

Real or Fake?

Activists take down fake business websites in
their fight against Internet fraud

Andreas Zingerle, University of Art and Design, Linz, Austria.
Oct. 23rd, 2015, NET ACTIVISM conference, Rome, Italy.

Andreas Zingerle

- PhD candidate
- Lecturer HCI at university of Art and Design, Linz, Austria.
- Media artist working in the field of Interactive installation and topics of Internet crime and HCI.
- Together with Linda Kronman → kairus.org

Overview

- Fake websites everywhere!?
- Activist strategies against fake websites
- Art installation “Megacorp.”
- Creative media competence training
- Q & A

Research into vigilante communities
and net activist groups who fight
against Internet fraud

Fake websites everywhere?

- 20% of the Web is fake (Gyongyi and Garcia-Molina 2005).
- 70% of “.biz” and
- 35 % of “.us” domain pages are fake (Ntoulas et al. 2006).
- 85% of phishing websites are registered “.cn”

Reserch motivation

- “Artists against 419” (aa419) activists & database visit the page and see what sort of 'new' companies were added each day.
- After a while you start seeing similar companies reappear again and you start reading the forums.
- Dig deeper into anti-scam activism practices
- Research for an visualisation: No visualization or artwork found that deals with fake websites.

Research questions

- How do these fake websites look like? Clones of existing websites vs. 'real fake' businesses
- Are there patterns depending on countries or industry branches?
- How are the fake websites detected?
- Why is this done by vigilante communities?
- Do they follow certain ethics or moral strategies?

Observation of AA419

artists against 419

- ◆ main site
- ◆ blog
- ◆ forum
- ◆ contact us

fake site database

- your account
- ◆ register

ARTISTS AGAINST 419

| 100% risk free ...



Fake Sites Database

DISCLAIMER: artists against 419 ("aa419") identifies fraudulent websites and makes this data available as a public service. We discourage any form of communication with these websites. If you chose to communicate with them you do so at your own risk.

The publicly available whois information listed in the aa419 database was accurate on the date that the website information was entered into the aa419 database. Inclusion in our database does not necessarily indicate criminal activity on the part of the registrant, host or any affiliated companies or individuals.

All data is provided for your personal information only. aa419 and its members shall not be liable for any errors in the database or for any actions taken in reliance thereon.

Quick Search (*) [Show all](#) [Advanced Search](#)

☒ Exact phrase ☐ All words ☐ Any word

[1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [11-20](#) [Next](#)

