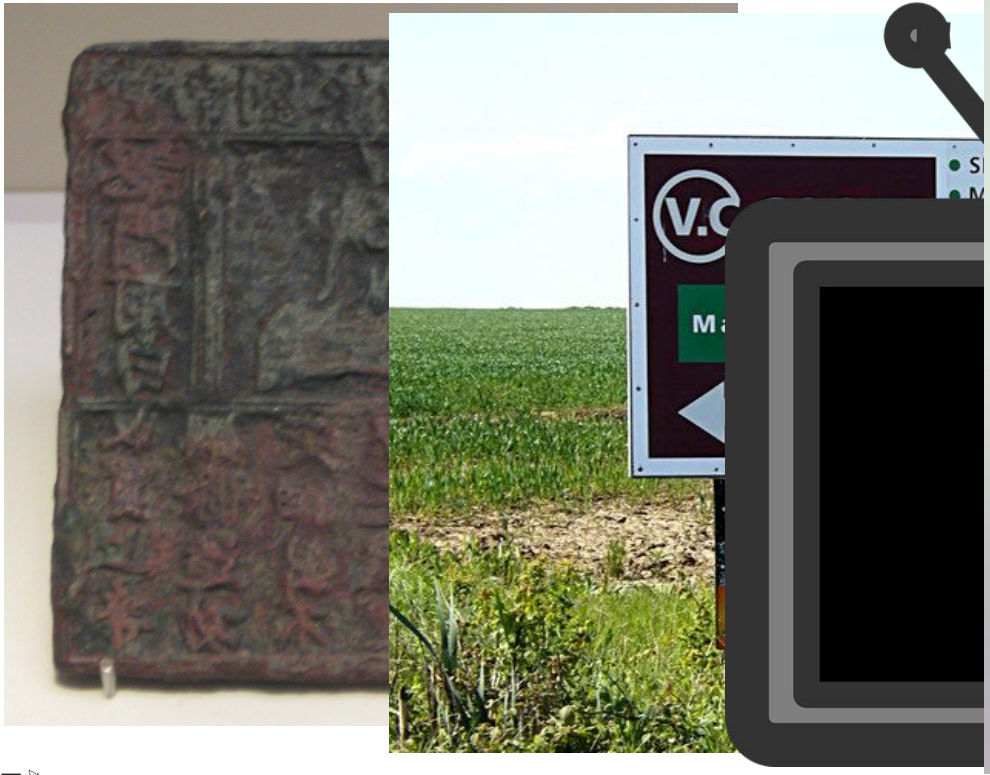
The Good, The Bad, and The Ugly.

Matthieu Faou
Joan Calvet
Pierre-Marc Bureau
Antoine Lemay & José Fernandez

Advertisement...



160 Billion $

World Wide

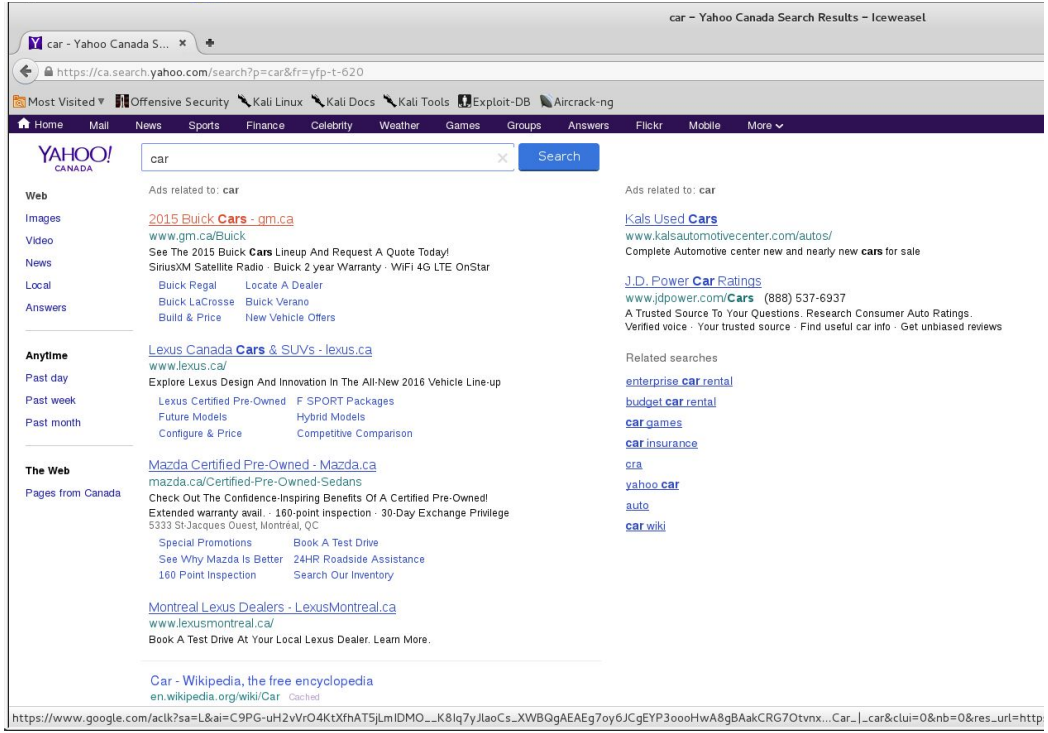
Online Advertising Fraud

- Click fraud.
- Approaches to this problem.
- Suggestions to improve the situation.
- Matthieu Faou’s Master's Thesis at Polytechnique.
- ESET and Dell SecureWorks malware related data.

