TRUST US AND OUR BUSINESS EXPANDS! HOW NET-ACTIVISTS TAKE DOWN FRAUDULENT BUSINESS WEBSITES

ANDREAS ZINGERLE
University of Art and Design
Linz, Austria
andreas.zingerle@ufg.at

Keywords
Fraud
Scambaiting
Anti-fraud activism
Open source intelligence

Internet criminals create fake websites that mimic real websites and use them for advance fee fraud or other criminal activities. Over the last ten years members of the vigilante scambaiting community “Artists against 419” maintain the biggest open-access database of fake websites. They use “passive reconnaissance” and “open source intelligence” (osit) tools to gather information to file reports with the hosting provider to get the websites taken off the web. This chapter takes a closer look at the group’s strategies and explains the artistic research installation called “Megacorp.” that visualises a sample probe of 1000 websites from the database collection.

2016.
xCoAx
.org
Computation
Communication
Aesthetics
& X
Bergamo, Italy

1 INTRODUCTION

In recent years the web has been increasingly used for end-user e-commerce to buy goods and services: flights and holiday recreation, music and film streaming (entertainment), ordering food and daily groceries for home delivery. The number of fake websites is increasing and scammers use them to present a trustworthy and professional appearance to trick people. It is easy for non-tech savvy people to design a website by using open-source Content Management Systems (CMSs) or freely available web design templates. They register Top Level Domains that use wording similar to that of the original companies. Often, clones of real websites are created by scraping real companies' websites, and then the fake login pages are used in phishing attacks. There are programs that report phishing incidents automatically, but they still rely on reports of phishing incidents from users. (Husak and Cegan, 2014) Vigilante online communities of scambaiters try to identify, block and report Internet crime activities. For this they have developed various strategies, ranging from creating warning platforms to collecting fake checks or blocking bank accounts, and organise themselves in different forums. One of these subgroups call themselves "Artists against 419" and host the biggest open-access database of fake websites. (Zingerle and Kronman, 2013b) As of May 2016, there are over 4800 registered users and an average of thirty-five websites are added to the database each day. They use "passive reconnaissance" and "open source intelligence" (osint) tools to gather information to file reports with the hosting provider to get the websites taken off the web. Since 2007, the group members discontinued using web programs such as "Lad Vampire" or "Muguito" to run "Denial of Service" attacks against the websites and instead now use their own tools and written reports to maintain a good relationship with hosting providers and law enforcement. (Cain, 2004, Brenner, 2007)

2 OPEN SOURCE INTELLIGENCE TOOLS

Scambaiters use various vernacular tools and social engineering techniques in order to run background checks on suspicious business websites. Open source intelligence (osint) refers to intelligence that has been derived from publicly available sources both on- and offline. In this paper, I want to cover the most popular tools for finding fake websites. These tools are used in ethical passive reconnaissance to gather as much information about the target as possible. (Bansal and Arora, 2012) In this version of passive reconnaissance, activists and hacktivists

seek to gain information that will support their political causes or other such ethical motivations. Law enforcement officials may also use passive reconnaissance as part of a criminal investigation. Ethical or not, passive reconnaissance is always done without the authorisation of the person or organisation that is being targeted. (Glassman and Kang, 2012) This leads to an effective combination of classical social engineering attacks on the target, which in turn can be used to harvest more information. The chapter concludes with the collection of the information and filing a report that is then sent to the registrar, hosting provider and other warning institutions. The following chapter was the hands-on part of a workshop called “Credible Fictions-Deceptive Realities”. In the workshop the “Megacorp.” installation served as a point of departure to further investigate Internet activism, fake websites and osint-tools. The online tools were presented to the group of participants, and information was gathered and discussed amongst the participants using the collaborative writing tool “piratepad”. As an example website I want to focus on start-office.biz. According to their website, start-office.biz is an international company specialising in organising virtual offices. They are located at the Wienerberg Twin Towers in Vienna, Austria, and currently offer jobs to local agents who should “provide relevant information online for direct clients and other relevant stakeholders through popular social networking sites”. In the following chapters, we will use the osint tools to analyse the website and raise the suspicion that the website is not legit. One browser-addon that merges a lot of the tools discussed here is called “Passive recon”. The Firefox extension adds a right-click menu option called “Passive Recon”, which opens a menu with a lot of possibilities. Around fifteen different options are available with the possibility of querying all databases at once. The queries are divided into groups, for example “DNS lookups”, “whois and domain lookups”, Netcraft Site reports, “Google queries” and “Email server mx record lookups”.

