

ChicagoCon Diary: Day 1 - I Can't Believe It

This is the first part of a series of articles chronicling my ChicagoCon experience. I use these words specifically, because this is meant to give you a view of ChicagoCon from my perspective. So I will readily admit that it is a biased opinion. But I also wanted to give you a look into some of the ideas behind how we came to make the decisions we did and also a behind the scenes look into running a complex event.

ChicagoCon 2007 is a unique event with its focus clearly on the students, their education and career development. We obviously want them to gain knowledge while going through the classes, but we also want them to see a wider view. With that in mind, we intentionally crammed some extracurriculars into the event like morning keynotes, evening presentations and hacking contests. This way, you can take what you learn in class, get industry insights from the speakers, compare that to what your other classmates are doing in the real world and eventually go back to your place of work with practical ideas that can be truly implemented. It's a lofty goal, but worthy of effort.

del.icio.us

Discuss in Forums {mos_smf_discuss:Editor-In-Chief}

With this goal at the forefront of my mind, I came up with the concept of ChicagoCon a number of years ago. I've attended shows of all shapes and sizes, have chosen boot camps to gain certifications as well as the self-study route, and I've been working in the industry for a number of years. I wanted to take the best part of every experience and combine them into one event. That included having extra study materials in each classroom in addition to the official courseware provided for each student, all meals including breakfast, lunch and dinner, common areas for the participants to network with all students and more.

From those of you that know me or know of me, I am willing to share my thoughts and feelings. Sometimes my bluntness gets me in trouble, and I hopefully make up for that with my enthusiasm for helping others in their IT careers. That being said, I can't divulge everything due to agreements, contracts and personal guarantees, but I will do my best to open up the process. I also welcome feedback gladly, so feel free to tell to forget the extra stuff in these articles and just give me the facts. On the other hand, you may ask for more. Either way, it's this philosophy that has grown EH-Net and made ChicagoCon a reality. And it will continue to shape our projects to ensure future success.

So let's get to it.

Day 1 Keynote Speaker - Lance Spitzner, Honeynet Project

The concept behind having keynotes every morning and only giving the speakers 30 minutes was to not overtax the student's noodle but to get the blood flowing. So there was no better way of blasting off the event than by having Lance Spitzner of the Honeynet Project give the first keynote on Monday morning. But what was supposed to be a bolt of energy for the students ended up being a lightning rod of panic for me. With 25 minutes before the scheduled start time of the morning keynote, Lance was nowhere to be found.

Trying to stay positive, I took this as an opportunity to go to some of the classrooms to introduce myself and let the students know that I was here for them if they needed anything at any time. With 10 minutes to go, I made my way to the auditorium and began to prepare my cancellation speech to the students, guests and business partners in the audience who flew in the night before to see how well I did in planning ChicagoCon. I stalled, and, with 5 minutes before start time, I decided to take one more walk towards the front of the facility. Coming out of the auditorium, I saw Lance. Whew.

Lance is a dynamic speaker that had no problem getting the energy up in the room, and I quickly lost my panicky feeling. He gave a quick overview of who he is, where he came from and the Honeynet Project itself. Then he discussed the trend that the malicious activity is no longer coming from script kiddies but from highly intelligent and organized individuals who have turned malware, in all its forms, into a billion dollar industry.

Several years ago, I caught a speech by Lance where he gave a number of examples of the types of attacks he saw coming from the Honeynet. They were getting more sophisticated, but he also peppered the speech with some very comical stories of stupid cyber criminals. So when he agreed to be a keynoter for ChicagoCon, I asked if he could throw out some new examples. It will still be educational but also entertaining and very funny. Mind you, Lance is an animated speaker and from my personal experience has a great sense of humor. So when he "very matter of factly" said no, I initially thought he was joking. I quickly realized he was not. He very politely explained that he would not give a false impression of the current scene of malicious activity on the net these days. I was taken aback but was also more intrigued than ever to hear him speak.

Based on the research gathered from the global Honeynet, he sees so many interesting and creative ways to not only fool the general internet population but also to evade detection and prosecution. Given the time constraints, he decided to bring only one of the many technologies that the bad guys are starting to use on a regular basis and not very well known... yet. Fast-Flux Service Networks in a nutshell uses the concept that if my web site is associated with IP address, I can prevent being shut down by simply changing it. How do they do that? Well why not use the IP addresses of the botnet machines to basically have an unending supply of new A records for the fully qualified domain names (FQDNs) of the bad guys web sites holding malicious code? When law enforcement or the ISPs catch wind the malicious activity and try to shut down the connection based on IP address, the bad guys simply change the DNS records to have the FQDN point to another IP address in their controlled botnet. But the bad guys are now doing them one better. Instead of waiting for the ISPs to catch them, they now flux the IP address automatically every few minutes. Pretty slick, huh?

But of course the main hole in this plan is the DNS servers for the bad guys' web sites. Since the DNS server is doing the fluxing, the ISPs could just filter the IP address of the DNS server. That's where double fluxing comes into play. The bad guys are getting smarter and more automated. So now they not only have the IP address pointing to the FQDN changing automatically every 3 - 5 minutes, they also flux the IP address of the DNS servers every 90 minutes. A year or so from now when that time frame is not fast enough, it's a simple change to decrease that interval. With the number of infected machines out there, IP addresses are plentiful enough to accommodate any fluxing speed.