Presentation Outline

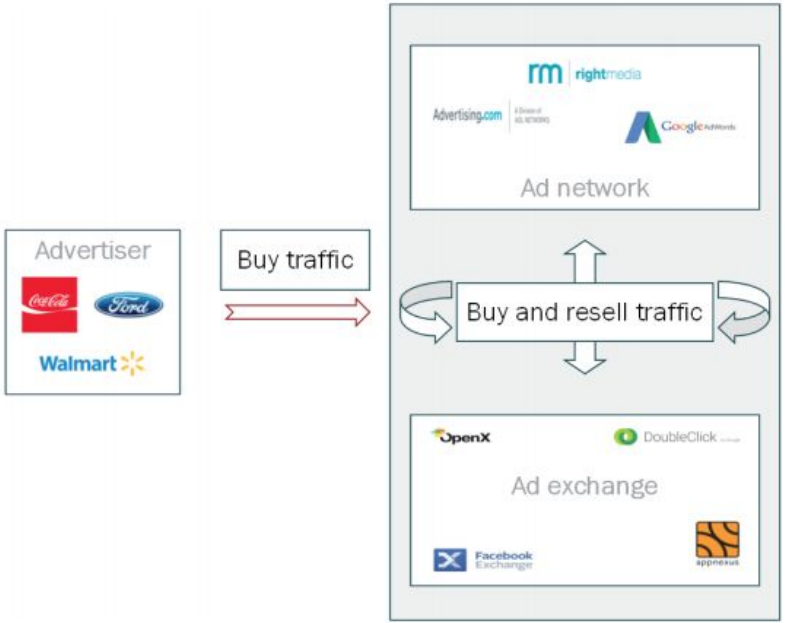
1. Online Advertising
2. Boaxxe
3. Ramdo
4. Data Collection Approach
5. Analysis Technique & Results
6. Disruption Ideas