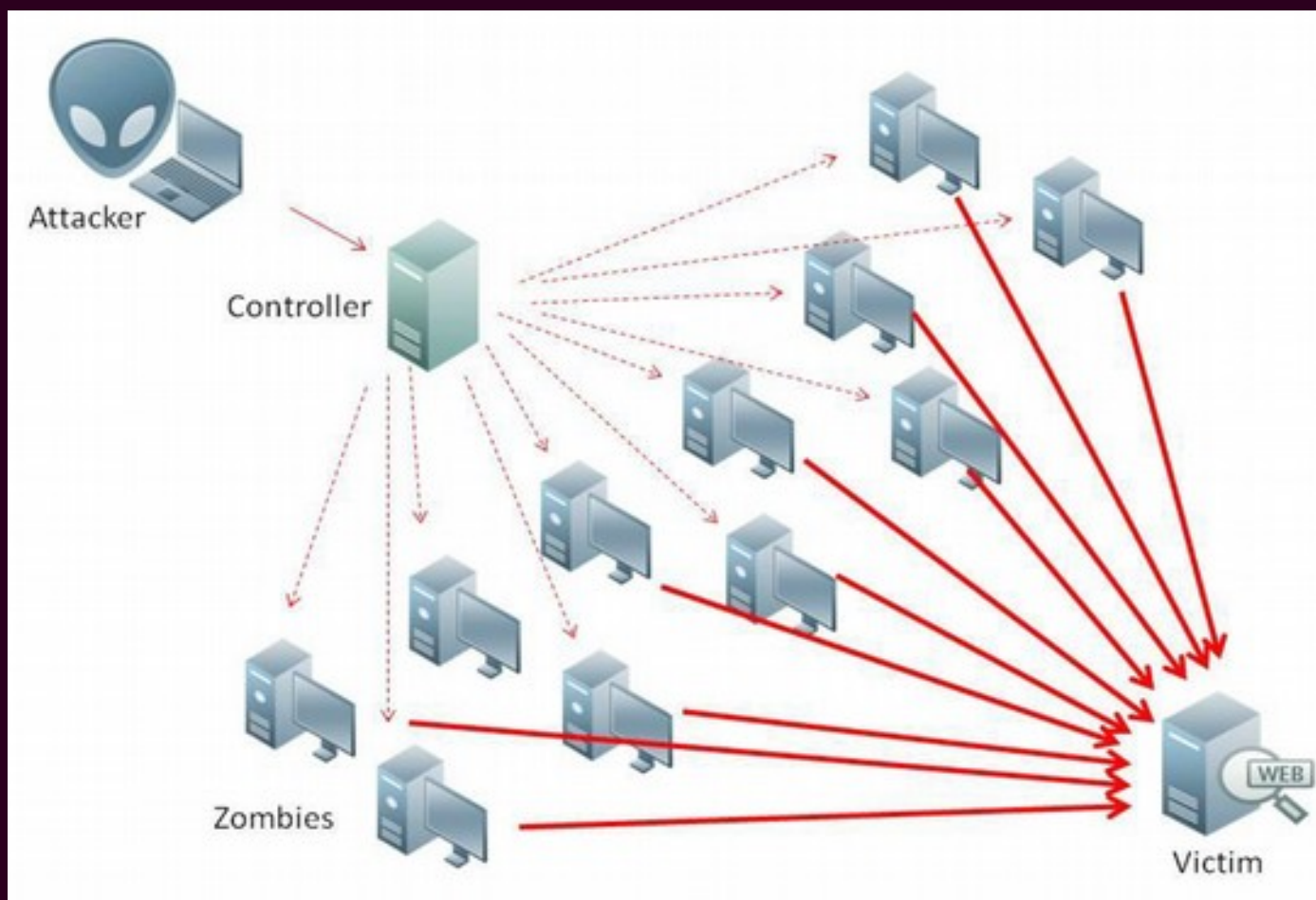
Records 1 to 20 of 104292

Url	Site Name	Status	Date Added (down)	Updated
http://www.brdexpress.com	Border Express	active	2015-09-30 15:10	2015-09-30 15:10
http://www.vehicles-store.com	Vehicles Store	active	2015-09-30 15:09	2015-09-30 15:09
http://www.churchhilltrust.com	Churchhill Trust Bank	active	2015-09-30 02:59	2015-09-30 02:59
http://www.apclogistic.net	APC Freight Courier	active	2015-09-30 02:32	2015-09-30 02:32
http://www.highlandglobaltradingptyltd.com	High Land Global Trading PTY LTD	active	2015-09-30 02:25	2015-09-30 02:25
http://www.ut-gh.com	UT Bank Ghana	active	2015-09-30 02:19	2015-09-30 02:19
http://www.a-shipping.co.za	Alert Shipping Services	active	2015-09-30 00:20	2015-09-30 00:20
http://www.ashippingltd.com	Alert Shipping Services	active	2015-09-29 23:37	2015-09-29 23:37
http://www.opalsecurities.com	Opal Securities Ltd	active	2015-09-29 23:17	2015-09-29 23:17
http://www.chemworldshipping.com	Chem World Shipping	active	2015-09-29 23:15	2015-09-29 23:15
http://www.fidelitybankltd.com	Fidelity Bank	active	2015-09-29 21:31	2015-09-29 21:31
http://www.glostrustint.com	GTINT'L	active	2015-09-29 21:20	2015-09-29 21:20
http://www.pmkpaperline.com	Paper Mill & Kraft Company	active	2015-09-29 21:08	2015-09-29 21:08
http://www.unitedexservice.com	United Express Courier Service	active	2015-09-29 21:05	2015-09-29 21:05