2.1 LOOK AND FEEL

Every website is designed differently. Over the years certain trends in usability set standards for web designers. You can always ask yourself how coherent the web design is. Does a photo with the company logo have a pixelated poor quality, whereas all other photos are crisp and sharp? Does the logo look badly manipulated into an image? On the front page of our example website we see the dark black logo of start-office.biz. Font type and size of the logo look misplaced and don’t fit the overall dominant grey and dark blue colour combination. In one of the header

images the logo is clearly squeezed into the image. The company's headquarters are supposedly located in Vienna, Austria. The website claims to operate on a global scale and runs hundreds of offices in the USA and Canada. The page language is English, and no German translation is available. On the "testimonials" page we find a review from a person called "Michel" from France, who refers positively to a different company:

"Sunex's virtual office allows me to service these clients from anywhere in the world, while maintaining a presence in Texas."

So it seems that this review was copied from another website and the company's name was not changed. The "career" page offers an application form to apply for a "local agent" position. The salary is stated in USD and is paid on a weekly basis, which is also a very uncommon practice in Austria.

2.2 DOMAIN NAME

Check the Domain name where you enter the site. If you click a link, the clicked text and the hyper-link that opens in a browser can be two different websites. That way, closely similar characters (e.g. i, l and number 1) can lead customers to fraudulent websites. "Wrong key typos" or "QWERTY typos" can occur when the user hits the wrong key that is near the intended key on the keyboard, e.g. "voding" instead of "coding". One can easily miss, transpose or double a character when typing on the keyboard. In our example the domain name is written correctly. A random sampling of over 105 million web pages revealed that 70% of .biz-domain pages analysed were fake. (Bansal and Arora, 2012)

Table 1. Different typo types for domain names.

Original website	Bankaustria.at	Amazon.com	Facebook.com
Look-alike chars	Bankaustrla.at	Amason.com	Faceb00k.com
Wrong key	Bankausgria.at	Amaz0n.com	Fadebook.com
Missed key	Bankastria.at	Amzon.com	Facbook.com
Transpose key	Bankasutria.at	Amzaon.com	Faceboko.com
Double a character	Bankaaustria.at	Amazoon.com	Faceboook.com

2.3 SECURE SOCKET LAYER (SSL)

Websites where you have to create a profile, login to your account or pay with a credit card offer additional security with an SSL encryption of your provided information. Internet scammers will not pay extra for this service in order to defraud you. In our

example the website does not offer a profile page or a login, so the use of https to secure the customer's data is not necessarily needed. Often, scammers include the logos of SSL Certification companies like Verisign, TRUSTe or Thawte.

2.4 CROSSLINKS

You can check how many other websites link to your targeted website. In search engines like Duck Duck Go or Waybackmachine, type "link: www.start-office.biz" or use online search tools like backlinkwatch to figure out how many websites link to your website in question. Neither of these tools report any backlinks. It is not a criminal act to not have any websites linking to your website, still it looks suspicious when a page claims to be a global player, but no customers link.

2.5 CONTACT INFORMATION

Every page needs a possibility for contacting the website owner. Is the contact email the same as the domain name or is it a free-to-use webmail service? Is the postal address a valid address? This can easily be checked through online streetmap services. Phone numbers can also be checked to see whether the area code belongs to a local number or if it is part of a call forwarding program. What happens when you call the number? Is the line in use during office hours? In our example the companies address is the Twin Towers in Vienna, although it does not provide a floor number. The phone number has the correct country code "+43" for Austria and "1" as a city code for Vienna. A quick search in the local online telephone database ensures that the telephone number is registered at the state telecommunication company A1, but there is no name entry to be found. There are two email addresses on the website: support(at)start-office.biz and hr(at)start- office.biz. An alter ego personality contacted both addresses and claimed to be looking for a job in Vienna. A person called Thomas Anderson replied as a representative of the company, sent me his Skype account details and three pdfs that I should read through, fill out and return in time. The three documents included an application for employment, a confidentiality agreement and a job offer signed by a Michael Adams, Director of Start-Office.biz. By using an IP tracker it is possible to analyse the email header and determine the IP address from where the email was sent. In the case of the email from Michael Adams, the email provider is Telmex Colombia S.a. in Barranquilla, Colombia. A NSA report identifies eleven main types of hidden data, metadata, and embedded content that may be found in PDF files. (Kaulback and

Datta, 2010) Most of the meta-data was swiped when the pdf was created with the online tool “go4convert.com”, just the creation date was left and from that we can see that the internal clock was set to “Central European Summer Time” (CEST). So the files have been sanitised and no metadata was found.

