EXHIBIT A

Mid-Pacific ICT Center

Blog

FRIDAY, FEBRUARY 4, 2011

Ethical Hacking and LIGATT Security

Legal Note: The opinions stated here are my own, and do not necessarily represent the positions of MPICT, CCSF, or any of my other employers. (Sam Bowne)

It's frustrating to deal with criminals, online or otherwise. The process of collecting evidence legally, preparing documents, trials, etc. is slow, and frequently bad guys escape punishment. And the temptation to cut corners and go outside the system is always there. I saw this whole thing happen this week in a case I am personally involved in, and I am documenting it as a case study.

Gregory Evans runs a company named LIGATT security, which has been notorious
in the information security community for years. He has been accused of plagiarism, falsifying his credentials, threatening researchers, and many other misdeeds, as detailed on Attrition.org;

http://attrition.org/errata/charlatan/gregory_evans/

A lot of security professionals have been resisting Evans' activities, including me. It is particularly galling that he is a media celebrity, appearing as a security expert on CNN, Fox News, Bloomberg, and Time magazine. So we complain about his actions to media companies, conference organizers, accrediting bodies, and potential victims. And many lawsuits are being prepared and filed on both sides. It all takes time and energy, and has very little immediate effect. But as security professionals, we all should understand the process. We face the same frustration convincing corporate and government administrations to change poor practices, and patience is an essential job skill. Entrenched bad habits can only be fixed by slow erosion, like water digging through stone.

This week, someone ran out of patience with Evans. He got hacked. Two of his sites went down completely, and his entire email database was stolen and released onto the torrents. These emails reportedly include personal information about Evans, his contacts and his victims. The thief couldn't even be bothered to use a search-and-replace function to remove Social Security numbers, bank account routing numbers, etc. Details are posted here:

http://www.thetechherald.com/article.php/201105/6775/Ligatt-Security-breached-company-emails-hijacked-and-sent-to-public

I cannot condemn all this strongly enough. Allowing criminals to drag you down to their level and become a criminal too is a terrible mistake. The difference between ethical security professionals and criminal hackers is that we have the maturity and patience to proceed slowly and carefully within the system.

SEARCH THIS BLOG

Search
powered by Google

TOPICS

(1) [redacted] (1) Diversity (4) [redacted] (2) [redacted] (2) [redacted] (1) ICT (1) ICT Applications (9) ICT Education (38) ICT Infrastructure (29) ICT Jobs [redacted] (1) [redacted] ICT (3) (65) James Jones (42) Mobility (8) MPICT Announcements (22) Multimedia (5) Networking (48) networking security (15) [redacted] (1) Operating Systems (7) [redacted] (2) Public Policy (17) [redacted] (1) [redacted] (3) [redacted] (4) [redacted] (1) [redacted] (2) Web (14) Wireless (5)

CONTRIBUTORS

Christopher Wu
jen giang icasiano
singer808
Grace Esteban
Pierre Thiry
James Jones
Sam Bowne
Mid-Pacific ICT Center
Rick Graziani

WEBSITES

Mid-Pacific ICT Center
MPICT YouTube Channel
MPICT on Facebook
National ICT Center
BATEC
ATETV
Cyberwatch
CSSIA

ARTICLES BY CONTRIBUTOR

Christopher Wu (4)
James Jones (42)
Pierre Thiry (2)
Rick Graziani (3)

SPREAD THE WORD

Share this on Facebook
Tweet this
Get more gadgets for your site

SUBSCRIBE

Posts
Comments

FOLLOWERS

Follow
with Google Friend Connect
Followers (7)

I disapprove of Gregory Evans and his harmful actions strongly, and I have been working to stop them. But this is not a personal fistfight with the goal of bringing him down by any means necessary. My goal is to help make the Internet safer for everyone, and protect innocent people. I cannot see how adding lawless vigilantes to the ecosystem helps that process.

We have laws, courts, police, and governments for good reasons. I am bound by the (ISC)^2 code of ethics, and so are my students:

https://www.isc2.org/uploadedFiles/(ISC)2_Public_Content/Code_of_Ethics/ISC2-Code-of-Ethics.pdf

I want to remind my students and all other aspiring security professionals to stay out of criminal schemes. Don't help Anonymous take down websites, don't steal copyrighted materials, and don't hack into other people's systems, even if you dislike what they are doing. Becoming a criminal yourself does not stop crime--it increases it. Comic books are escapist fantasies--in the real world, vigilantes are no better than the people they oppose.

