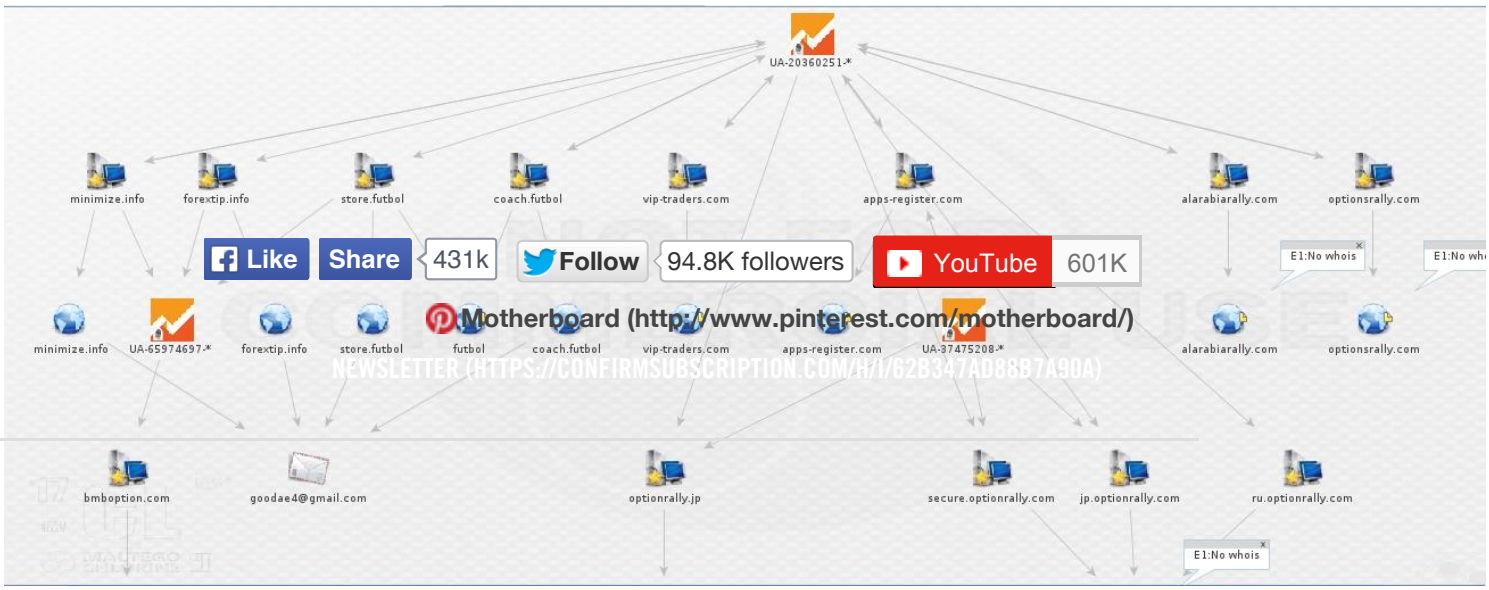
These Scammers Used My Face in an Ad, So I Mapped Out Their Network

WRITTEN BY JOSEPH COX (/AUTHOR/JOSEPHCOX)

October 27, 2015 // 10:48 AM EST



Tracking connections to "Deep Web Signals" via Google Analytics accounts. Image: Maltego

"Find It On The Deep Web," the advert read. It looked just like any other dodgy banner on the internet: a scantily clad woman suggestively urging you to click her. But, intrigued but what exactly "It" was, and why "It" was available on the "deep web", I followed her.

Then, I saw myself, quite literally. On the site, "Deep Web Signals" (http://deepwebsignals.com/), which claimed to have the secret to financial wealth and stability, was a video, that around 15 seconds in, included a snippet of a talk I had given previously about the deep web.

Little did I know, this was just one part of a scam site empire.

The site's creator claims in the same video he has discovered a method that, through "complex algorithms", scrapes the deep web for secret financial information, allowing anyone to get a serious payday. And he's only asking for a measly 1 percent partnership fee! And these obviously paid actors have made tens of thousands of dollars!

(/EN_US?TRK_SOURCE=HEAD

Obvious snake oil campaign aside, I checked the page's source to see if there was anything that would provide more clues as to who was behind the website. A quick search revealed a Google Analytics code: "UA-20360251."

Google Analytics is a commonly used service for web site administrators to track various stats about their visitors, such as where they're from, what operating system they use, and other demographic information. One Google Analytics account can be

used to keep tabs on multiple sites (https://support.google.com/analytics/answer/1102152), and is identified with the "UA" code.

So, it's a fair inference that any sites sharing a Google Analytics code are likely owned by the same person or company, or at least strongly connected in some way. Bearing that in mind, I decided to see what other websites were using "UA-20360251."

Nine, it turns out. Those included VIP-Traders.com (http://vip-traders.com/), a London-based "exclusive trading club," which seems to also be a money-making scheme. Apps-register.com (http://www.apps-register.com/) was a low budget site, complete with a cringe-worthy stock-image of "Josh", an apparent lawyer who "never believed that trading on financial markets could be so exciting!"