2.6 IMPRINT

Depending on in which country the company operates in, a trade registry number, VAT number, company address and other legal metadata and terms of use have to be published as a “Site notice”, “Legal notice” or “Legal disclosure”. This information can be double checked on pages like VIES/VAT number validation from the EU Commission[1] or the BBB-Better Business Bureau.[2] According to E-Commerce law, Austrian companies operating commercially must have a legal notice on their webpage. In the contact section there is no legal notice or VAT number published.

1. http://ec.europa.eu/taxation_customs/vies/

2. http://www.bbb.org/

2.7 DOMAIN WHOIS

WHOIS[3] stands for “Who is?” and is a web-utility used to look up information on domain names, contact information as well as some technical information such as the domains name servers (DNS). Every domain owner has to provide valid contact information. This is part of the registration agreement and providing false information can result in your domain name being deleted, although some types of domains do allow you to have placeholder information for another company as the domain owner. By doing a whois look-up on a targeted domain, you can see when a domain was registered, updated and how long this registration is valid. Scammers often use the minimum timeframe of one year to register their domain, since they are sure to operate for only a few months and then open another domain. Further important information one can gather is the hosting provider’s name and contact information. It is also possible to track down inconsistencies, e.g. different addresses or website owner other than what is stated on the website. In our example the registrant contact is a Mr. Fred Bohnsack, living in 2775 Holdom Avenue in Surrey, B.C., Canada. The website is hosted with hostgator.com and is registered for one year.

3. http://www.whois.net/

2.8 REVERSE IP LOOKUP

Using a reverse IP Address lookup tool[4] it is possible to gain more insight about all the different websites and domains hosted on that IP-address. Often scammers run several websites at once

4. http://reverseip.domaintools.com/

and it is just easier, cheaper and more convenient to host them under the same provider. This way, it is often possible to observe the working methods of a group of scammers who operate several websites at once.

2.9 HTML CODE AND TEXT ANALYSER

Scammers often reuse their website templates. Once their websites are taken off the Internet, they make small changes e.g. the business name, address, the logo or in the written text, and then they register a different domain and upload the site again. To be able to more quickly track the website once it re-surfaces, anti-scam activists use online services like “Talkwater alerts” and “Google alerts”. With these services one can search for certain keywords or phrases and get instant alert messages when the website is indexed. Activists specialise in certain businesses and build up alert clusters. When we look into the HMTL code we find a reference that the website was “mirrored from sunexsolutions.com/ by HTTrack Website Copier/3.x [XR&CO’2013], Sat, 11 Oct 2014 06:46:46 GMT”. That way we know that the website “start-office.biz” is a clone from “sunexsolutions.com”. Another toolset that can be used to track copied content on the web are online plagiarism detection services like “citeliner” or “copyscape”. Once you copy/paste phrases of the websites text into the searchbox, the services use the Google API to return websites that use the same or similar text. The matching text areas are highlighted.

3 FILE A REPORT TO THE HOSTING PROVIDER

In the previous chapter we discussed various different online tools for gathering background information about a website. Now it is time to bring the information together and file a “Terms of Service (TOS) and Acceptable Use Policy (AUP) Violation” report. This report is sent to “Hostgator”, the hosting provider of the website. First, the website was reported on the AA419 forum with a copy of the whois registry and the links to the copied websites. A moderator of the forum checked it and added it to the database. Then it was possible to file a report email and sent it to the hosting provider, asking the abuse team to double check our suspicion and delete the website. Another possibility for sending a warning to an Austrian institution is the “Watchlist Internet”, where it is possible to file a report online.

Subject line: TOS/AUP Violation start-office.biz

Dear HOSTGATOR abuse team:

The following domain is hosted on your servers or is within your IP block. Please investigate and suspend this fraudulent domain: Website: start-office.biz, IP: 192.254.186.125.

THIS SITE IS FRAUDULENT FOR THE FOLLOWING REASONS:

+ Site is listed in Artists Against 419's database of fraudulent websites:
http://db.aa419.org/fakebanksview.php?key=106062

+ The listed telephone number does not exist.

+ The address listed for the site is false. The address listed belongs to another business or does not house any business named "start-office".
Twin Tower, Wienerbergstrasse 11, 1100 Wien, Austria

+ The WHOIS registration does not appear to be affiliated with the site, or with a domain registration company. The contact details are likely fake: (copy whois link)

+ Site is being used in a job scam, also known as a "check" or "money mule" scam.

Check the "job description" listed on the suspected site. I am sending a copy of this message to fakebanks@aa419.org, which retains copies of all such abuse letters. If you feel more information is needed before you can proceed with closing this domain, please feel free to contact me under the email address xyz@gmail.com.