Posted by Sam Bowne at **12:49 PM**

16 comments:

thelightcosine said...

Sam Bowne: Well put. I think it shows true character to stand up and call this out for what it is. I have to admit that I initially let myself be pleased with this turn of events in a moment of human weakness. As a security professional I cannot possibly condone this type of behaviour though. Fortunately, I have the luxury of nobody particularly caring who I am, you have a bit more spotlight on you, so I say kudos to you sir.

February 4, 2011 3:41 PM

Jericho said...

Why do you point out the difference like that? All you do is imply that an ethical hacker(s) went rogue and hacked Evans, when there is no public basis for that. The fact you and others write this suggests that the person(s) who did this are otherwise the same as you or I. This is baffling to me.

February 4, 2011 6:57 PM

Sam Bowne said...

Jericho:

I don't know that a white hat hacker did this. But there are those who applaud these tactics, and I want to make the ethical point clear to my students, and anyone else who cares about my opinion. Which, I suppose, means white hats.

February 4, 2011 9:25 PM

Sam Bowne said...

Here are some comments that came in via Twitter:

"@sambowne: RT @MJCdotMe: @sambowne You are in fantasy land trying to differentiate black hats/white hats/"real infosec pros"/unicorns, etc..""

"@hypatiadotca: @sambowne feels like fussing over terminology. Not everyone who abides by the law identifies as wearing a particular hat."

"@attritionorg: @sambowne @MJCdotMe on paper yes, clear cut difference. real world? much more colorful and shades of gray."

I have heard these statements before, but somehow I have never understood them. I still don't.

My students face real temptations to become criminals, and I want them to resist them. And I regard it as an essential job skill to understand what the legal rules are, and know which side you are on. I do not understand how it is more complicated for you.

February 4, 2011 9:40 PM

Jericho said...

Probably because I know people that walk the line. Infosec pros by day protecting networks and doing a great job, occasional "black hats" by night if the cause is worth it in their eyes. They weigh the greater good and act. If you know some of these people, you will start to see that away from paper, it is a lot more complicated.

Our founding fathers broke the law for the greater good, are they only criminals? Does a soldier in Iraq that violates an order or law to save a civilian get pegged as a criminal?

February 4, 2011 9:47 PM

Leigh Honeywell said...

@Sam: it's more complicated than who calls themselves a professional or a whitehat or whatever because identification does not always correlate with what people actually do.

In the workplace your students will see people who identify loudly and publicly as whitehats/professionals behaving in an unethical and even illegal manner. It does happen. They will see conflict between those professed identities and how people actually behave. They will need to respond responsibly to the unethical or illegal actions of others. Just saying "whitehat/professional" == "only does legal/ethical things" is insufficient. I hope that makes my point clearer, hooray for more than 140 characters :)

There's a whole other discussion to be had about what to do when ethics and the law disagree. As I said on Twitter, What's happening in Egypt is the perfect illustration of that. But civil disobedience is not really the subject of my argument here, so I'll leave that for another time.

February 4, 2011 9:51 PM

Sam Bowne said...

Jericho and Leigh:

Thanks for presenting your views here. You are both luminaries in the ethics of hacking, and I respect your opinions highly.

It would help me if you could answer these questions:

1. Was it right to hack LIGATT?

2. Is the (ISC)^2 Code of Ethics a good guide to proper conduct?

My answers are:

1. Absolutely not.

2. Yes, although I dispute the requirement to "not associate with criminals". I go to Defcon and other conventions, and I am willing to talk to anyone and learn from them. My CISSP exam approval was delayed for a week or two because of my unexpected answer to this qualifying question.

February 5, 2011 6:17 AM

Sam Bowne said...

Jericho:

I know there are people who break laws for what the see as a high good, like the Jester and AnonOps. And I think they are in very dangerous territory.

The best way to defy authority is the way Socrates, Jesus, Ghandi, and Martin Luther King did--openly, publicly, with your real name, and accepting the consequences. If you hide and refuse to accept society's sanctions for your deeds, how can anyone trust you? And who will stop you when you are wrong?

February 5, 2011 6:25 AM

Sam Bowne said...

Leigh:

I certainly agree with you that merely claiming to be a professional does not mean someone is ethical. Those who claim to be ethical and are not are frauds. A student entering this profession must agree to abide by professional ethics, just like doctors and lawyers. If they fail to live up to those standards, they have failed to be professionals.