Online Advertising - Pay Per Click

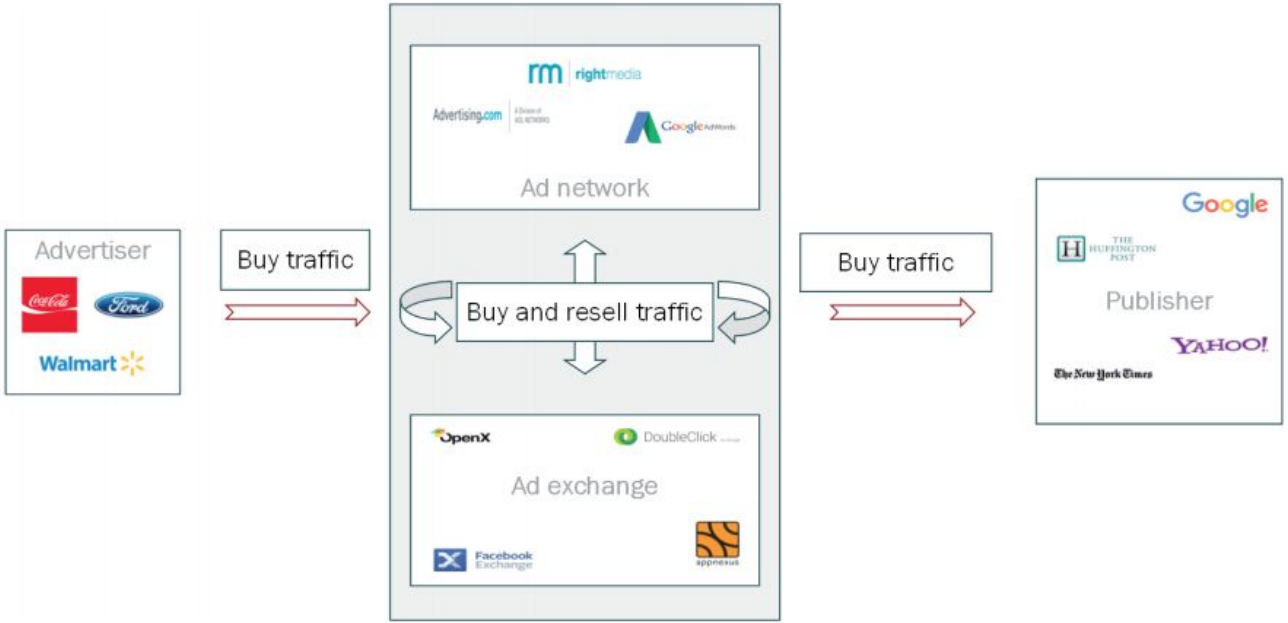


Online Advertising

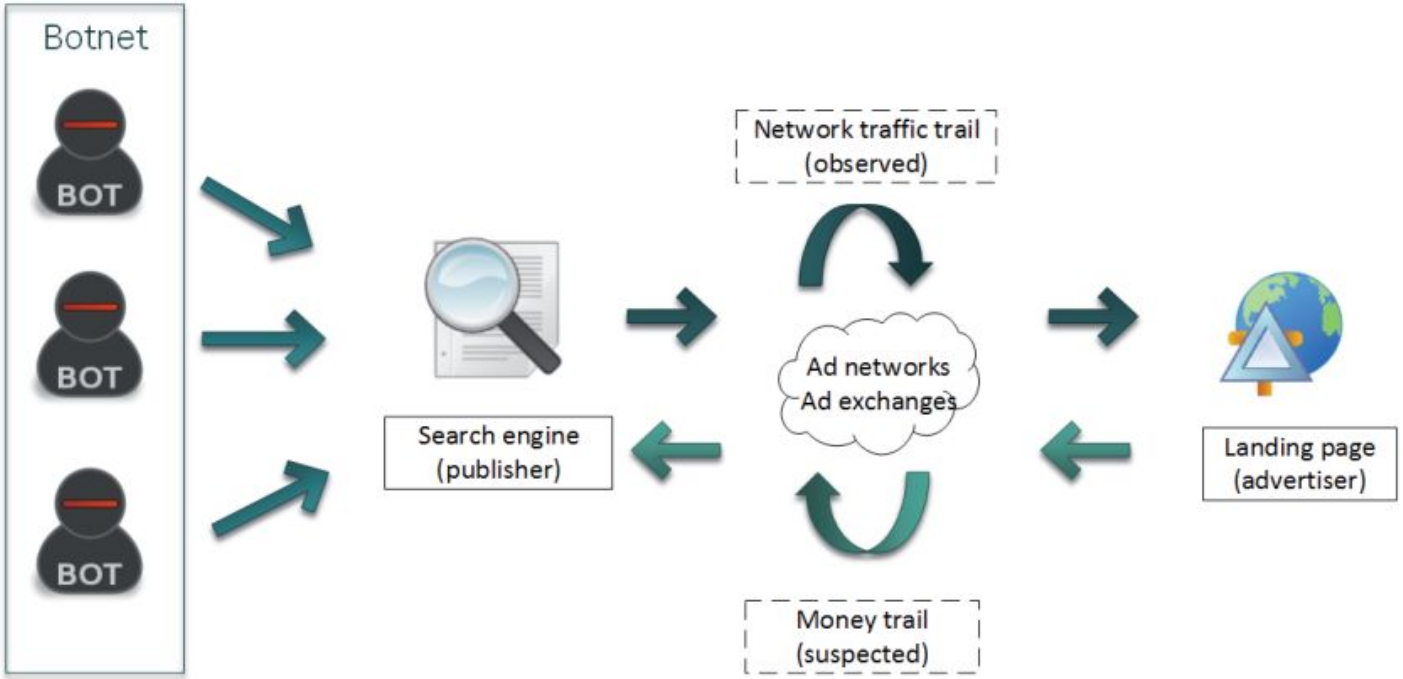
Online Advertising



Online Advertising



Click Fraud


Botnet
BOT
BOT
BOT
Search engine
(publisher)
Network traffic trail
(observed)
Ad networks
Ad exchanges
Money trail
(suspected)
Landing page
(advertiser)

Click Fraud Malware

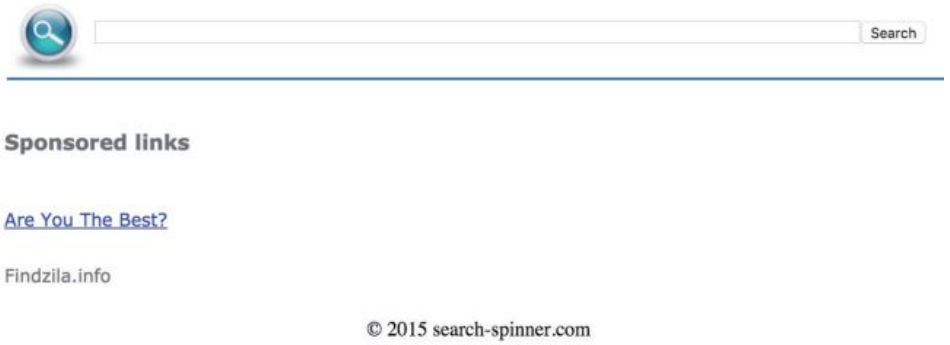
Boaxxe/Miuref

- Operating since 2010
- Installs a Chrome/Firefox extension (search hijacking).
- Performs **automated click fraud** through dummy search engines.
- Uses steganography to decrypt its payload.

http://www.welivesecurity.com/2014/01/14/boaxxe-adware-a-good-ad-sells-the-product-without-drawing-attention-to-itself-pt-1/
http://www.welivesecurity.com/2014/01/17/boaxxe-adware-a-good-advert-sells-the-product-without-drawing-attention-to-itself-part-2/

Ramdo/Redyms

- Operating since (at least) 2013.
- Installed by various exploit packs.
- Uses affiliate program.
- Domain Generation Algorithm.
- Downloads CEF to perform **automated click fraud**.



https://www.secureworks.com/blog/ramdo-click-fraud-malware

Common Characteristics

- Actively developed and maintained.
- Use partnerships for distribution.
- Efforts in avoiding detection and mitigation.
  - Sandbox detection.
  - Code obfuscation.
  - Frequent updates.
- Use web search portal to perform click fraud.

Analyzing the Ecosystem

Data Collection

- Boaxxe
  - Ran a sample in a Virtual Machine
  - Recorded the network traffic
- Ramdo
  - Crawled the search engine with PhantomJS
  - Interception of the redirections

Chain reconstruction

[redacted]	192.168.7.2	HTTP	309 HTTP/1.1 200 OK (text/html)
192.168.7.2	23.250.0.11	HTTP	470 GET /clk2?d=lW3zu7IRUze6BYYIDWRyvtXuVG5tQJiqPPNcn55EKsJhV.GgiREcPbr3TQ5m HTTP/1.1
192.168.7.2	[redacted]	HTTP	497 GET /ajs.php?zid=6423 HTTP/1.1
[redacted]	192.168.7.2	HTTP	173 HTTP/1.1 200 OK (text/javascript)
23.250.0.11	192.168.7.2	HTTP	492 HTTP/1.1 200 OK (text/plain)
192.168.7.2	[redacted]	HTTP	720 GET /wp-content/uploads/2015/08/800px-Audioslave_small-620x319.png HTTP/1.1
192.168.7.2	[redacted]	HTTP	731 GET /wp-content/uploads/2015/08/Dr._Dre_at_Coachella_2012_cropped-300x200.jpg HTTP/1.1
192.168.7.2	[redacted]	HTTP	732 GET /wp-content/uploads/2015/08/Screen-Shot-2015-08-04-at-09.54.39-300x200.png HTTP/1.1
192.168.7.2	[redacted]	HTTP	732 GET /wp-content/uploads/2015/08/Screen-Shot-2015-08-04-at-09.54.39-230x150.png HTTP/1.1
192.168.7.2	[redacted]	HTTP	720 GET /wp-content/uploads/2015/08/800px-Audioslave_small-230x150.png HTTP/1.1
[redacted]	192.168.7.2	HTTP	86 HTTP/1.1 200 OK (JPEG JFIF image)
[redacted]	192.168.7.2	HTTP	1207 HTTP/1.1 200 OK (PNG)
[redacted]	192.168.7.2	HTTP	602 HTTP/1.1 200 OK (PNG)
192.168.7.2	23.250.0.11	HTTP	567 GET /r?q=accepted&subid=z182518056&link=8Ua6BDvwEeWf6AzEegUOMA HTTP/1.1
23.250.0.11	192.168.7.2	HTTP	319 HTTP/1.1 302 Found
192.168.7.2	23.250.0.11	HTTP	536 GET /search?q=accepted&subid=z182518056 HTTP/1.1
23.250.0.11	192.168.7.2	HTTP	722 HTTP/1.1 200 OK (text/html)