40-50 websites added per day, about 105.000 db entries since 2005-11-03, 4856 users

Old tactics

- 'Bandwidth hogging' and DDos attacks



Self programmed software called “Muguito” and “Lad Vampire”, discontinued 2007

Present tactics

- Collect evidence and information about the fake website that proves that it is a fake business or at least raises certain suspicion
- Write complaint letters to hosting providers
- Maintain good relations to hosting providers and law enforcement.

Open Source Intelligence Tools

- AA419 members use OSIT to collect evidence:
 - 'Whois' and DNS Entries
 - contact the 'official' website owner
 - crawl the web for copies of the website
 - check if the company is registered in this country
 - visit the physical addresses to see if a company is located there.

Domain Whois Lookup

- Do a whois lookup to see who owns the domain
- The result will tell you the registrar (company that the domain was purchased through), when it was created, when it expires as well as contact details.
- e.g. able to confirm that the domain was owned by a company in China, not the running shoe company located in the U.S.
- Another key observation to look for is how long the domain has existed. If it has been active for less than a year, then it is most likely a scam website.



DOMAINS ▾

HOSTING ▾

WEBSITES ▾

andreaszingerle.com registry whois

Domain Name: ANDREASZINGERLE.COM
Registrar: KEY-SYSTEMS GMBH
Sponsoring Registrar IANA ID: 269
Whois Server: whois.rrproxy.net
Referral URL: http://www.key-systems.net
Name Server: DNS0.SERVUS.AT
Name Server: DNS1.SERVUS.AT
Status: ok http://www.icann.org/epp#OK
Updated Date: 27-jan-2015
Creation Date: 11-jul-2008
Expiration Date: 11-jul-2016

andreaszingerle.com registrar whois

Domain Name: andreaszingerle.com
Registry Domain ID: 1507699390_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.rrproxy.net
Registrar URL: http://www.proserver1.at
Updated Date: 2015-01-27T19:09:30.0Z
Creation Date: 2008-07-11T11:55:23.0Z
Registrar Registration Expiration Date: 2016-07-11T11:55:23.0Z
Registrar: Key-Systems GmbH
Registrar IANA ID: 269
Registrar Abuse Contact Email: **abuse@key-systems.net**
Registrar Abuse Contact Phone: +49.68949396850
Domain Status: ok http://www.icann.org/epp#ok
Registry Registrant ID:
Registrant Name: Treuhand Account Peter Vratny
Registrant Organization:
Registrant Street: Welser Strasse 91
Registrant City: Pettenbach
Registrant State/Province:
Registrant Postal Code: 4643
Registrant Country: AT
Registrant Phone: +43.1236605060
Registrant Phone Ext:
Registrant Fax:

Contact information

- Is there a way to get in touch with someone?
- Is the contact email using the TLD or is it a free email service? (gmail, hotmail)
- Is it a valid address? Can I find the address through OSM, Google.maps, etc.
- If there is a phone number provided, is it a valid number? Does the country code fit the address? Can I find the phone number in a phone book? Can I call there during their business hours?

SSL (Secure Socket Layer)

- Many fake or fraudulent sites will not bother to buy an SSL (Secure Sockets Layer) certificate.
- SSL certificates secure the transfer of your data when you submit sensitive information (creating an account, or submitting payment info) and cost money.
- A scam site, quite often, won't bother with an SSL certificate, as the site will likely be shutdown within a couple months after the fraud has been reported.



UniCredit Bank Austria AG (AT) | <https://online.bankaustria.at/wps/portal/userlogin>

HOME PAGE

ABOUT US

SERVICES

CLIENTS

TESTIMONIALS

CAREERS

CONTACT

Be Successful
WITH US!



