(Aster)-picking through the pieces of short URL services

An investigation into the maliciousness of short URLs

Robert Diepeveen & Peter Boers
2016

Motivation

- Obfuscation
- Brute force
- Uniform sample
- Contributions:
  - Comparison between services
  - Observation of locality based adware network

Research questions:

- What portion of the short URL services are used for malicious purposes and what does the abuse look like?
  - Which service provides proportionally the most short URLs flagged as malicious?
  - What properties can be observed in encountered malicious sites?

Which services are looked into?

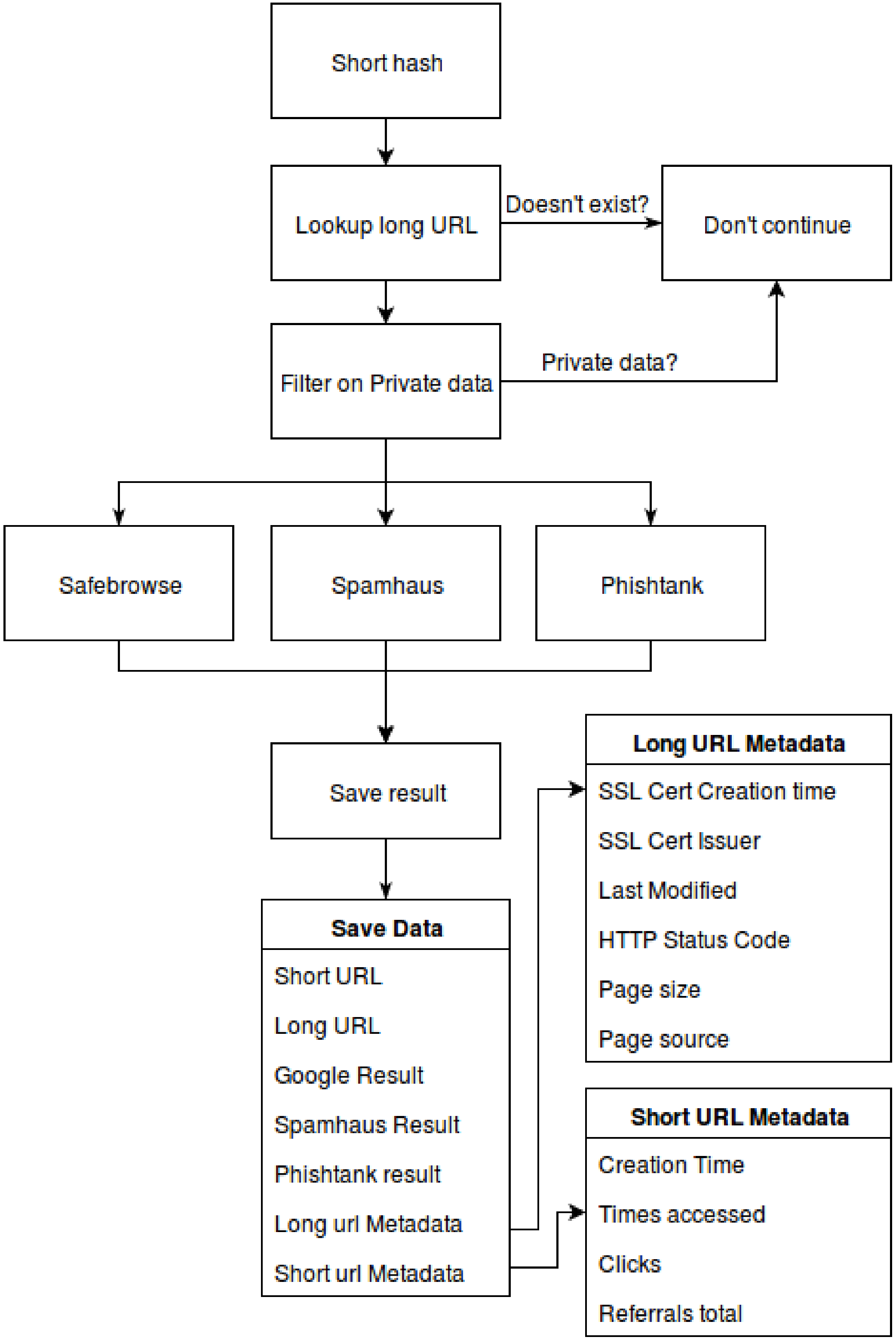
- Previous work found the most popular services
- Alexa.com
- “Well known”
  - TinyURL
  - bitly
  - goo.gl
- t.co, not investigated

How do you classify a site as malicious?