Lance found one other way of stopping this activity, and that is to have law enforcement shut down the actual machines running the DNS services. Once again the bad guys have found a way around this problem, and that is to house their servers in the Russian Business Network (RBN). Now they are outside of our jurisdiction and can't be shut down by our law enforcement agencies.

Lance did offer some other ways to mitigate the problems. This can be found in the PPT file in the Library section of <http://www.chicagocon.com/>. I do have to apologize to Lance as we had audio difficulties with the microphone during his keynote. It was a back of the house kind of issue, so it did not affect those in attendance, but it did make the audio recording unusable. Good news is that we do have audio recordings freely available in the Library for most of the keynotes and presentations.

Needless to say, this type of talk has a way of getting your brain going as you head off to class. And that's exactly what happened. All of the attendees were buzzing with anticipation to get to class.

Impromptu Problem Solving

To get extra exposure for the event, we setup an agreement with John Iasiuolo of the Computer Outlook Radio Program to do Daily Podcast with the keynote speakers and a live wrapup of ChicagoCon 2007 on Friday night's show. As each of the attendees headed to their classrooms, the keynoter and I were supposed to make our way to my makeshift office to record an interview. Lance unfortunately had other commitments. Although we'll try to get a recorded interview scheduled with him soon, this was one of those moments where you have to think on your feet. I was fully prepared to have Lance in the interview. But considering how he threw his support to this small and new event, I still felt grateful. On the other hand, what do I do now?

So instead of wasting an opportunity and just letting the interview drop, we pulled in Michael Yaffe, Director of Marketing for Core Security Technologies. Core Security has been a long time supporter of EH-Net and also the Platinum Sponsor of ChicagoCon. In fact, Monday was basically Core Day at ChicagoCon as they were responsible for all meals that day, presented in the evening on Client-Side Pen Testing and also sponsored a hacking contest giving the participants hands on experience with Core IMPACT, an awesome automated pen testing tool. Offering them this open slot was the least I could to make up for their incredible support of my crazy ideas. ;-)

Evening Presentations

The thought process behind the evening presentations was to give the attendees a look into what security professionals do on a day-to-day basis. That includes both technical and non-technical items. Of course, being presented by The Ethical Hacker Network and adding the "Hacker Con" component to the event, we felt it was a must to present live demos of real tools.

We came out of the gates on Monday with "IT Security Policy: Do we practice what we preach?" by CompTIA's Carol Balkcom, Project Manager for Security+. Every year CompTIA their Security Survey covering many interesting areas in the field, one of them is security policy. Although she quickly reviewed some of the more interesting findings (see the report in The Library), most of the time was spent actually engaging the audience on the issues of 1. Do you have a written policy in place and (more importantly) 2. Do you actually use it?

In order to ensure audience participation, we all agreed to leave the names of the organizations out of the conversation. Suffice it say that CompTIA's research findings rang true for our audience as a number of people from sectors such as the government, banking and higher education. They openly shared their practical experiences dealing with security policy from several points of view including creation, implementation and modification.

Next up was Alex Horan of Core Security presenting "Client-Side Penetration Testing." The basic idea behind client-side pen testing is to go after the user. Servers and networks still need to be pen tested, but most companies have done a great job in protecting those areas. Hackers know this as it has become increasingly difficult for them to use this attack vector. But it's the end-user that has been, is now and will always continue to be the weakest link in the chain.

Most of the presentation was explaining how to get into a corporate network through electronic social engineering. It was essential background information for the presentation, but, being a crowd of security professionals, it was nothing new. But the impressive part was when he took the examples (like getting an email seemingly from a co-worker with a standard company report as an attachment or a link to a malicious web site) and showed us how this can all be done within the framework of Core IMPACT.

This was a perfect lead-in to the Core Security sponsored "Capture the Flag" Hacker Challenge. The challenge was housed in a classroom where the computers were provided for the competitors and setup in advance with full versions of Core IMPACT. The challenge not only tested your basic skills as an ethical hacker AKA penetration tester, but it also was a showcase for some great new features in IMPACT including the ability to easily hack one computer and use it as the launching pad to hack another. Each of the boxes that needed to be compromised were multihomed, so if you didn't get into the first machine, you couldn't even find the second. Once on the third, it wasn't as easy as just opening a file and reporting your findings. There was an extra step needed to crack the message required for winning. Great stuff. Every participant in the event was given a signed copy of Daemon, A Novel by Leinad Zeraus, and the winners were given Amazon Gift Certificates. Our friends from the local Chicago 2600 club were the winners. Congrats.

That wrapped up a long day of security education and was an indication of the great lineup of keynotes and evening presentations in the coming days.

Final Thoughts

On a side note, I want to personally thank everyone who was so kind in their compliments of the event and giving of their time to make ChicagoCon happen. This event was formed not only on what I thought would be great, but also what numerous readers have shared with me. In the end, we had to make a number of hard decisions in the initial planning to ensure the future success of the event. You can't please everyone, but one can do their best. And when all is set in motion, you can only hope that others enjoy the end result of a vision that was initially formed years ago.

So when I saw a student pass by me on his way to class with a ChicagoCon badge around his neck while carrying a ChicagoCon bag full of all of the items I begged and pleaded to get from various third parties; that was too cool. That finally made it real for me. ChicagoCon is really happening and is here to stay!

Donald C. Donzal

Editor-In-Chief

The Ethical Hacker Network