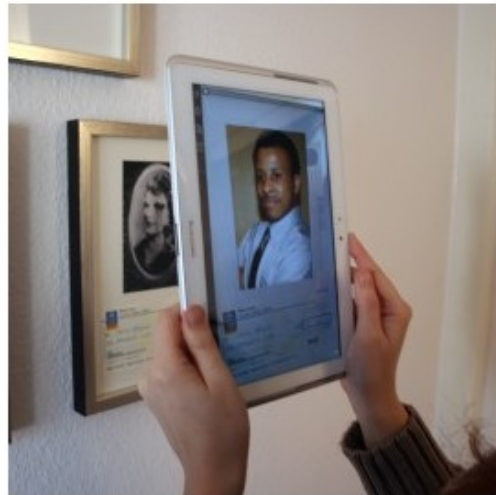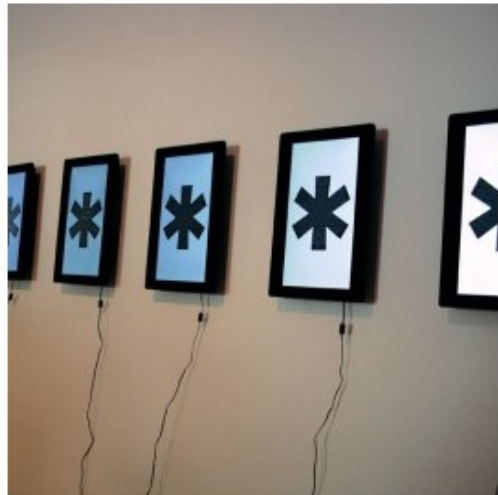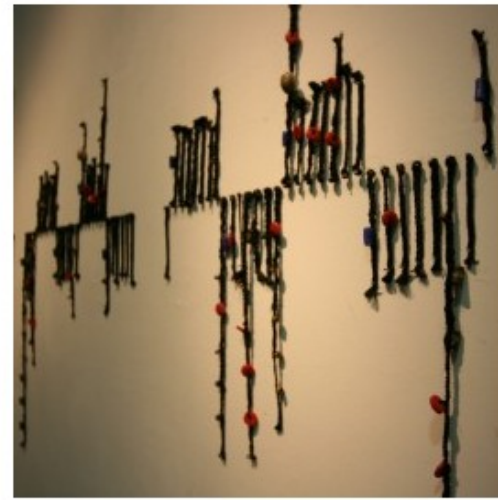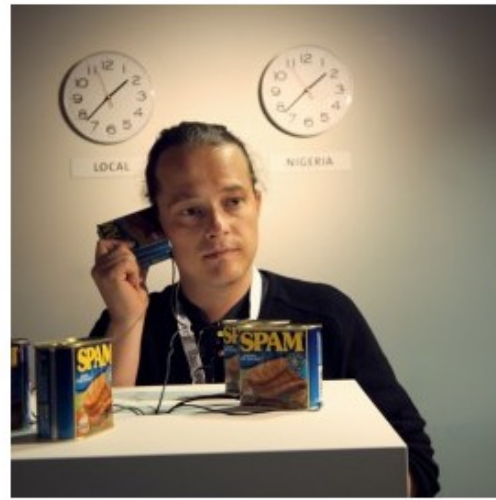# Trust Us and Our Business Expands! How Net-activists Take Down Fraudulent Business Websites

Andreas Zingerle, Linda Kronman, Kairus.org
July, 8th, 2016, xCoAx Conference, Bergamo, Italy.

KairUs Art collective

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

Fraudulent websites everywhere?

- 20% of the Web is fake (Gyongyi and Garcia-Molina 2005).

- 70% of ".biz" and

- 35 % of ".us" domain pages are fraudulent (Ntoulas et al. 2006).

- 85% of phishing websites are registered ".cn"

ARTISTS AGAINST 419

| 100% risk free ...

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 (*) [_____] [GO]   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.glotrustint.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

Research questions

- How do these fraudulent websites look like?