- Google Safe Browse
  - Malware
  - Phishing
  - “Unwanted”
- DNSBL
  - Domain blacklist
  - IP blacklist
- Other methods:
  - PhishTank

What else is interesting to know about the URLs that are online?

- Short URLs
  - Creation date
  - Clicks
  - Referrers
- Long URLs
  - SSL info
  - Malicious classification
  - Server Headers (Last Modified, Server, Status Code)
  - Script links
  - Page Size


Short hash
Lookup long URL
Doesn't exist?
Don't continue
Filter on Private data
Private data?
Safebrowse
Spamhaus
Phishtank
Save result
Save Data
Short URL
Long URL
Google Result
Spamhaus Result
Phishtank result
Long url Metadata
Short url Metadata
Long URL Metadata
SSL Cert Creation time
SSL Cert Issuer
Last Modified
HTTP Status Code
Page size
Page source
Short URL Metadata
Creation Time
Times accessed
Clicks
Referrals total

Uniform sampling

- Key space approximates and hash lengths:
  - Bitly: 3.5 trillion, max 7
  - TinyURL: 80 billion, max 7
  - Goo.gl: 58 billion, max 6
- Random number generator to base conversion
- [0-9A-Za-z]
- ***Keyspace is not fully used***

Setup

- 12 VMs
- 4 days of data gathering
- 96 threads per service
  - Except goo.gl
- 4 short URLs inserted in MongoDB per second
- Average traffic:
  - 8,52 Mbit/s out
  - 2,44 Mbit/s in

The numbers

- Approx 1.4 million short URLs encoutered
  - TinyURL: 1,39 million visited.
  - Bitly: +/- 6 K visited.
  - Goo.gl: +/- 4K visited.
- Malware – undetected hits
  - TinyURL: 946
  - Bitly: 2
  - Goo.gl: 0

The numbers (2)

Service	Undetected	Detected	Total	Percentage
TinyURL	946	70,302	71,248	5.17%
Bitly	2	1	3	+/- 0.05%
Goo.gl	0	4	4	+/- 0.01%
Totals	**948**	**70,307**	**71,255**	

asterpix.com

Domain	Count
www.asterpix.com	495
video.asterpix.com	113
www.tagvn.com	75
www.filelodge.com	57
keyknowhow.com	23
hurl.content.loudeye.com	16
static.zangocash.com	14
www.perfectporridge.com	13
www.content.loudeye.com	5
Small counts (<= 4)	137

What is asterpix.com?

- Origins in 2006 as a video sharing site
- Short URLs are created during that period
  - video.asterpix.com/v/<ID>/<Title>/
  - www.asterpix.com/console/?avi=<ID>
- 2009: links and short URLs “die”
- 2015: malware registered