A click-fraud chain

Position	URL	Role
1	web-find.org/clk2?d=w4NK8...	Publisher
2	web-find.org/r?q=kungfu4less&subid=...	Publisher
3	web-find.org/search?q=kungfu4less&subid=...	Publisher
4	web-find.org/click?q=kungfu4less&subid=...	Publisher
5	88.214.241.236/click?sid=eef15...	Ad network
6	207.244.71.165/redirect js.php?ht domain=web-find.org...	Ad network
7	207.244.71.165/onclick.php?ht domain=web-find.org...	Ad network
8	207.244.71.165/local bidding/onclick.php?affid=...	Ad network
9	adupmediaxml.com/bid redirect.php?id camp=...	Ad network
10	adupmediaxml.com/header redirect.php?id camp=...	Ad network
11	www.entrepreneur.com/topic/youve-arrived	Advertiser

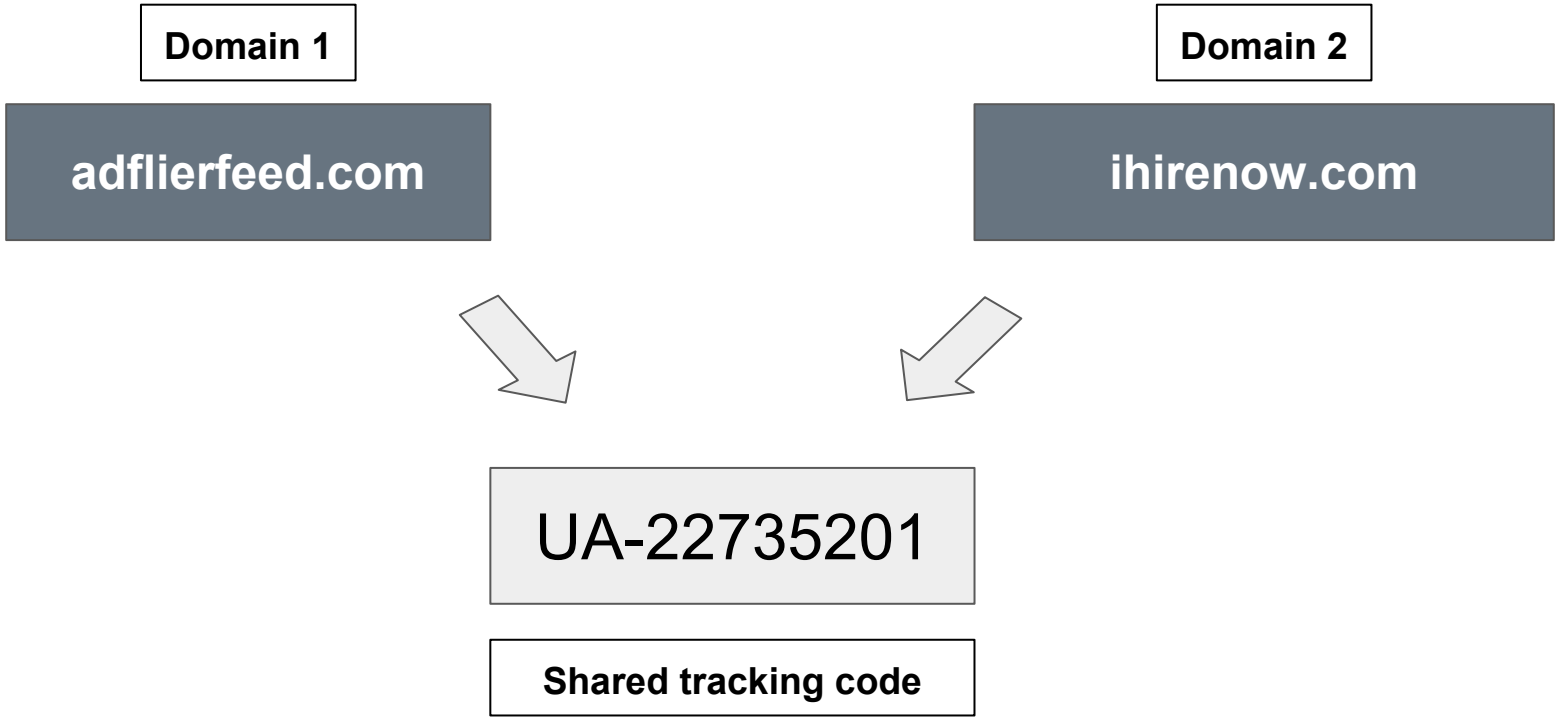
Data Collection

Malware	Boaxxe	Ramdo
# Days	207	54
# Redirection chains	1,380	9,596
# External redirections (from one domain to another domain)	3,218	32,369