- Are there patterns depending on countries or industry branches?

- How are the fraudulent websites detected?

- Why is this done by vigilante communities?

- Do they follow certain ethics or moral strategies?

Old tactics

- 'Bandwith hogging' and DDos attacks by using self programmed software called "Muguito" and "Lad Vampire", discontinued 2007

Present tactics

- Collect evidence and information about the website that proves that it is a fake/fraudulent 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 the given country

  - visit the physical addresses to see if a company is located there.

- There are other tools available, we wanted to focus on the tools and strategies that this online community is using.

Domain Whois Lookup

- WHOIS lookup

- Registrar information

- when it expires as well as contact details.

- How long is the domain registered

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?

- Is it a valid physical address?

- Is there a valid phone number?

Start-Office

Reinvent the way you do IT

Wednesday, September

HOME PAGE   ABOUT US   SERVICES   CLIENTS   TESTIMONIALS   CAREERS   CONTA

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

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 Inclusion in our database does not necessarily indicate criminal activity on the part of the registrant, host or any affiliated c

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

Quick Search (*) [_____] [GO]   Show all   Advanced Searc

⊙ 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.

http://www.start-office.biz/ [Go]

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

File a report

- <u>host</u> is responsible for physically hosting the site / email addresses

- <u>registrar</u> is responsible for the domain name registration

- Look for other possibilities to warn other people and potential victims.

Idea how to visualize parts of the AA419 DB

- We were curious to find out what kind of businesses were represented on these fake websites

- We wanted to comment on the template based aesthetics of todays company representations

- We wanted to put an emphasis on the structures of centralization of money and power

Fictional examples
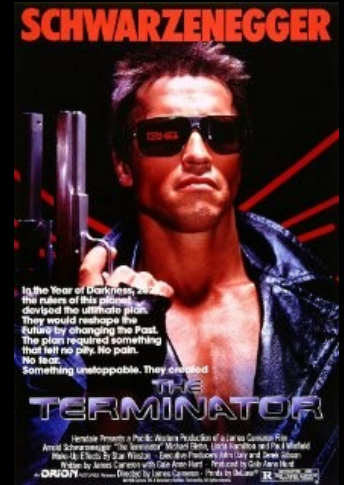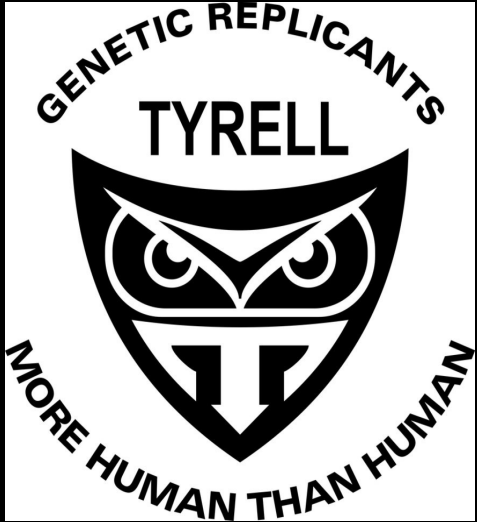
'T OOST INDISCHE MAGAZYN, EN SCHEEPS-TIMMER-WERF.

J. Mulder Fecit

Powering
Possibilities

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 ›

ارامكو السعودية
Saudi Aramco

Challenge

- when websites where listed in the AA419 the hosting providers closed the websites