4 THE MEGACORP. BUSINESS CONGLOMERATE

The research into the scambaiting community "Artists against 419" led to a deeper investigation of how this community tracks fake business websites and reports them. We wanted to visualise the database, so our idea was to look at all these fake companies as though they were be one big evil corporate conglomerate that wants to take over the world. This so called "Megacorp." is inspired by its equally powerful counterparts in science fiction.

The term was coined by William Gibson and inspired many other authors of the dystopian cyberpunk science fiction genre to create megacorps in their fiction, amongst others the Tyrell corp. (Do Androids dream of Electric sheep), Encom corp. (Tron), Weyland-Yutani (Alien series), Cyberdyne skynet systems (Terminator).

The artwork is based on a collection of 1000 fake websites scraped from the Internet. “Megacorp.” serves as an umbrella company that tries to visualise the overall business segments and countries where these fake businesses are present. An interim report was published for the exhibition, where visitors had an opportunity to browse locally through the network of fake websites. Additionally a corporate presentation video and a location reconnaissance video reflect both the imaginary and the real world outreach of the “Megacorp.” In the following I describe the processes of gathering and analysing data and finding a language to visualise the dataset thus created.

3.1 DATA GATHERING

The data gathering process took several months, from September 2014 to April 2015. We visited the “AA419” database on a daily basis and automatically downloaded websites using a site scraping tool. The scraped websites were analysed and categorised according to business segment, street address, colours used, registered city and country. Once 1000 companies were gathered, we grouped them initially in twenty business segments, which we later reduced to ten, since we figured out that e.g. companies in transportation, courier and logistics are are similar enough to be grouped together. When analysing the different cities and countries, we focused on the top eight countries and correlated them with the top five cities (Fig. 1).

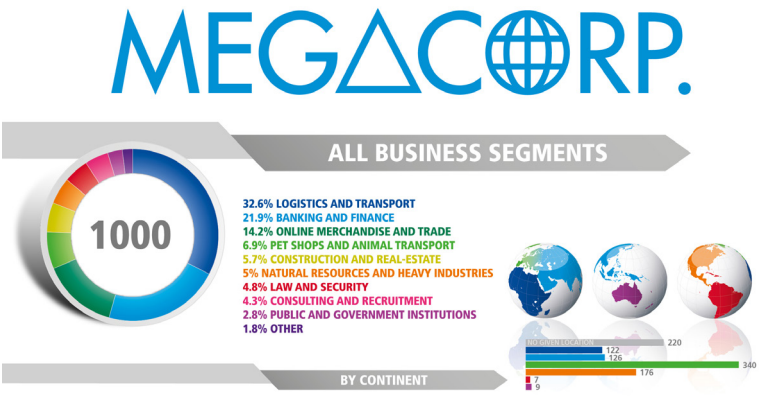

Fig. 1. All business segments and visualisation by continent

3.2 DATA VISUALISATION

To visualise the gathered data and to tell a compelling narrative about the fake business conglomerate, we decided to reenact a business corporate presentation in the form of a fair booth (Fig. 2). To achieve this we highlighted the main parts of the data visualisations on roll-up posters and created a corporate image show-reel (Fig. 4) that gives a fast overview of the main business segments and the global outreach. Since we created the Megacorp. within a year we decided to present all the gathered material in form of an interim report (Fig. 3), a financial report that is usually used to cover a period of less than a year that is not typically audited. In the installation we also presented a local website where visitors can browse through the acquired companies alphabetically, sorted by country and by business segment. Another video (Fig. 4) showed some of the companies' websites and our attempt at physical reconnaissance, when we visited the addresses where the companies claimed to have their headquarters and see what kind of company is actually registered there. During the "Credible Fictions - Deceptive Realities" workshop we extended this video through a virtual reconnaissance of companies addresses through the workshop participants, who mainly used Open Street Map, Google maps and local company registrars to figure out which companies are registered at a certain address. The collected screen-shots were added to the existing video, and so one outcome of the workshop became part of the exhibited installation.

Fig. 2. The 'Megacorp.' installation setup represents a business fair booth

Fig. 3. The 'Megacorp.' interim report

Fig. 2. The business showreel and the passive reconnaissance video

5 RELATED WORK

The culture jamming artist duo "The Yes-Men" initiate campaigns and actions to raise awareness about what they consider problematic social and political issues. One of their mottoes is that "lies can expose the truth". Since 1999 they have created fake websites that mimic global corporations like Monsanto, General Electric or Apple or organisations like the World Economic Forum or U.S. Chamber of Commerce. On the websites "The Yes-Lab"[5] they published fake news reports, bogus press-releases and invitations to fake press conferences.