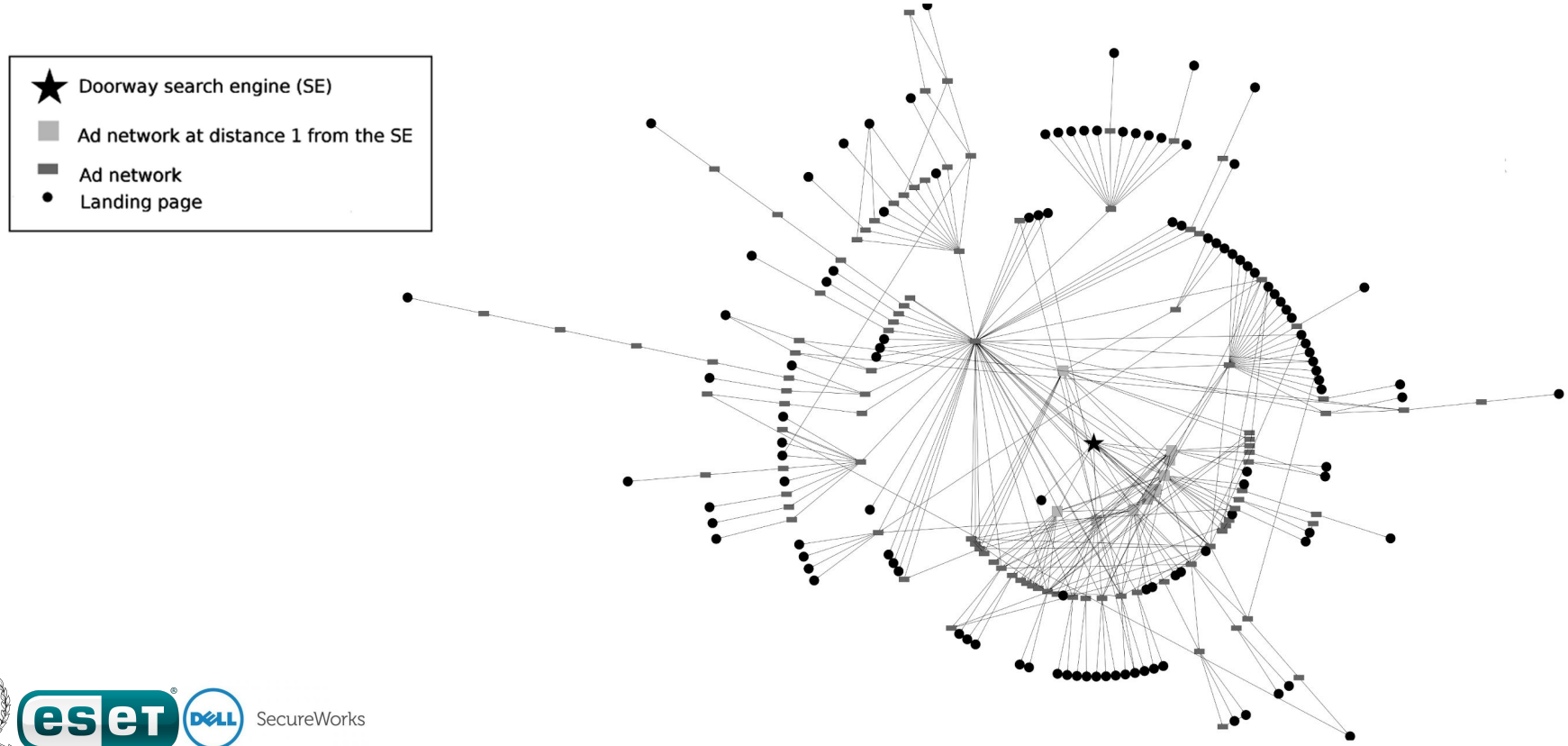
Aggregation

- Redirection chain -> graph of IP addresses and domains
- We did not consider the edge weights.
- IP addresses and domains -> actor
  - Whois
  - Passive DNS
  - **Tracking codes**
  - SSL certificates
  - …