- we could not go back to the websites to analyze them

**KEY FIGURES:
ALL BUSINESS SEGMENTS**

1000

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
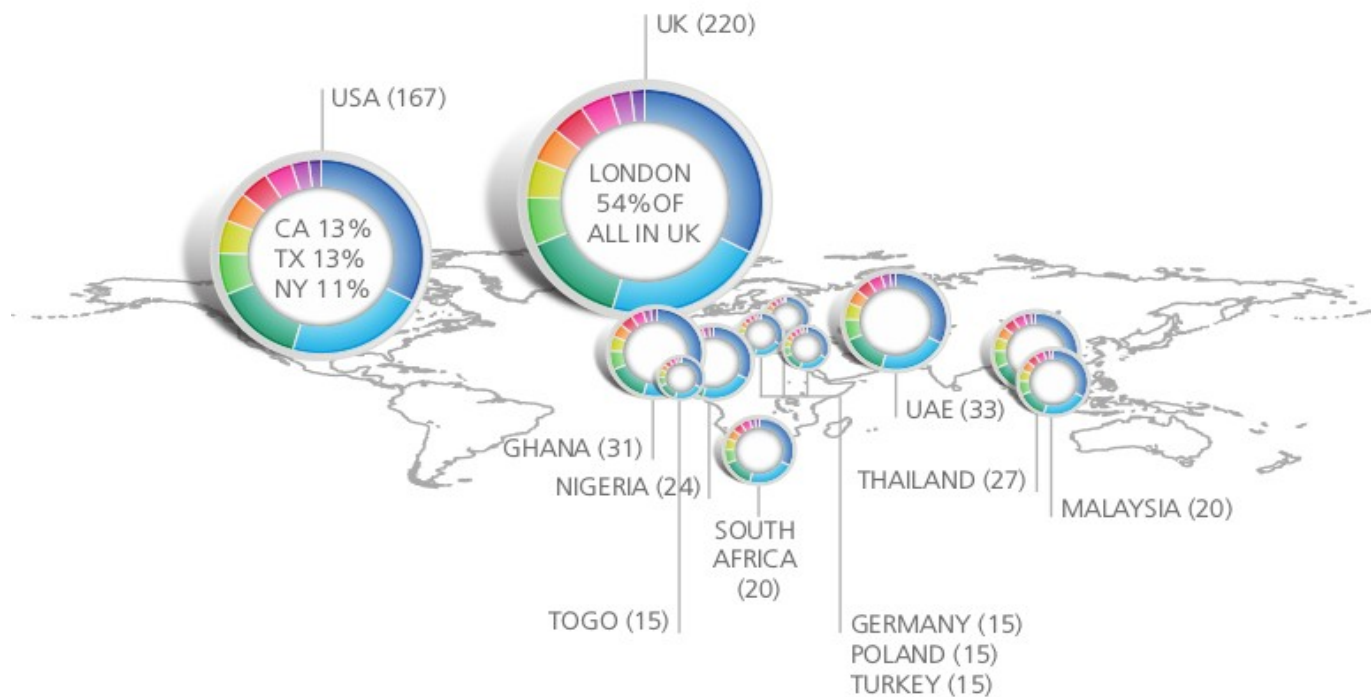4.3% CONSULTING AND RECRUITMENT
2.8% PUBLIC AND GOVERNMENT INSTITUTIONS
1.8% OTHER

London
(118)

Accra
(28)

New
York
(16)

Dubai
(15)

Lomé
(15)

Abu
Dhabi
(14)

UK (220)

USA (167)

CA 13%
TX 13%
NY 11%

LONDON
54% OF
ALL IN UK

GHANA (31)

NIGERIA (24)

SOUTH
AFRICA
(20)

TOGO (15)

UAE (33)

THAILAND (27)

GERMANY (15)
POLAND (15)
TURKEY (15)

MALAYSIA (20)
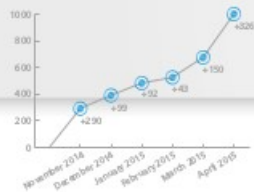
LETTER FROM THE CEOs

During the period from 9th November 2014 to 6th April 2015 the Megacorp. holding was established and acquired its first 1000 affiliated companies. A main requirement for a company acquisition by the Megacorp. holding is that the companies website in question is listed on 'Artists Against 419 - Fake Sites Database'[i]. Megacorp. can thus be seen as a giant umbrella company for evil businesses with its sources for inspiration in science-fiction[ii] and the real world.