Taxonomy

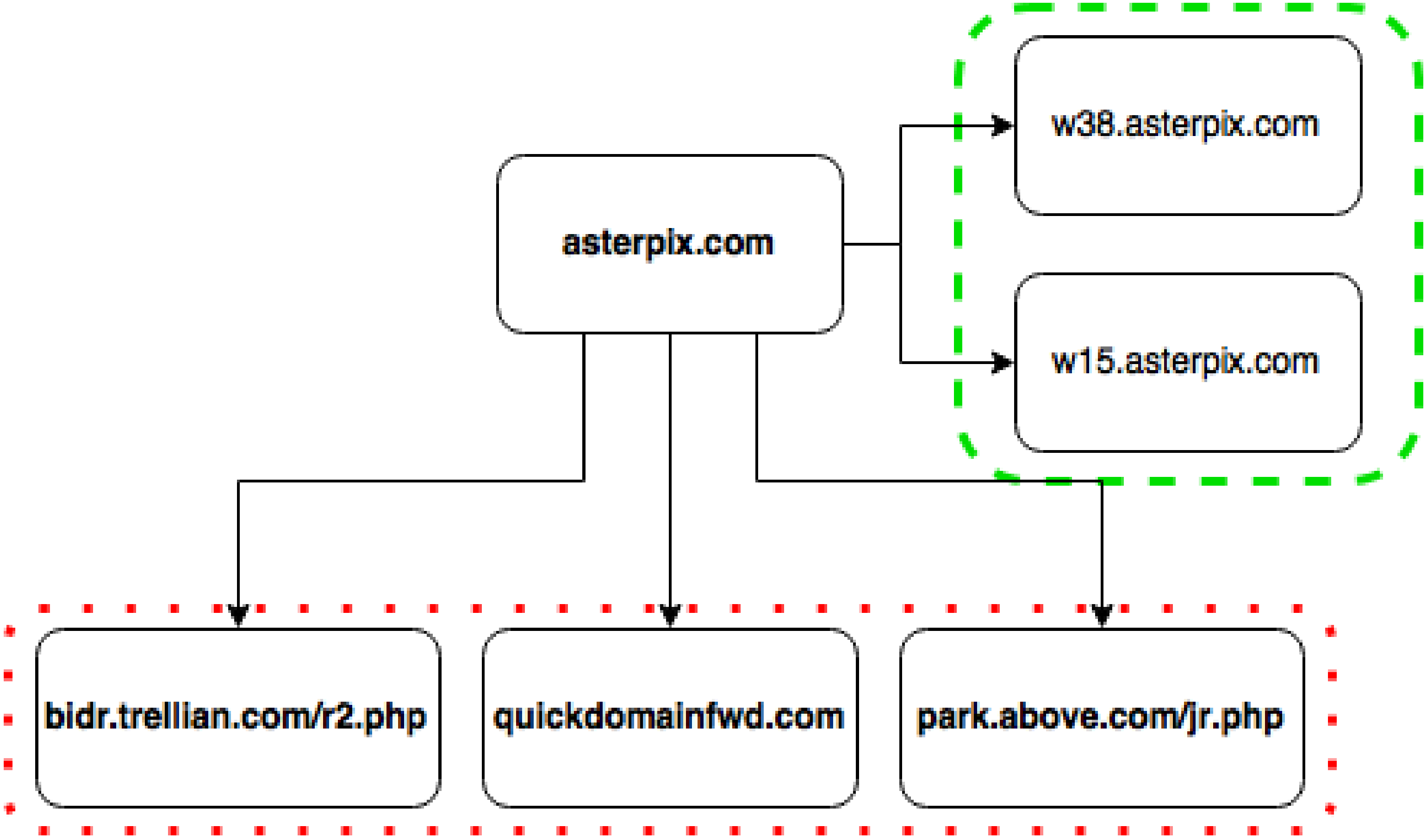
- Encountered a dutch site during first visit.
- How does locality influence redirection?
  - Asia
  - America
  - Europe
- Three phases
  - Entry
  - Redirection
  - Hand off

