DEFCON19 – Spy Vs Spy

David Holmes, 2011-22-08

I've been attending the DEFCON "Security Conference" (or "Hacker Convention") in Las Vegas since DC7. Here's my report from this year.

The Badges - "Wik" got his badge tattooed on himself

The DEFCON Hacker Convention continues to social-engineer its own attendees. After introducing the world to electronic badges years ago (a practice which is now widely copied), DC decided to go WAY old school. This year the badges were constructed out of commercial-grade sheet titanium. And since they had to made 10,000 of them, they ended up buying almost all the available sheet titanium in the country. The badges were designed to get attendees talking to each other, and it definitely worked.

Timothy studies the wheel

The Badges themselves were part of a giant puzzle that only insanely bright people could possibly finish in 3 days. The solution to the puzzle involved the badges, the schedule, several ciphertexts spread around the talks, sleeper agents among the crowd, a set of logic gates, and a crypto wheel laid down on the floor of the rotunda. In spite of all of these obstacles, several people were able to complete the puzzle, including this CalTech college kid named Timothy.

Without a doubt, the absolute best talk at DC19 was Moxie Marlinspike's "**The Future of SSL Authentication**" talk. His talk started with the hacking of the Comodo CA system (which we wrote about on our Security blog here). He made a convincing case that it is unacceptable that we have to rely on a certificate authority that is apparently cavalier about issuing bad certificates. One cannot just revoke the trust without "turning off" 20% of the secure sites on the Internet. So he introduced a new technology, called Convergence, (similar to SSH "Perspectives"), and released a FireFox plug-in for it. This simple technology literally has the ability to make CA's somewhat obsolete, at least if they don't start adding more value. At the Convergence.io site, one can download the source code and check it out. I must say, Moxie writes some tight code. Track down the video of the talk – it's definitely worth it.

Among the "awards" given out this year were the following highlights:

- Most Interesting Malware = Stuxnet

- Lamest Corporate Response to a Breach = RSA
- Most Epic Fail = Sony
- Best new Technology = Moxie Marlinspike's Whisper Systems

Out in Force

Elements from the Hactivist group Anonymous were in attendance. And, from talking with people, I'd say that everyone who was not a paid security professional was **definitely** leaning toward supporting Anonymous and their political agenda. There were a few LulzSec references around, as well.

The Jester vs Sabu

The most exciting drama at DC19 was the real-life "spy vs spy" game going on at the conference itself. Sabu, the former leader of LulzSec, a man whom the authorities would very much like to talk to to, was supposedly at the conference. Stalking him, trying to call him out, was none other than Pro-US lone gunman Th3J35t3r (The Jester). The adversaries stalked each other for four days, taunting each other via twitter. I ended up having a small personal connection with the stalking but I'll save that story for later...

On LulzSec and Cloud Security

Speaking of LulzSec, several of us attended the talk "3 generations of DDoS". There was a guest speaker from the cloud provider Cloudflare. Cloudflare could be described as "reverse Akamai" - they provide a combination of geographic DNS and caching, more like an ISP than a hosting service. Anyone can sign up their website for free Cloudflare support.

Interestingly, it turns out that the LulzSec hackers signed up for Cloudflare and thus, Cloudflare had to defend the LulzSec content from daily DDoS attacks (the Jester, perhaps?) for about 50 days. Cloudflare was able to absorb the attacks against LulzSec. The biggest attack against LulzSec came as retaliation for attacks against Minecraft servers. Don't mess with Minecraft!

Where are the POISONED apples?

Contests

F5 should be proud of its people; several F5ers entered the contests this year. One of the contests, "Capture the Packet", was **won by a pair of F5 Network Support Engineers.**

Threats at DEFCON 19

The collateral damage caused by the Hackers was **out of control** this year. Or perhaps, more accurately, the Rio hotel was not sufficiently locked down to host the world's premiere hacker convention. According to the volunteer network staff, there was **223 DoS attacks PER HOUR**. The hotel's **wired** network was hacked so hard that the staff apparently just unplugged the main switch because **I couldn't even get link** in my hotel room after the first day. Of course there were all kinds of rogue 802.11x wireless access points. Most impressively (and evilly, and illegally), there was apparently a CDMA rogue mini-cell used as a platform to man-in-the-middle Android phones. See here for details.. But **the lamest hack of all was to the elevators** to our rooms. In one bank of elevators, the System32 directory had been deleted. Thanks guys, now we can't get to our rooms. See actual screen shot above.

Conclusion

In every way, from the Speakers, to the content, to the Contests to the crowd, this was the best DEFCON I'd ever attended. Next year will be the 20th DEFCON and the Dark Tangent is planning on "blowing the doors off". Can't wait for the next one.

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com