While the aqusition of 1000 companies in the first operating year might sound like a major investment, this is only a small part of the Megacorp.'s potential. The 'Artists Against 419 - Fake Sites Database' publishes tens of new websites every day, recording mainly websites that are in English language. What potential does the German-, Spanish- or Chinese-speaking market offer? According to research[iii] fake websites comprise nearly 20% of the entire web, and 70% of ".biz" and 35% ".us" domain pages analyzed in a sampling of 105 million web pages were fake. A great deal of our holdings are clones of existing companies published under non-legimite domains. These websites are mostly used for phishing[iv], and according to the Anti-Phishing Working Group's 2H2014-Report[v] there were at least 123,972 unique phishing attacks worldwide during the second half of 2014, which occurred on 95,321 unique domain names. In view of these numbers, the Megacorp. holding has infinite possibilities to grow, and we envision it to be the most evil conglomerate ever.

Based on a short review of the first 1000 companies that we acquired, we can proudly confirm that we are well on our way to achieving our strategic objectives to offer complete services from one source, which can serve the entire market. We have divided our enterprise into 10 business segments, of which the biggest are 'Transport and Logistics' (32.6 %), 'Banking and Finance' (21.9%) and 'Online Merchandise and Trade' (14.2%). It may come as a surprise that the 'Pet Shops and Animal Transport' (6.9%) segment has a good chance of being the fourth largest business segment. While most of our companies are definitely into the phishing business or eCommerce scams, we also acquired several unique websites supporting more story-driven e-mails scams. One of them is the 'SDD-solution' retailers, who promise to wash your black money and render it back into a usable currency (see page 10). Megacorp. operates world wide. That said, we have a strong focus on Europe where 32% of all our companies are based, and especially the greater London area can be considered a major hub for our businesses, hosting 118 of our companies headquarters. A considerable amount (22%) of our companies are purely virtual products of our globalised era and do not have a given location for their activities. As mentioned, our company language is currently restricted to English, and this might limit our presence on some continents, especially Asia's lucrative market, while apparently the Chinese phishers are responsible for 85% of the domain names that were registered for phishing[v].

This report highlights some key figures of our first 1000 companies, providing a unique insight into our business structure.

Yours Trustfully,

Scarlett Abbot   James A. Husby

i) Artists Against 419 - Fake Sites Database, an online watchmen group related to the vigilante scambaiting communities available at: http://db.aa419.org/fakebankslist.php

ii) Megacorp, is a term popularized by well known science fiction writer William Gibson. A megacorp is a massive conglomerate, holding monopolistic or near-monopolistic control over multiple markets. Well known examples of megacorps are for example: LexCorp (DC Comics), Tyrell Corporation (Blade Runner), Weyland-Yutani (Alien franchise), Cyberdyne Systems Corporation (Terminator films) and Omni Consumer Products (Robocop).

iii) A. Abbasi, Z. Zhang, D. Zimbra, H. Chen, and J. F. Nunamaker, (2010) "Detecting Fake Websites: The Contribution of Statistical Learning Theory".

iv) Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.

v) Global Phishing Survey: Trends and Domain Name Use in 2H2014. www.antiphishing.org

CEOs

ABOUT MEGACORP.

Megacorp. is a corporate conglomerate inspired by its equally powerful counterparts in science fiction literature. The enterprise is based on a collection of fake websites scraped from the Internet by the artist duo KairUs. These companies exist only virtually and are used by cyber criminals for phishing attacks or to support scam stories. The Megacorp. exists therefore as an umbrella company for subsidiary companies that are 100% dummy corporations. Megacorp. operates on a global scale and is constantly growing with firms represented in almost every branch of the industry. The subsidiary companies consequently comprise domestic and international export, real estate agents, insurance companies, law firms, security companies, banks, educational institutions, hospitals, online commerce, economic communities and ministries.

OUR MISSION:
is to offer complete services from one source which can serve the entire market.

CONTACT

megacorp.kairus.org
megacorp@kairus.org

OUR VISION: *is to BE EVIL!*

TABLE OF CONTENT

OUR SLOGAN: Trust us and we will expand!

THANK YOU!

Questions?
Come and get your report!

megacorp.kairus.org