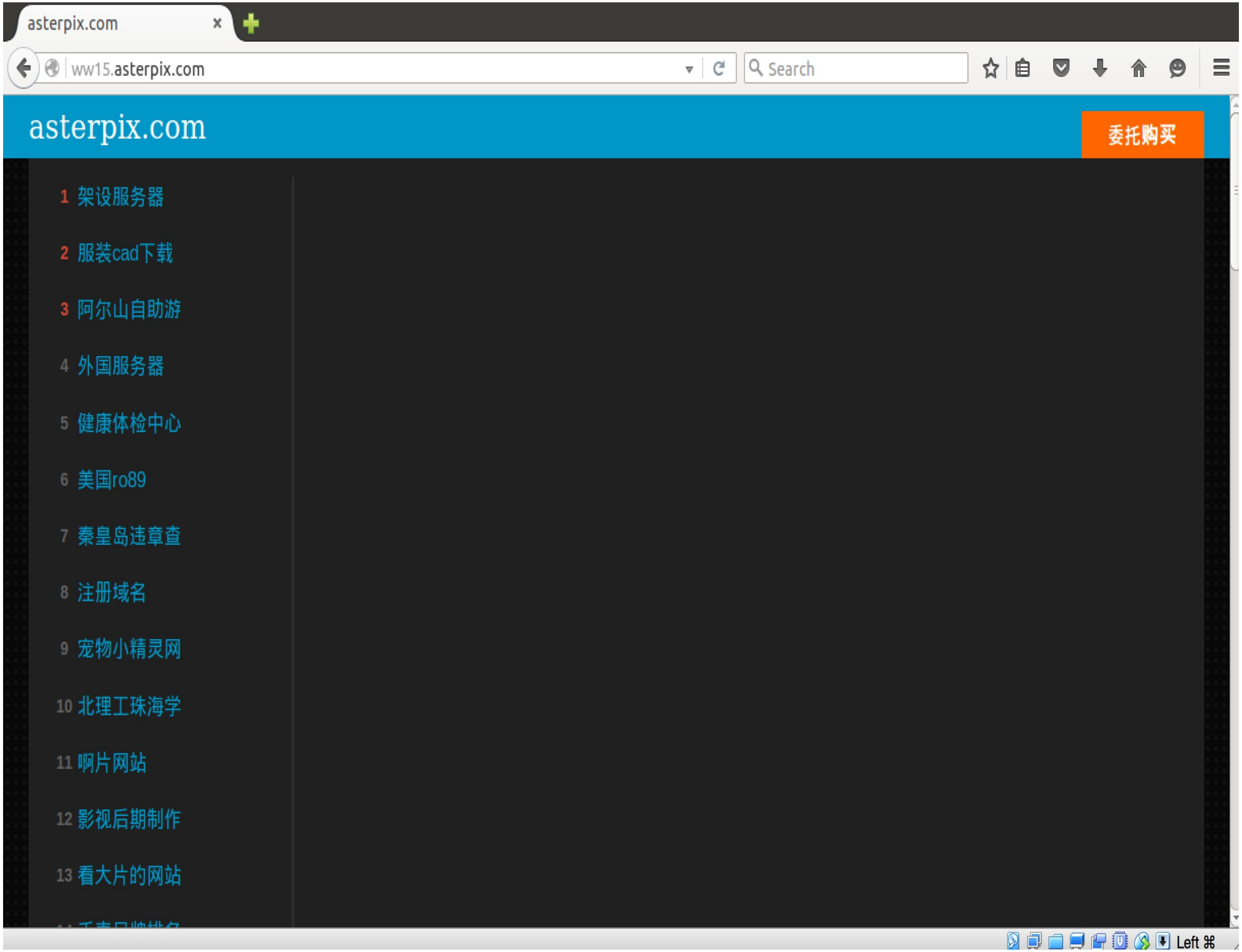
The phases

- Entry
  - Where is the visitor from?
  - Has he visited in the past?
- Redirection
  - Typical JS redirection to obfuscate paths
  - All over the world and at least 4 hops
  - Depending on location of visitor
- Hand Off
  - Catered to the visitor in language and offering

What was observed?

- One known entry point
- Two known non malicious landing pages
- Eight known malicious landing pages
  - Surveys
  - “Free” money
  - Vouchers
- Overlapping redirect chains
  - park.above.com
  - bidr.trellian.com
  - z[a-z].zeroredirect.com


asterpix.com
w38.asterpix.com
w15.asterpix.com
bidr.trellian.com/r2.php
quickdomainfwd.com
park.above.com/jr.php



