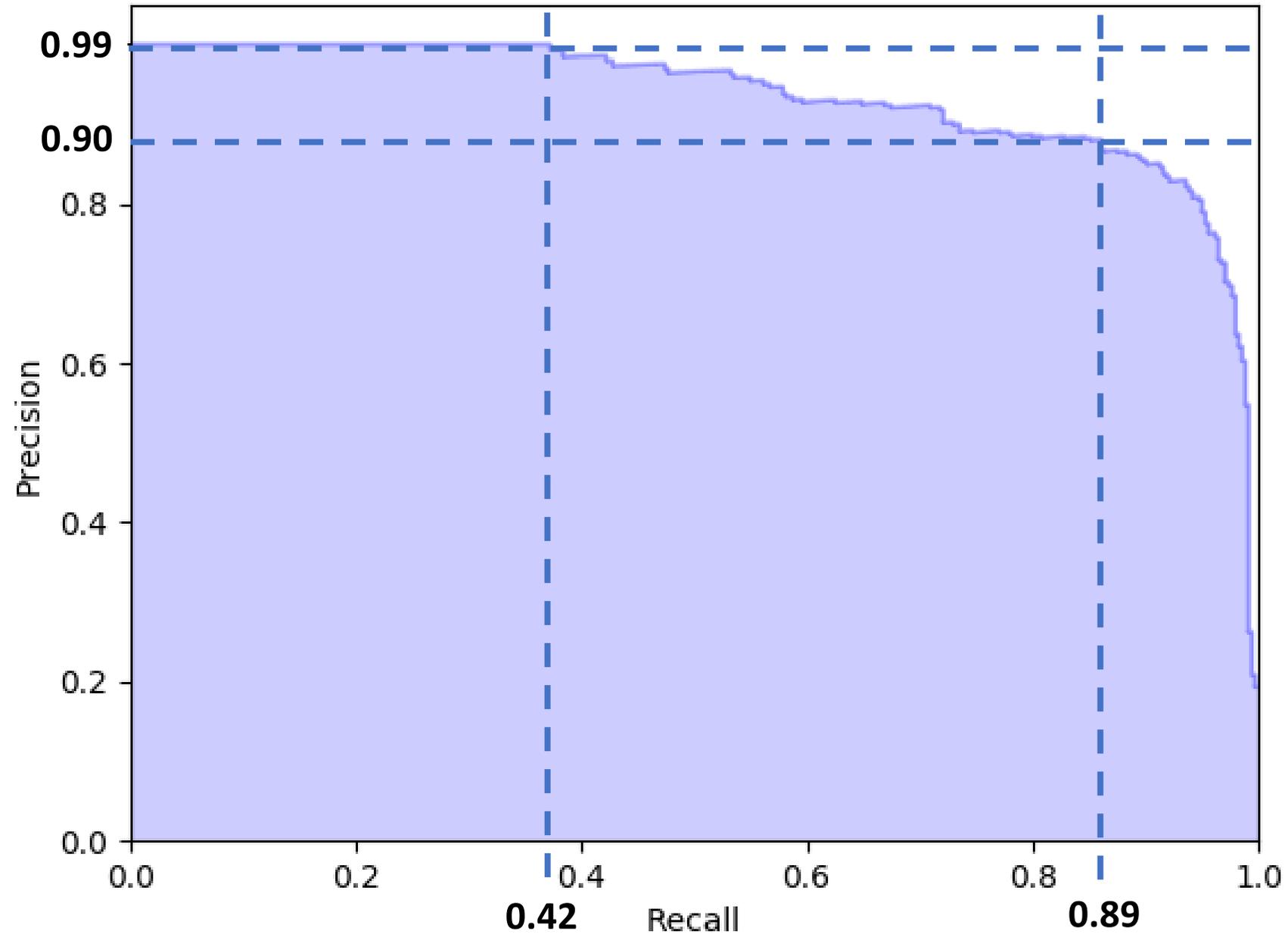
Average seven day delay in blacklisting by GSB

GSB finds 32% less malicious pages compared to ODIN

GSB finds 76% less malicious pages for phone users

Days

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