Inspector Console Debugger Style Editor Performance Network

html > body#page > div.light > div.container_24 > div.wrapper > div.grid_24 > header > div.wrapper.indent-bottom > h1 > a

```
<!DOCTYPE html>
<html lang="en">
<!-- Mirrored from sunexsolutions.com/?p=index by HTTrack Website Copier/3.x [XR&C0'2013], Fri, 10 Oct 2014 22:40:18 GMT -->
</html>
<body id="page">
  <div class="light">
    <div class="container_24">
      <div class="wrapper">
        <div class="grid_24">
          <!-- ***** header ***** -->
          <header>
            <div class="wrapper indent-bottom">
```

ARTISTS AGAINST 419

| 100% risk free ...



[artists against 419](#)
[main site](#)
[log](#)
[rum](#)
[contact us](#)
[site database](#)
[account](#)
[register](#)

Fake Sites Database

DISCLAIMER: artists against 419 ("aa419") identifies fraudulent websites and makes this data available as a public service with these websites. If you chose to communicate with them you do so at your own risk.

The publicly available whois information listed in the aa419 database was accurate on the date that the website information was included. Inclusion in our database does not necessarily indicate criminal activity on the part of the registrant, host or any affiliated company.

All data is provided for your personal information only. aa419 and its members shall not be liable for any errors in the data or omissions thereon.

Quick Search (*) [Show all](#) [Advanced Search](#)

☒ Exact phrase ☐ All words ☐ Any word

1

Records 1 to 1 of 1

Url	Site Name	Status	Date Added (down)
 http://www.sunexsolutions.com	Sunex Solutions	dead	2014-10-10 19:25

Copyscape

Search for copies of your page on the web.

Watch the **Video Intro to Copyscape** ^{New!}

PROTECTED BY **COPYSCAPE** DO NOT COPY

Defend your site with a free [plagiarism warning banner!](#)

A lot of the fake sites are found by searching text from known fakers
... or it is possible to find the source – the original – page that has been faked

Tip: Search for copies of a specific page on your site by entering its URL.

Only top 10 results shown for **Start-Office, Inc.** Click a result below to see the matching content.

 Share this page...



Do you buy content?

Check if it's original before you purchase with [Copyscape Premium](#).

Want Copyscape alerts?

[Copsentry](#) monitors the web and emails you when new copies are found.

Got a large website?

Check up to 10,000 pages in a single click with [Premium](#) batch search.

New! Check www.start-office.biz for internal duplicate content and more with [Siteliner](#).

[Regus Portland, OR | LinkedIn](#)

... Our products and services allow our customers to concentrate on their core business, and use their talents to best effect. Be they the largest global corporate or an entrepreneur with an idea, we help them be more flexible, more cost-effective and more agile – and better able to face the
<https://www.linkedin.com/pub/regus-portland-or/104/5b7/410>

[Services : GettheOffice](#)

... Our products and services allow our customers to concentrate on their core business, and use their talents to best effect. Be they the largest global corporate or an entrepreneur with an idea, we help them be more flexible, more cost-effective and more agile – and better able to face the
<http://gettheoffice.com/services.html>

[Our Products & Services - Regus USA](#)

... Our products and services allow our customers to concentrate on their core business, and use their talents to best effect. Be they the largest global corporate or an entrepreneur with an idea, we help them be more flexible, more cost-effective and more agile – and better able to face the
<http://www.regus.com/about-us/our-products-and-services.aspx>

[Start-Office, Inc.](#)

... Welcome! Create a business presence anywhere you want to be - Virtually. Our products and services allow our customers to concentrate on their core business, and use their talents to best effect.
<http://pinkomote.com/>

[lance portland profiles | LinkedIn](#)

... we help them be more flexible, more cost-effective and more agile – and better able to face the unexpected challenges of business in the 21st century. Offices Office space on
<https://www.linkedin.com/pub/dir/lance/portland>

[Regus USA Coupon September 2015 | Businessworld from \\$59](#)

... Regus help you be more flexible, more cost-effective and more agile - and better able to face the unexpected challenges of business in the 21st century.
<http://www.promopro.com/merchant-Regus-USA-coupons-deals-17242.html>

File a report

- host is responsible for physically hosting the site / email addresses
- registrar is responsible for the domain name registration
- Look for other possibilities to warn other people and potential victims.