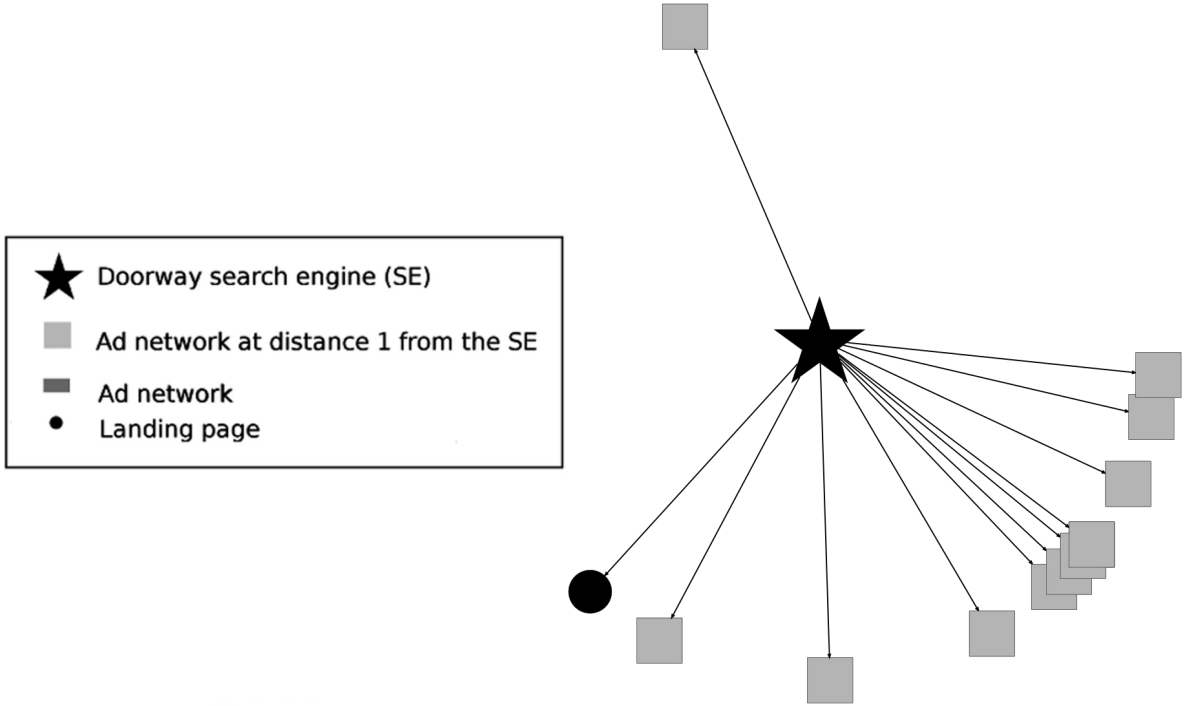
Tracking code



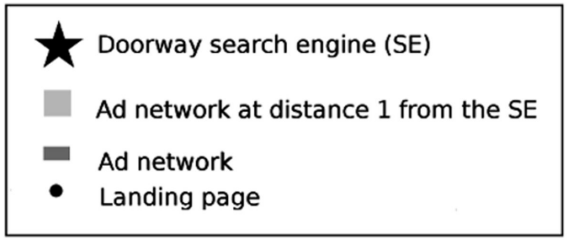
Boaxxe business relationships graph

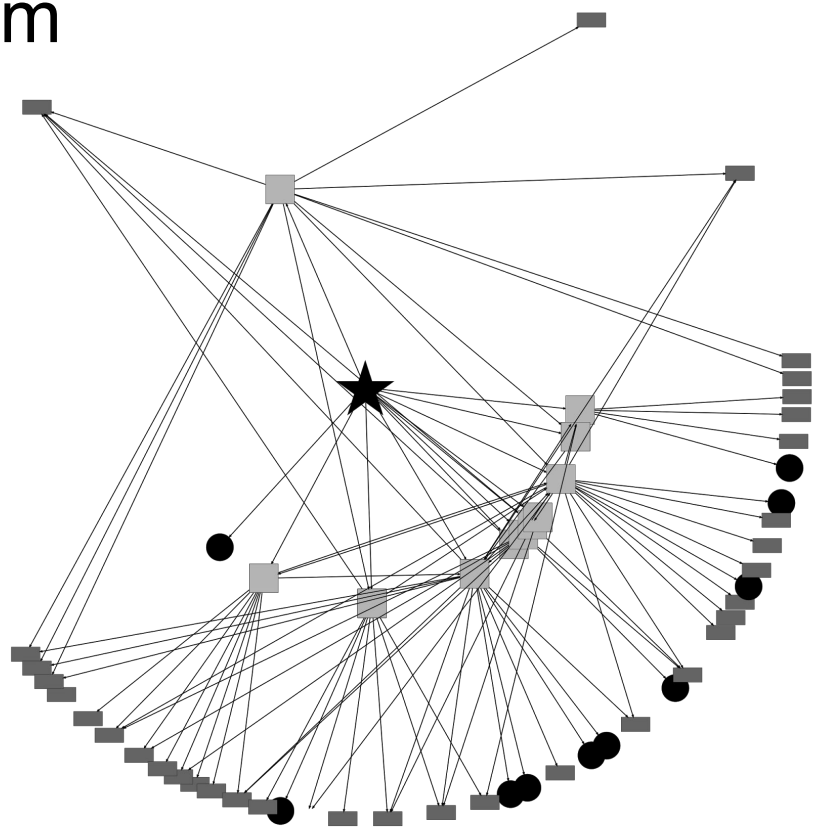


Boaxxe core ecosystem

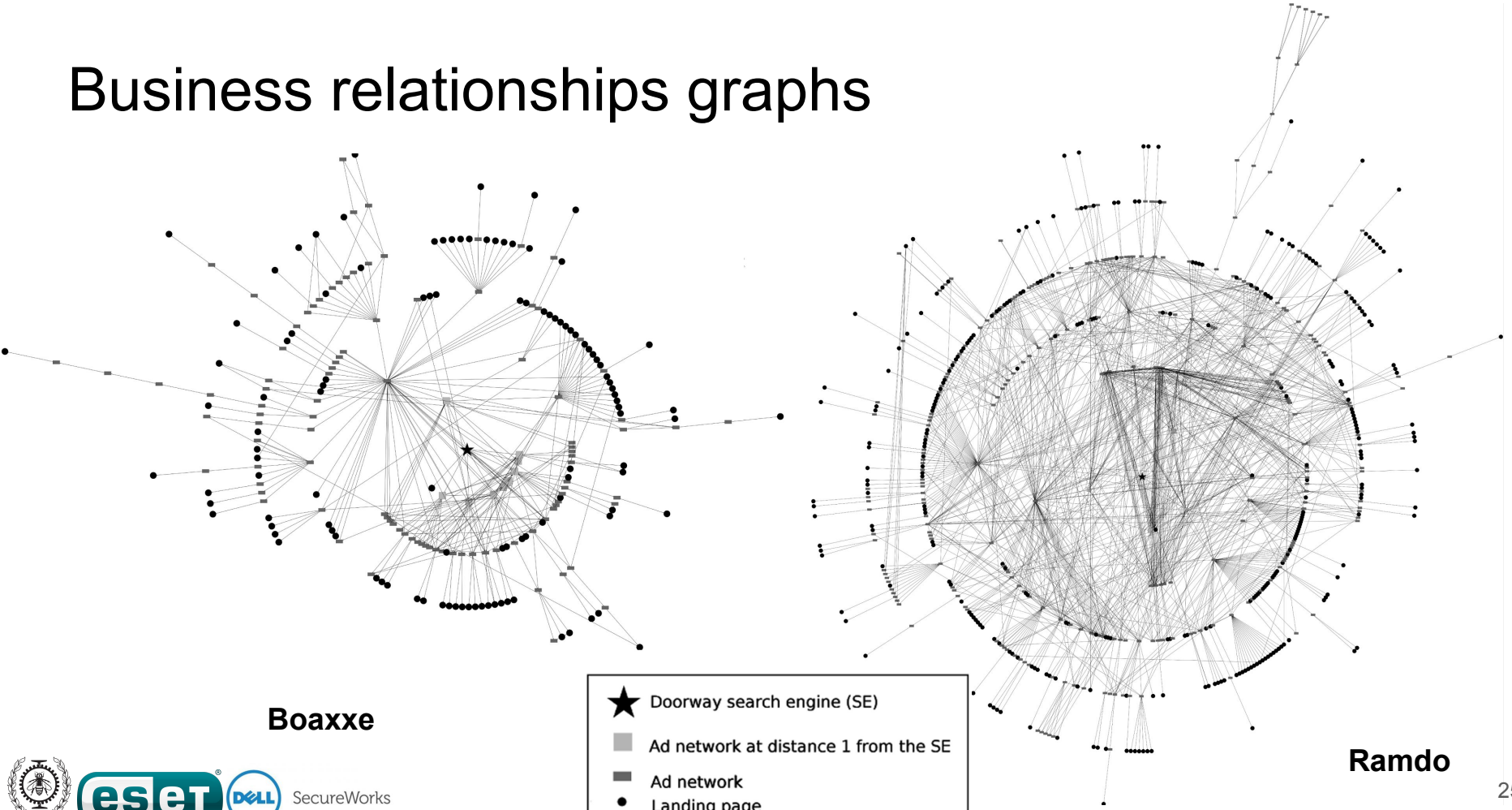


Boaxxe core ecosystem





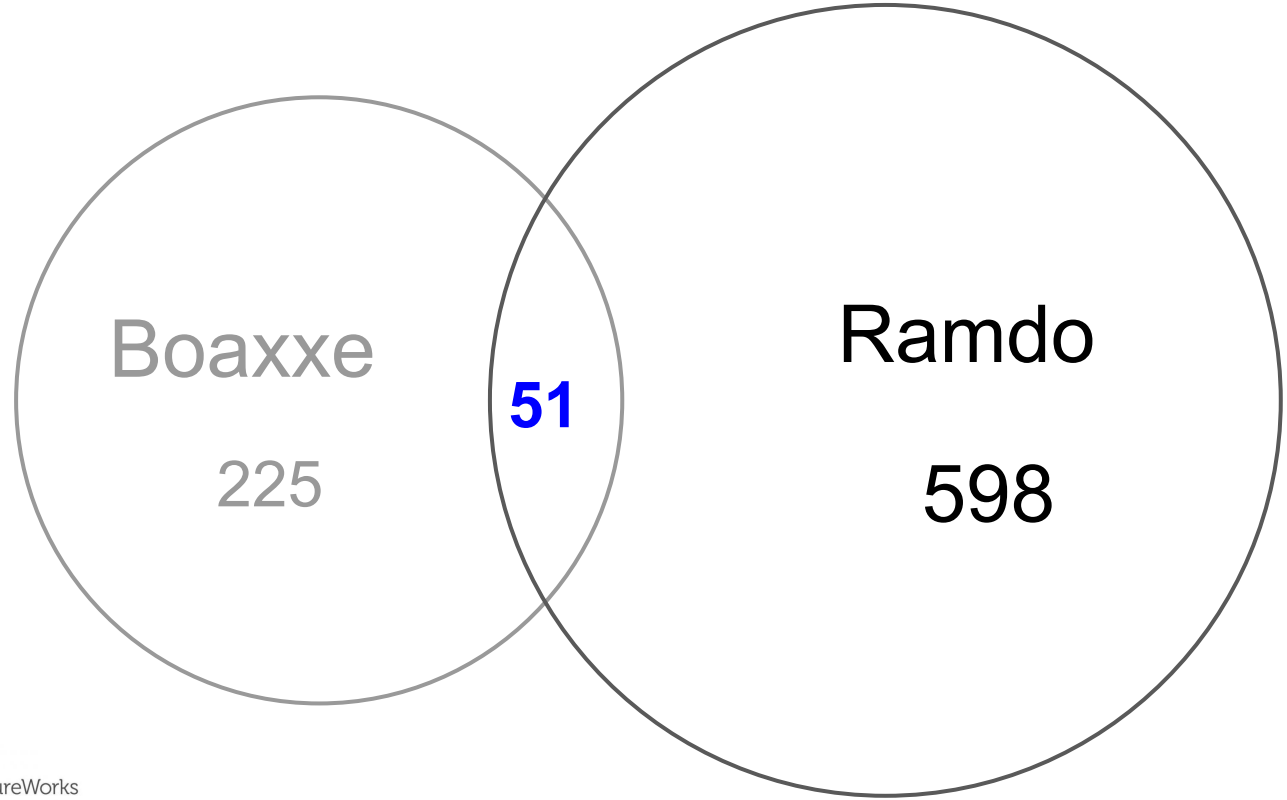
Business relationships graphs



Boaxxe

Ramdo

Ecosystems common actors

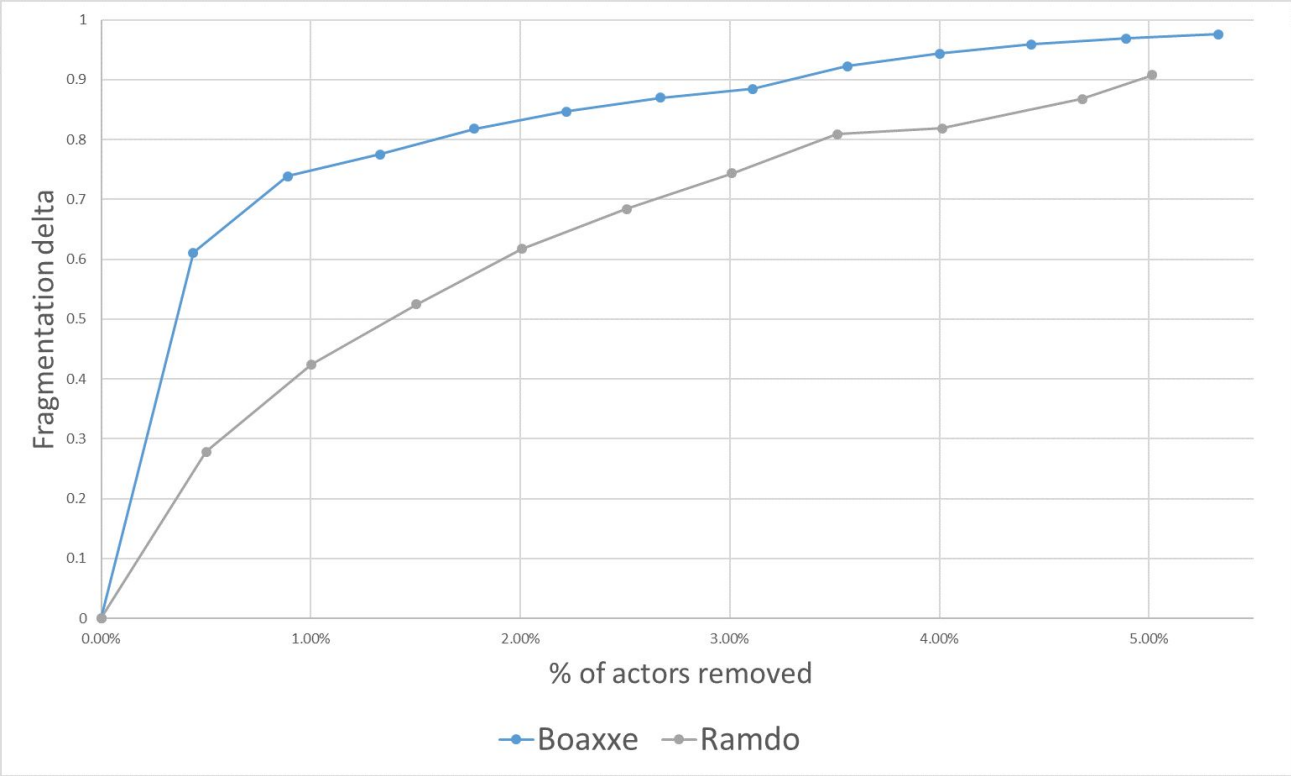


Disruption

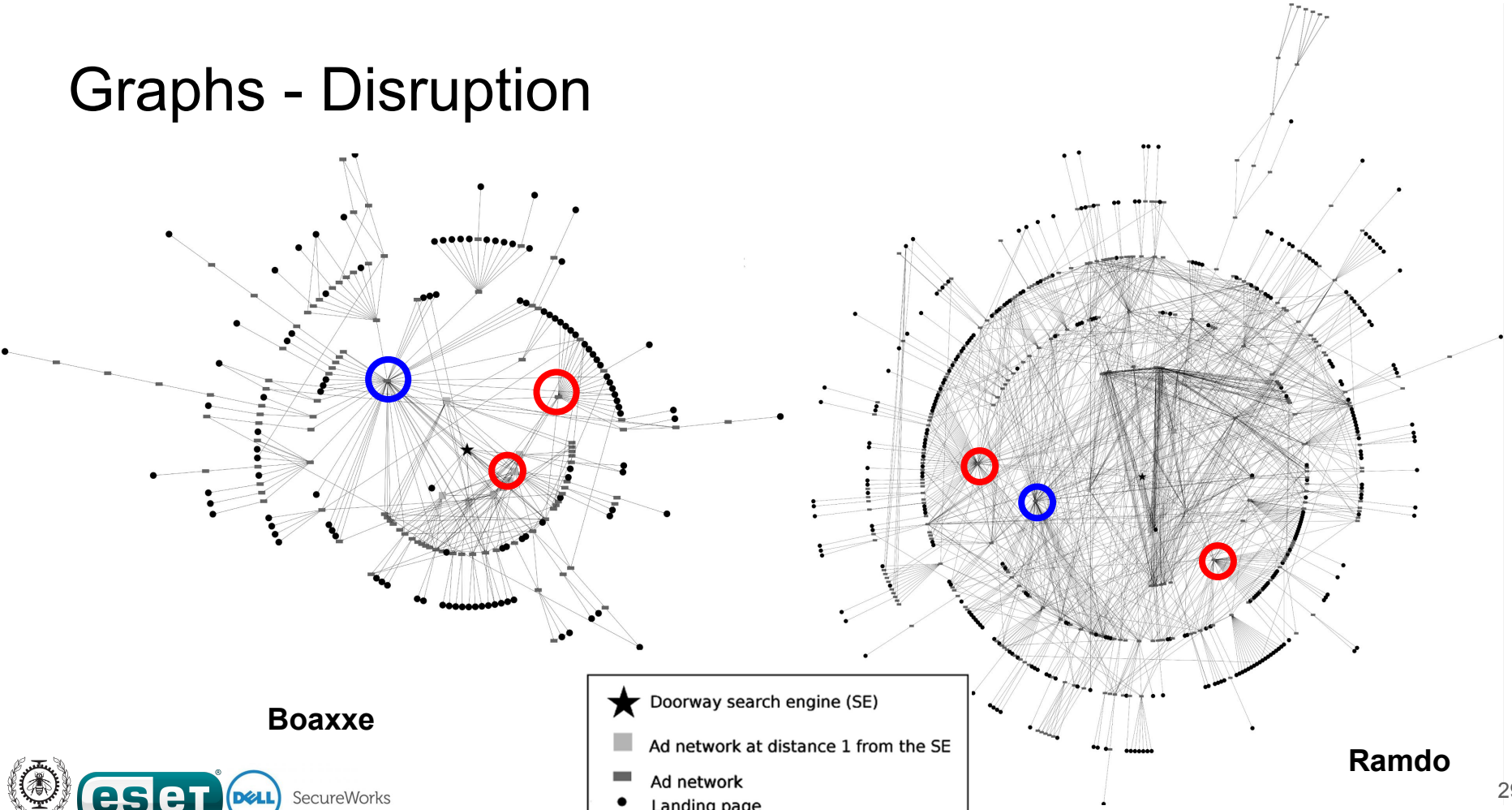
- Breaking paths between the doorway search engine and the advertisers

- Keyplayer (Criminology method)
  - Find the nodes that increase the most the fragmentation of the graph when removed.

Results


Fragmentation delta
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
0.00%
1.00%
2.00%
3.00%
4.00%
5.00%
% of actors removed
Boaxxe
Ramdo

Graphs - Disruption



Boaxxe

Ramdo

Disruption in practice

- Removing a **node** is **not** removing a **company**
- Advertisers can put pressure on their ad network(s)
- Ad exchanges can ban fraudulent ad networks

Conclusions

- Click fraud is a major problem for the advertising industry
- Several malware families uses the same intermediaries to perform click fraud
  - send us PCAPs from other click-fraud malware families!
- Removing a limited number of nodes can disrupt the fraudulent ecosystem.

Acknowledgement

- David Décary-Hétu et Benoît Dupont from the Criminology department of the University of Montréal.
- Polytechnique Montréal security lab (SecSi)
- ESET
- Dell SecureWorks