asterpix.com

委托购买

1 架设服务器

2 服装cad下载

3 阿尔山自助游

4 外国服务器

5 健康体检中心

6 美国ro89

7 秦皇岛违章查

8 注册域名

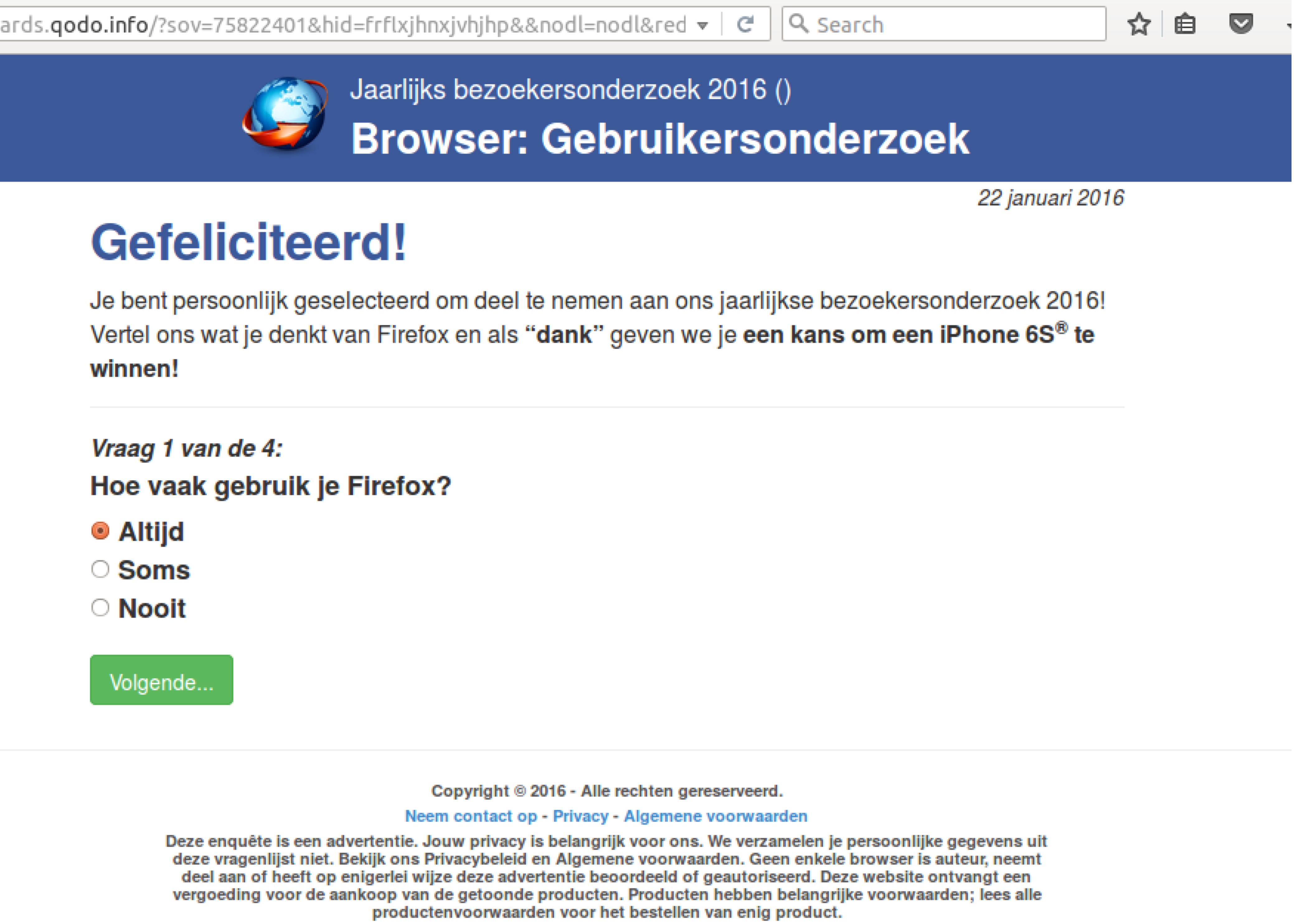
9 宠物小精灵网

10 北理工珠海学

11 啊片网站

12 影视后期制作

13 看大片的网站



ards.qodo.info/?sov=75822401&hid=frflxjhnxjvhjhp&&nodl=nodl&red

Jaarlijks bezoekersonderzoek 2016 ()

Browser: Gebruikersonderzoek

22 januari 2016

Gefeliciteerd!

Je bent persoonlijk geselecteerd om deel te nemen aan ons jaarlijkse bezoekersonderzoek 2016! Vertel ons wat je denkt van Firefox en als **“dank”** geven we je **een kans om een iPhone 6S® te winnen!**