Internet-Falle melden

Was mit Ihrer Meldung geschieht:

Nachdem Ihre Meldung bei uns eingegangen ist, wird sie von unserem Team überprüft und entschieden, ob ein Artikel dazu verfasst wird. Wir bitten um Verständnis, dass die Watchlist Internet **keine Beratung oder Weiterverfolgung** zu einzelnen Betrugsfällen oder Internet-Fallen anbietet. Für Beratungsanfragen wenden Sie sich bitte an den [Internet Ombudsmann](#) bzw. für Betrugsanzeigen direkt an die Polizei.

Meldung

Name*

Ihr Name

Dieses Feld muss ausgefüllt werden!

E-Mail*

Ihre E-Mail-Adresse

Keine gültige E-Mail-Adresse!

Beschreibung

**Informieren Sie uns
über aktuelle Fallen
im Netz!**

[Internet-Falle melden](#)

[Beratung & Hilfe](#)

[Wie mache ich eine Anzeige?](#)

[Newsletter abonnieren](#)

**Tipps und
Informationen zu
den Themen**

Abo-Fallen 55

Facebook-Betrug 43



Welcome to Scamwarners 

HOME 
The Main stuff

FORUM 
See the trends

SEARCH 
Search it up

LOGIN 
Hang around

REGISTER 
Join the club

HOME

This is the forum index page























It is currently Wed Sep 30, 2015 11:20 am

GENERAL TOPICS

STATISTICS

LAST POST

 Welcome to ScamWarners Learn about us and introduce yourself	493 Topics 3235 Posts	 by kzleadshine   Thu Sep 17, 2015 8:29 am
 News and announcements What's new in the world of scams and ScamWarners.	670 Topics 1149 Posts	 by James   Mon Sep 28, 2015 3:37 pm
 An Introduction to scams An overview of the main types of scam we deal with and the basics of how to avoid being a victim of a scam.	22 Topics 33 Posts	 by AlanJones   Mon Feb 17, 2014 5:03 pm
 Help! Is this a scam? What should I do? - Victim Support HAVE QUESTIONS? - ASK FOR HELP HERE - Have you received an email you aren't sure about? Are you currently corresponding with someone you suspect is a scammer? Do you have questions about a scam? Post here for answers and advice.	2314 Topics 16068 Posts	 by vonpaso xlura   Wed Sep 30, 2015 6:32 am
 I've received a warning. Is it real? If you have received a warning from someone claiming to be a ScamWarner and want to check if it is genuine, please ask here.	76 Topics 235 Posts	 by Bill F   Tue Jul 28, 2015 10:59 am

www.scamwarners.com


[artists against 419](#)

[main site](#)
[blog](#)
[forum](#)
[contact us](#)

[fake site database](#)

[your account](#)
[register](#)

Fake Sites Database

DISCLAIMER: artists against 419 ("aa419") identifies fraudulent websites and makes this data available as a public service. We discourage any form of communication with these websites. If you chose to communicate with them you do so at your own risk.

The publicly available whois information listed in the aa419 database was accurate on the date that the website information was entered into the aa419 database. Inclusion in our database does not necessarily indicate criminal activity on the part of the registrant, host or any affiliated companies or individuals.

All data is provided for your personal information only. aa419 and its members shall not be liable for any errors in the database or for any actions taken in reliance thereon.

