Not Everyone Steals A Trade Secret for Money: Some Do It For Fun.

Insights
3.01.11

Profit isn't always the motive underlying trade secret theft.Sometimes people simply want revenge or to wreak havoc.

Last month, a group of hackers self-denominated as "Anonymous" set out to do just that against federal contractor HBGary.Until recently, Anonymous was best known for launching attacks on Visa and MasterCard in retaliation for the companies' perceived hostility towards WikiLeaks.In those attacks, Anonymous used a method known as DDos to direct its ire at Visa.com and MasterCard.com, knocking the sites offline with seemingly little effort. Illustrating the power of social media, the group rallied its members to the cause via Twitter.

In February, however, Anonymous turned its attention to HBGary, a computer security firm enlisted by the FBI to help investigate the cyber attacks. Departing from its previous mode of DDos attacks, Anonymous hacked into HBGary's computer systems and publicized its success on HBGary's own website. Seizing the website, Anonymous explained that it had hacked into HBGary's computers systems and reviewed thousands of emails. HBGary had boasted that it had discovered the identities of Anonymous' leaders. Anonymous taunted HBGary in response: "Your recent claims of 'infiltrating' Anonymous amuse us.... You think you've gathered the full names and home addresses of the 'higher-ups' of Anonymous? You haven't.... We've seen your internal documents, all of them, and do you know what we did? We laughed." That's not all Anonymous did. It also posted over 60,000 HBGary emails on the web for anyone to read.

Among the many lessons for companies is that threats to your trade secrets do not always emanate from within. You need to think about more than the risk that your employees may resign to join a competitor. If you want to claim you have a trade secret, you need to take steps that are reasonable under the circumstances to protect your secrets. This means doing more than simply requiring your employees to sign confidentiality agreements. It means taking steps to secure your company's computer system and network. If you fail to do so, you just may log on to your website and see a message similar to the following message left by Anonymous:

This domain has been seized by Anonymous under section #14 of the rules of the Internet.

Greetings HBGary (a computer "security" company),

Your recent claims of "infiltrating" Anonymous amuse us, and so do your attempts at using Anonymous as a means to garner press attention for yourself. How's this for attention?

You brought this upon yourself. You've tried to bite at the Anonymous hand, and now the Anonymous hand is bitch-slapping you in the face. You expected a counter-attack in the form of a verbal braul (as you so eloquently put it in one of your private emails), but now you've received the full fury of Anonymous. We award you no points.

What you seem to have failed to realize is that, just because you have the title and general appearence of a "security" company, you're nothing compared to Anonymous. You have little to no security knowledge. Your business thrives off charging ridiclous prices for simple things like NMAPs, and you don't deserve praise or even recognition as security experts. And now you turn to Anonymous for fame and attention? You're a pathetic gathering of media-whoring money-grabbing sycophants who want to reel in business for your equally pathetic company.

Let us teach you a lesson you'll never forget: you don't mess with Anonymous. You especially don't mess with Anonymous simply because you want to jump on a trend for public attention, which Aaron Barr admitted to in the following email:

"But its not about them...its about our audience having the right impression of our capability and the competency of our research. Anonymous will do what every they can to discredit that. and they have the mic so to speak because they are on Al Jazeeera, ABC, CNN, etc. I am going to keep up the debate because I think it is good business but I will be smart about my public responses."

You've clearly overlooked something very obvious here: we are everyone and we are no one. If you swing a sword of malice into Anonymous' innards, we will simply engulf it. You cannot break us, you cannot harm us, even though you have clearly tried...

You think you've gathered full names and home addresses of the "higher-ups" of Anonymous? You haven't. You think Anonymous has a founder and various co-founders? False. You believe that you can sell the information you've found to the FBI? False. Now, why is this one false? We've seen your internal documents, all of them, and do you know what we did? We laughed. Most of the information you've "extracted" is publicly available via our IRC networks. The personal details of Anonymous "members" you think you've acquired are, quite simply, nonsense.

So why can't you sell this information to the FBI like you intended? Because we're going to give it to them for free. Your gloriously fallacious work can be a wonder for all to scour, as will all of your private emails (more than 66,000 beauties for the public to enjoy). Now as you're probably aware, Anonymous is quite serious when it comes to things like this, and usually we can elaborate gratuitously on our reasoning behind operations, but we will give you a simple explanation, because you seem like primitive people:

You have blindly charged into the Anonymous hive, a hive from which you've tried to steal honey. Did you think the bees would not defend it? Well here we are. You've angered the hive, and now you are being stung.

It would appear that security experts are not expertly secured.

```
We are Anonymous.
We are legion.
We do not forgive.
We do not forget.
Expect us - always.
```

Download HBGary email leaks

Michael R. Greco is a partner in the Employee Defection & Trade Secrets Practice Group at Fisher Phillips. To receive notice of future blog posts either follow Michael R. Greco on Twitter or on LinkedIn or subscribe to this blog's RSS feed.

Related People

Michael R. Greco
Regional Managing Partner
303.218.3655
Email