THE 'MEGACORP.' BUSINESS CONGLOMERATE: HOW NET-ACTIVISTS TAKE DOWN FRAUDULENT BUSINESS WEBSITES

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

LINDA KRONMAN
KairUs Art+Research
linda@kairus.org

Keywords
Fraud
Scambaiting
Anti-fraud activism
Open source intelligence

Internet criminals create fraudulent 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

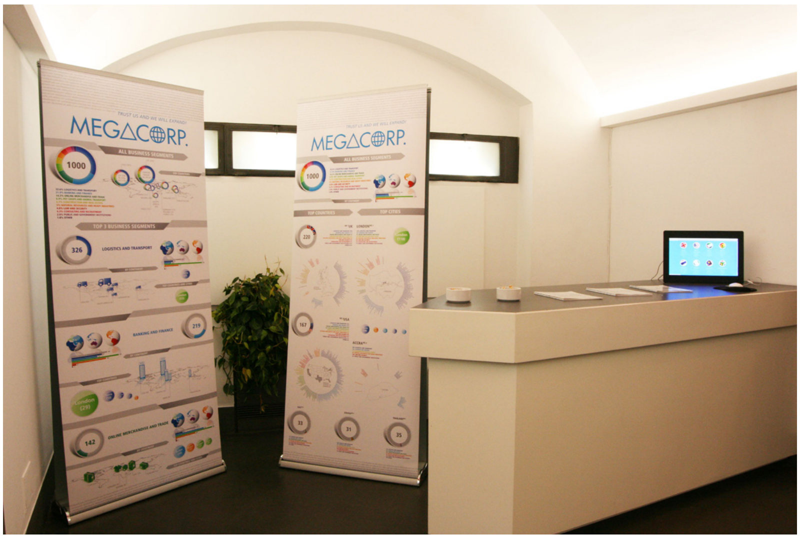
The number of fake websites is increasing and scammers use them to present a trustworthy and professional appearance to trick people. It is easy for non-tech savvy people to design a website by using open-source Content Management Systems (CMSs) or freely available web design templates. They register 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. (Glassman, and Min Ju, 2012) 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 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 fraudulent websites scraped from the Internet. “Megacorp.” serves as an umbrella company that tries to visualise the overall business segments and countries where these fake and fraudulent businesses are present. To visualise the gathered data and to tell a compelling narrative about the fake business conglomerate, we decided to reenact a corporate business presentation in the form of a fair booth. To achieve this we highlighted the main parts of the data visualisations on roll-up posters and created a corporate image show-reel 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 material gathered in form of an interim report, 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 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.

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



REFERENCES

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.

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

Zingerle, Andreas and Kronman, Linda. "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.