Quick Search (*) [Show all](#) [Advanced Search](#)

☒ Exact phrase
 ☐ All words
 ☐ Any word

[1](#)
[2](#)
[3](#)
[4](#)
[5](#)
[6](#)
[7](#)
[8](#)
[9](#)
[10](#)
[11-20](#)
[Next](#)

Records 1 to 20 of 104292

Url	Site Name	Status	Date Added (down)	Updated
http://www.brdexpress.com	Border Express	active	2015-09-30 15:10	2015-09-30 15:10
http://www.vehicles-store.com	Vehicles Store	active	2015-09-30 15:09	2015-09-30 15:09
http://www.churchhilltrust.com	Churchhill Trust Bank	active	2015-09-30 02:59	2015-09-30 02:59
http://www.apclogistic.net	APC Freight Courier	active	2015-09-30 02:32	2015-09-30 02:32
http://www.highlandglobaltradingptyltd.com	High Land Global Trading PTY LTD	active	2015-09-30 02:25	2015-09-30 02:25
http://www.ut-gh.com	UT Bank Ghana	active	2015-09-30 02:19	2015-09-30 02:19
http://www.a-shipping.co.za	Alert Shipping Services	active	2015-09-30 00:20	2015-09-30 00:20
http://www.ashippingltd.com	Alert Shipping Services	active	2015-09-29 23:37	2015-09-29 23:37
http://www.opalsecurities.com	Opal Securities Ltd	active	2015-09-29 23:17	2015-09-29 23:17
http://www.chemworldshipping.com	Chem World Shipping	active	2015-09-29 23:15	2015-09-29 23:15
http://www.fidelitybankltd.com	Fidelity Bank	active	2015-09-29 21:31	2015-09-29 21:31
http://www.glostrustint.com	GTINT'L	active	2015-09-29 21:20	2015-09-29 21:20
http://www.pmkpaperline.com	Paper Mill & Kraft Company	active	2015-09-29 21:08	2015-09-29 21:08
http://www.unitedexservice.com	United Express Courier Service	active	2015-09-29 21:05	2015-09-29 21:05

<http://db.aa419.org/fakebankslist.php>

Idea how to visualize the website

- William Gibsons naming of big evil corporations that want to take over the world as MEGACORP.'s
- Part of Cyberpunk dystopian sci-fi genre

Fictional examples



Real life examples



T OOST INDISCHE MAGAZYN. EN SCHEEPS-TIMMER-WERF.

J. Schellin fecit.

Real life examples

Powering Possibilities

أرامكو السعودية
Saudi Aramco



We do so much more than provide energy to the world. We also grow new businesses, fuel the economy and drive innovation. [Find out more >](#)



The Megacorp. conglomerate



MEGACORP.

TRUST US AND WE WILL EXPAND!



ALL BUSINESS SEGMENTS

- 32.6% LOGISTICS AND TRANSPORT
- 21.9% BANKING AND FINANCE
- 14.2% ONLINE MERCHANDISE AND TRADE
- 6.9% PET SHOPS AND ANIMAL TRANSPORT
- 5.7% CONSTRUCTION AND REAL ESTATE
- 5% NATURAL RESOURCES AND HEAVY INDUSTRIES
- 4.8% LAW AND SECURITY
- 4.3% CONSULTING AND RECRUITMENT
- 2.8% PUBLIC AND GOVERNMENT INSTITUTIONS
- 1.8% OTHER

TOP 3 BUSINESS SEGMENTS



LOGISTICS AND TRANSPORT

BY CONTINENT



BANKING AND FINANCE



MEGACORP.