Others were Japanese (http://optionrally.jp/), Russian (http://ru.optionrally.com/) and English versions of the same trading site, Optionsrally.com (https://www.optionrally.com/), which promised 81 percent profits in as little as 15 seconds. Alarabiarally.com (http://alarabiarally.com/) was essentially the same thing but in Arabic, albeit with a slicker presentation, and then several domains all redirected to a site for "Benjamin Morris Binary Option", an investment firm that even has its own apps for Android (https://play.google.com/store/apps/details?id=com.spotoption.android.bmboption&hl=en) and iOS (https://itunes.apple.com/us/app/bmboption/id1034307425?ls=1&mt=8) devices.

I found these sites by using Maltego, a programme (https://www.paterva.com/web6/products/maltego.php) used to collect as much open source information about a target as possible. (It's sometimes used by penetration testers (http://null-byte.wonderhowto.com/how-to/hack-like-pro-use-maltego-do-network-reconnaissance-0158464/) in order to find weak points of a client's network to attack, while Lawrence Alexander at Global Voices uncovered several pro-Kremlin websites (https://globalvoices.org/2015/07/13/open-source-information-reveals-pro-kremlin-web-campaign/) by searching for others sharing the same UA code.)

Four of the scam sites were registered with the same email address, goodae4@gmail.com (mailto:goodae4@gmail.com). Some more traditional internet digging revealed that this address had been used to register a ton of other (http://domainbigdata.com/email/goodae4@gmail.com) dodgy sites (http://website.informer.com/email/goodae4@gmail.com), including Trafficsmania.com, a site that, unsurprisingly, provides visitor traffic for a fee.

Then the process started again: searching for other sites sharing the UA code on Trafficsmania.com led to more selling pretty much the same thing, and the network spread even wider, with more sites redirecting back to the Benjamin Morris investment site.

It appears that these scammers cast their fishing net far and wide: creating sites in different languages, buying up domains with slight spelling differences, and using all sorts of tactics and buzz words to hook people in. Also, it looks like they either get busted or moved along: eventually the links only led to sites that were offline.

The phone numbers I found linked to various sites went unanswered, as did requests for comment to goodae4@gmail.com (mailto:goodae4@gmail.com). The office of London-based VIP-traders doesn't exist, and instead the building is populated with doctors' and lawyers' offices.

Regardless, whoever is behind Deep Web Signals, if you could ask about using a video of me next time, I'd appreciate it.

--

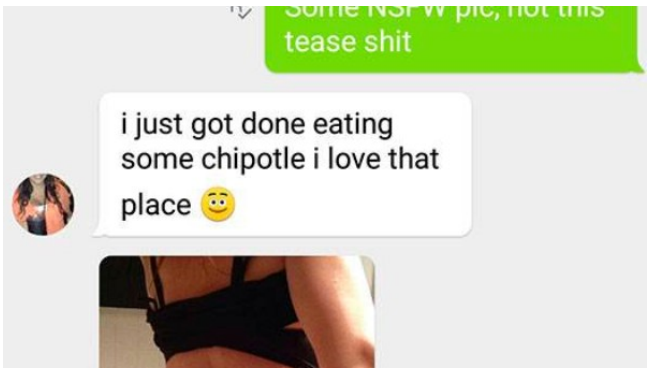
TOPICS: spam (/tag/spam), scams (/tag/scams), deep web (/tag/deep+web), dark web (/tag/dark+web), crime (/tag/crime), spam networks (/tag/spam+networks)

Contact the author by email (mailto:josephcox@riseup.net) or Twitter (https://twitter.com/josephfcox).

You can reach us at letters@motherboard.tv

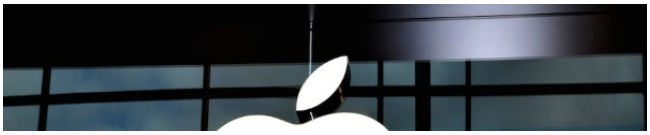
(mailto:letters@motherboard.tv). Want to see other people talking about Motherboard? Check out our letters to the editor (http://motherboard.vice.com/tag/letters+to+the+editor).

RECOMMENDED



A Q&A With the Redditor Who Made a Sexy Spam Bot Short-Circuit (/read/a-qa-with-the-redditor-who-made-a-sexy-spam-bot-short-circuit?trk_source=recommended)

I Broke Bitcoin (/read/i-broke-bitcoin?trk_source=recommended)



Scammers Set Up Their Own Apple Tech Support (/read/scammers-set-up-their-own-apple-tech-support?trk_source=recommended)

Why Chip Credit Cards Are More Secure than Magnetic Stripes (/read/why-chip-credit-cards-are-more-secure-than-magnetic-stripes?trk_source=recommended)

Tidal Accounts Are Being Sold for $1 on the Dark Web (/read/tidal-accounts-are-being-sold-for-1-on-the-dark-web?trk_source=recommended)

The Dark Web Is Becoming a Safe Haven for Malware (/read/malware-is-using-the-dark-web-to-stay-hidden?trk_source=recommended)

print