February 5, 2011 6:29 AM

Marcus J. Carey said...

Sam,

Ethics is something learned at through various means. They derive from home, environments, cultures, religions, countries, etc...

You don't become ethical when you become a CISSP or CEH.

If I'm in Russia and I write malware to feed my family am I unethical? If I'm American and sell exploits to the highest bidder am I unethical? If I make guarantees that you are hacker proof after I scan you network for vulnerabilities. Does a PCI scan guarantee I won't get hacked? Does antivirus defend against APT?

All the questions above have fuzzy answers. They could be morally or ethically wrong to many people. The deeper you get into the community you'll see that there is no firm dividing line. Just to get things to work you may have to violate licensing agreements or void warranties. Does that make someone a grey/black hat?

The White Hat/Gray Hat/Black Hat analogies are just like the OSI Model. They are great for teaching purposes only. We can tell people what the law is and that is it. They make the decision on what they do with it.

There have been criminal cases involving stealing open WiFi. Does that make those people black hats. Most people that I know have jumped on an open WiFi hotspot (unethical??). Ever used bootleg music, software, movies, or anything else?? Most White Hats I know bootleg music, software and movies at the minimum. That's illegal and unethical right??

I'm rambling, but hopefully you'll get the point. Feel free to contact me for a more in depth discussion.

-MJC

February 5, 2011 6:59 AM

Sam Bowne said...

Marcus:

Thank you for participating in the discussion.

I understand that there are greater and lesser crimes, and exigent circumstances that sometimes justify extreme actions. So for clarity, let me focus on a specific situation:

Was it right to hack LIGATT?

What do you think?

February 5, 2011 7:22 AM

Marcus J. Carey said...

Why are people jumping to conclusions saying LIGATT was "hacked"? The initial letter thanked, a "brave soul" who made it possible. Today on Pastebin there is a file with all LIGATT passwords in it. If that file was compromised, it would have left the door wide open for .

We do not have any motive at this time. We have no clue who did this, probably never will. If it was an insider as it seems, maybe that person was acting as a whistle blower.

February 5, 2011 8:07 AM

---

albino said...

From what I can see hijacking Evans's twitter feed has enlightened quite a few of his victims, while hardly hurting anyone. Releasing the emails, however, doesn't seem to have achieved much good (except exposing a couple of Evans's sympathisers) and done some serious harm. I don't buy the whole binary criminal/professional distinction since the law, while marvellous, is hardly perfect, especially with regard to IT.

'course I could be hopelessly wrong; I am new in the field and not a professional, ZDI/google/mozilla bounties aside. I think you might violate 'profession recognition of or association with amateurs' if you reply ;)

February 5, 2011 11:47 AM

Anonymous said...

Well said. I'd be interested to hear your opinions on th3j35t3r and the use of his self-developed XerXes tool that he uses to temporarally take down sites known for terrorist activities.

February 6, 2011 1:45 PM

Ryan Dewhurst said...

Hi Sam,

As a fellow security student I applaud your condemnation of the hack/leak what-ever anyone wants to call it and thank you for it.

The morals/ethics white/grey/blackness of it may all be a little blurred for some. However no matter what shade your ethics/morals are there is no debating that what happend was illegal.

This kind of behavior is exactly what we should be trying to stop. It is not up to us to be law makers or deciders of who is right or wrong.

I like any other person who has witnessed Ligatt's exploits know that they are a joke to the community. But just because we do not like someone does not mean we should break the law.

Ryan Dewhurst

February 6, 2011 4:45 PM

Sam Bowne said...

th3j35t3r is wrong to take down sites he dislikes with DoS attacks. Anonymous is also wrong to take down sites with the ridiculous LOIC DDoS tool.

The principle is simple: you have no right to control someone else's server without their permission. And freedom of speech means that anyone is free to post almost anything on the Web. If someone has posted something that is actually illegal, the proper legal procedures must be followed to take it down.

However, I think Anonymous is more repugnant than th3j35t3r, because Anonymous lies to children to suck them into criminal schemes, converting naive kids into felons. Th3j35t3r commits his crimes alone.

February 8, 2011 3:35 PM

Post a Comment

Comment as: Select profile... [▾]

Post Comment | Preview

Newer Post **Home** **Older Post**

Subscribe to: **Post Comments (Atom)**

EXHIBIT B