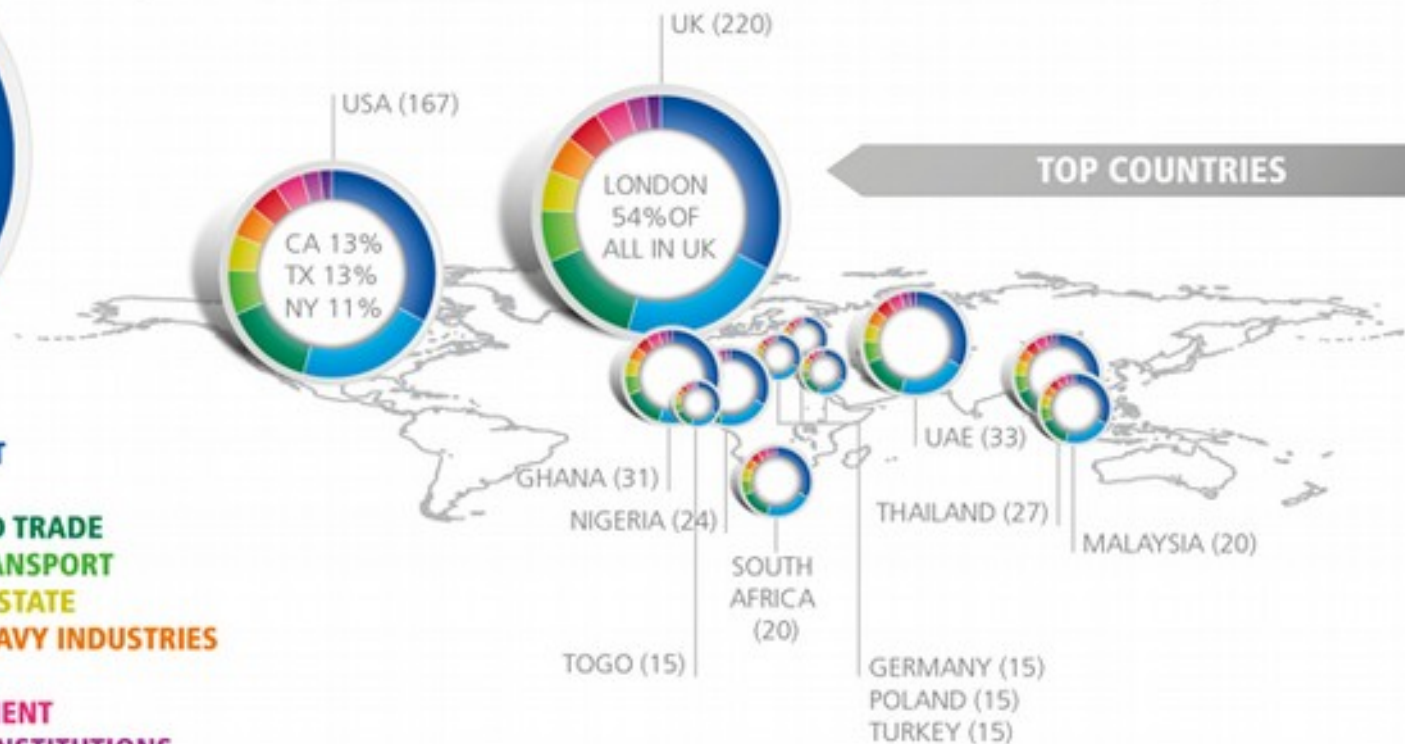
MEGACORP.

ALL BUSINESS SEGMENTS



32.6% LOGISTICS AND TRANSPORT
21.9% BANKING AND FINANCE
14.2% ONLINE MERCHANDISE AND TRADE
6.9% PET SHOPS AND ANIMAL TRANSPORT
5.7% CONSTRUCTION AND REAL-ESTATE
5% NATURAL RESOURCES AND HEAVY INDUSTRIES
4.8% LAW AND SECURITY
4.3% CONSULTING AND RECRUITMENT
2.8% PUBLIC AND GOVERNMENT INSTITUTIONS
1.8% OTHER