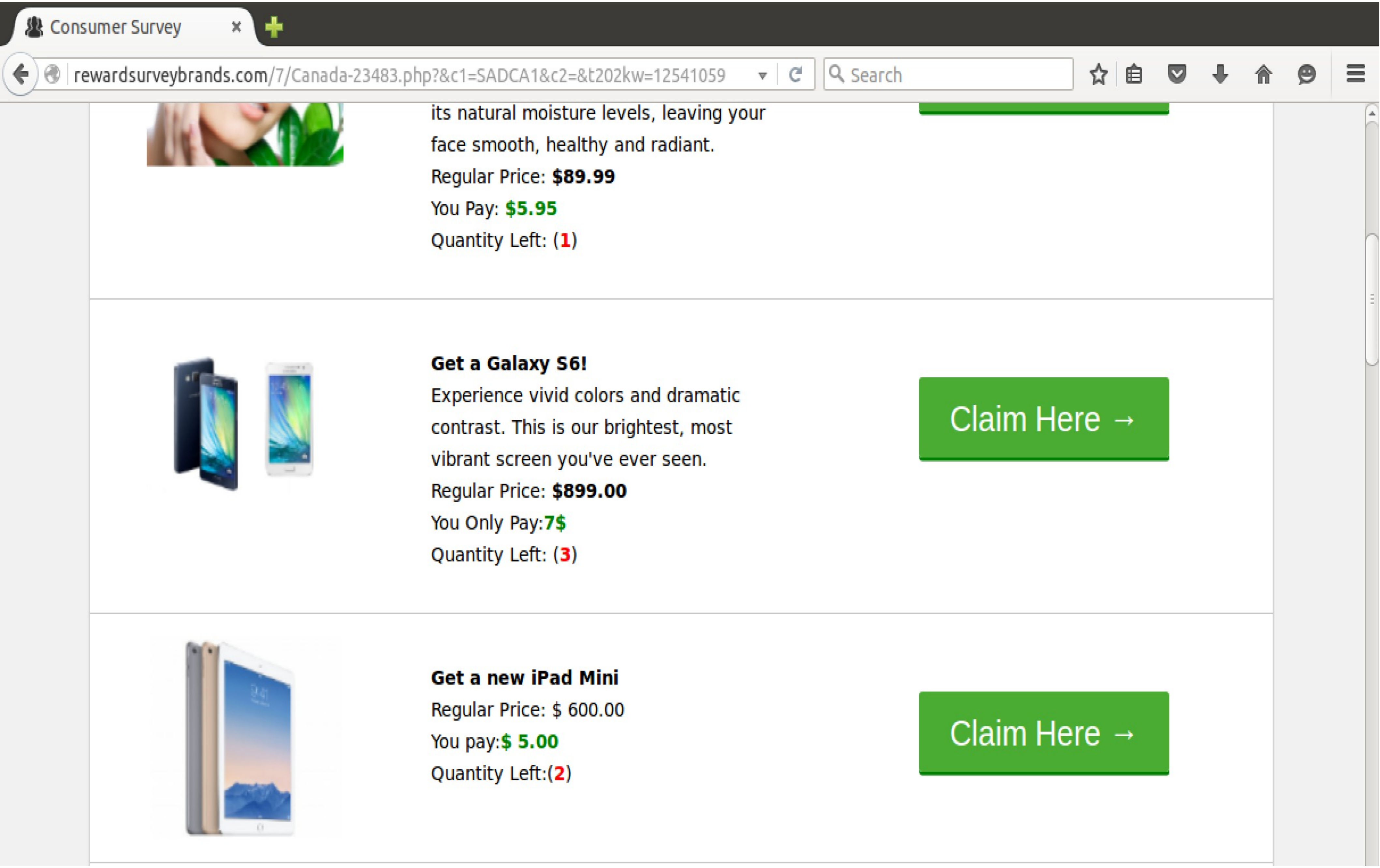
Vraag 1 van de 4:

Hoe vaak gebruik je Firefox?

● **Altijd**
○ **Soms**
○ **Nooit**

Neem contact op - Privacy - Algemene voorwaarden

Deze enquête is een advertentie. Jouw privacy is belangrijk voor ons. We verzamelen je persoonlijke gegevens uit deze vragenlijst niet. Bekijk ons Privacybeleid en Algemene voorwaarden. Geen enkele browser is auteur, neemt deel aan of heeft op enigerlei wijze deze advertentie beoordeeld of geautoriseerd. Deze website ontvangt een vergoeding voor de aankoop van de getoonde producten. Producten hebben belangrijke voorwaarden; lees alle productenvoorwaarden voor het bestellen van enig product.


Consumer Survey
rewardsurveybrands.com/7/Canada-23483.php?&c1=SADCA1&c2=&t202kw=12541059
Search

its natural moisture levels, leaving your face smooth, healthy and radiant.

Regular Price: **$89.99**

You Pay: **$5.95**

Quantity Left: (**1**)

Get a Galaxy S6!

Experience vivid colors and dramatic contrast. This is our brightest, most vibrant screen you've ever seen.

Regular Price: **$899.00**

You Only Pay:**7$**

Quantity Left: (**3**)

Get a new iPad Mini

Regular Price: $ 600.00

You pay:**$ 5.00**

Quantity Left:(**2**)

Conclusion/Discussion

- Significant amount of malicious sites TinyURL
- Undetected rate more or less the same over the services.
- Proportionally more malicious long URLs at TinyURL in total.
- Sites change over time, short URLs remain active
  - Unable to see if this is actively abused
- Locality based redirection observed
  - Block secondary/tertiary redirectors.

Future work

- The “repurposing” of short URLs and its abuse
- The effectiveness of blocking underlying redirectors
- A further case study into locality based adware networks to find commonalities
- Optimization of the search for bitly and goo.gl
- Look into smaller, lesser known providers.