For over ten years, from 2005 to 2015 Nicholas Feltron published a yearly report of himself trying to quantify his daily actions and behaviour. Each year he tried different approaches to

5. http://yeslab.org/museum

give very intimate perspectives into his daily life: which places he travelled to, how many steps he took, what he ate, who he talked to, how many photos he took, to what he drank. He tried several different devices that helped him track his activities, and he even designed his own iPhone app called Reporter. Nowadays Felton works at Facebook and was lead designer in the development of the Facebook timeline. (Wilson, 2015)

The artist duo Jodi exhibited L.V.Y. at linkcabinet.eu in Oct 2015. The work features three mistyped top domains "LinhedIn.com", "Vodacone.com" and "YouTuhb.com" and "reveal the double intent to mimic one of the most common glithc (sic!) that occur while using a keyboard, while while at the same time trying to exploit it to reach a chance audience"[6].

The hacker "Amped Attacks" specializes in distributed denial-of-service (DDoS) attacks targeting Islamic State websites and white power supporters. "Amped Attacks" uses #tangodown in his tweets[7], a hashtag commonly used by the Anonymous hacktivist group to report websites they have taken down. The name "tangodown" refers to a term used by the US Special Forces to describe an eliminated enemy during a firefight. (Protalinski, 2015)

6. http://linkcabinet.eu/About/index.html

7. https://twitter.com/Sgtbilko420

6 CONCLUSIONS

In this paper I analysed the scambaiting community "Artists against 419" and their use of open source intelligence tools to report and shut down fake business websites. In a workshop setting we used an example website to test these out and file a report with the hosting provider to get the website taken off their servers. The artistic research lead to the creation of the artwork "Megacorp.", that serves as a business conglomerate and visualises a sample probe of 1000 fake business websites. The visualisation shows that most of the websites we found are located in the UK (220), USA (163) and UAE (35), whereas 220 companies do not indicate a direct address. A lot of websites resurface again once they are deleted, so they can be found by using "plagiarism checkers" and "text alert services". To track down and report several fake businesses the activists use reverse IP-lookup, so completely new and unknown websites can be added to the database. In future workshops we plan to use the Megacorp. repository to further explore strategies to uncover and report clones and copies of fake business websites.

Acknowledgements. The "Megacorp." installation was developed for the Steirischer Herbst 2015 and was exhibited at the "esc—medien kunst" in Graz (Austria) as part of the exhibition "What remains—Strategies of saving and deleting" curated by Reni Hofmüller.

REFERENCES

Bansal, Akanksha, and Monika Arora. "Ethical Hacking and Social Security." *Radix International Journal of Research in Social Science* 1, no. 11 (2012).

Brenner, Susan W. "Private-public sector cooperation in combating cybercrime: In search of a model." *J. Int'l Com. L. & Tech.* 2 (2007): 58.

Cain, Patrick. "Scam trap." *The Toronto Star, http://www.thestar.com, referenced March* 21 (2004): 2011.

Enterprise Applications Division of the Systems and Network Analysis Center (SNAC) Information Assurance Directorate, "Hidden Data and Metadata in Adobe PDF Files: Publication Risks and Countermeasures", https://www.nsa.gov/ia/_files/app/pdf_risks.pdf. 2008.

Glassman, Michael, and Min Ju Kang. "Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT)." *Computers in Human Behavior* 28 (2012): 673-682.

Husak, Martin, and Jakub Cegan. "*PhiGARo: Automatic Phishing Detection and Incident Response Framework."* In *Availability, Reliability and Security (ARES), 2014 Ninth International Conference on* , vol., no., pp.295-302, 8-12 Sept. 2014 doi: 10.1109/ARES.2014.46

Protalinski, Emil. "A single hacker is taking down racist and homophobic sites one by one", http://venturebeat.com/2015/10/21/a-single-hacker-is-taking-down-racist-and-homophobic-sites-one-by-one/

Wilson, Mark, "10 Years In The Making, Nicholas Felton Files His Final Feltron Report", http://www.fastcodesign.com/3052301/10-years-in-the-making-nicholas-felton-files-his-final-feltron-report, Oct. 2015.

Zingerle, Andreas and Linda Kronman. "Humiliating Entertainment or Social Activism Analyzing Scambaiting Strategies Against Online Advance Fee Fraud." in Cyberworlds (CW), 2013 International Conference on. IEEE, 2013, pp. 352-355.