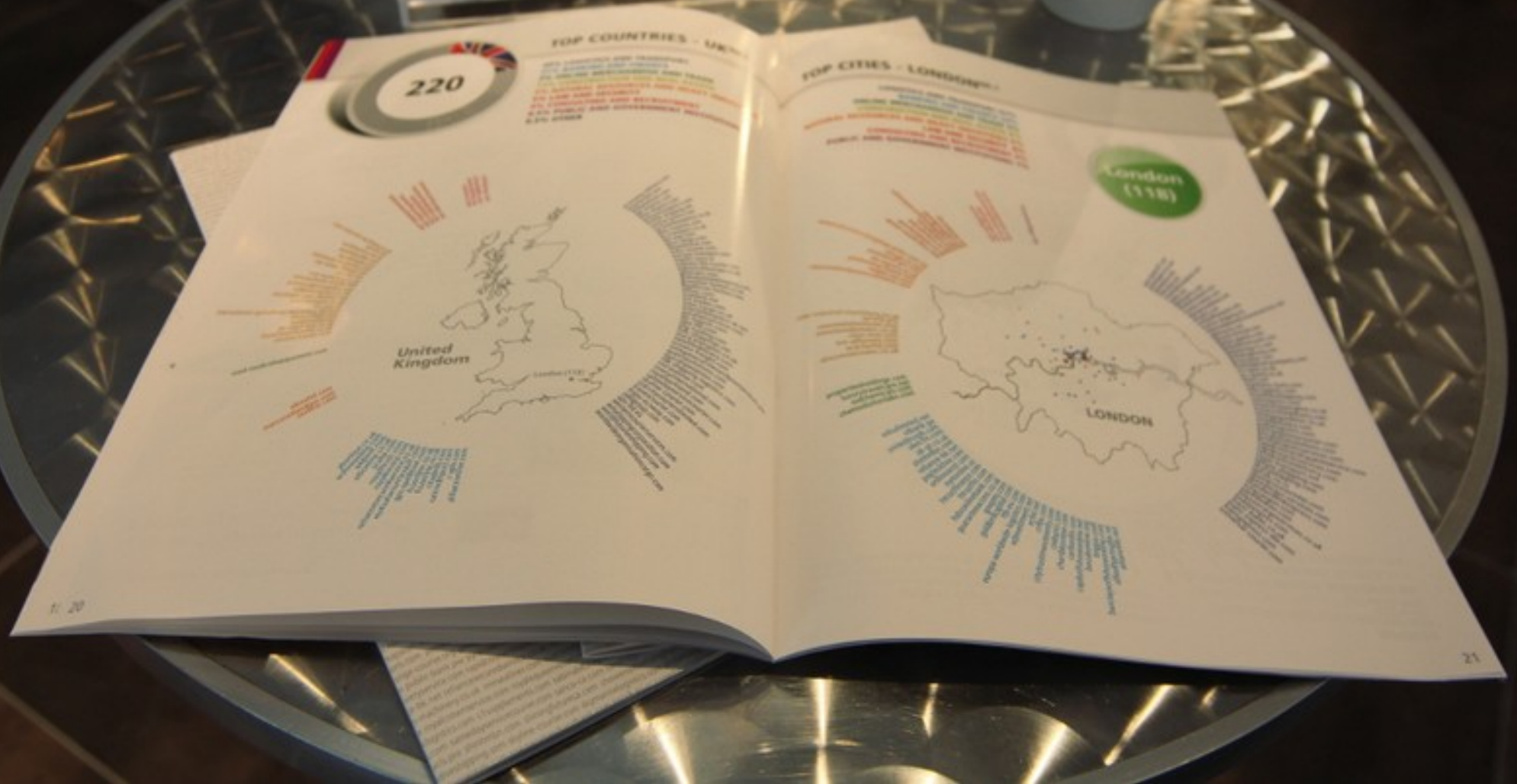
TOP COUNTRIES





Megacorp.kairus.org







Company showreel / Location check / website

Conclusions

- Vigilante communities fight against fake websites
- Use open source intelligence tools to collect evidence
- Write complaint letters to hosting providers
- Artwork “Megacorp.” visualizes the actions and teaches their strategies in workshops.

THANK YOU!

Questions & remarks?

Megacorp.kairus.org / db.aa419.org

Contact:

Andreas Zingerle, University of Art and Design, Linz, Austria.

Andreas.zingerle@ufg.ac.at

Kairus.org