

## Book Review: Kingpin: How One Hacker Took Over the Billion-Dollar Cybercrime Underground

Review by RichM

Kevin Poulsen has worked tirelessly to become a respected expert in the information security field and is a senior editor for Wired Magazine. Kevin edits the Threat Level Blog covering various topics mostly intersecting between law enforcement and hacking, but there are other relevant posts like the latest goings on with Wikileaks. The now white hat was not always on the straight and narrow and made a name for himself as his alter ego, "Dark Dante";

The legend of his "exploits" is well known and has him counted amongst America's most infamous hackers. Dark Dante's most impressive hack was when he used his phreaking skills to win a Porsche 944. He rigged the phone lines of an LA radio station, guaranteeing he would be their 102nd caller! Kevin Poulsen and Max Butler, the person on whom the book is based, have many similarities. Both are very skilled and have a natural ability, but while one was able to find legitimate work after a conviction, the other was not. It is because of Kevin's past that he can bring to life such a fascinating topic. Most mainstream reporters would (at best) turn this story into a 5-page magazine article, whereas Mr. Poulsen has created a suspenseful page-turner in Kingpin: How One Hacker Took Over the Billion-Dollar Cybercrime Underground.

[del.icio.us](http://del.icio.us)

Discuss in Forums {mos\_smf\_discuss:Book Reviews}

Max Butler (pictured on the right) is and was an idealist that simply wanted to help others. The problem is, he never recognized when he had gone too far, until, as they say, it was too late. One day while doing research he discovered a vulnerability in the Berkeley Internet Name Domain (BIND) Server. At first he was content to see others find it and report it, but once a weaponized version was found in the wild, Max felt a duty to act. He began patching every vulnerable machine that he could access. While this seemed like a benevolent act, Max also patched computers owned by the United States government and military. This was the end of Max Butler and any shot at a legitimate career in Information Security.

Once released, Max tried to find work in the private sector. His reputation was too far gone, and no one would even take a chance on him for minimum wage! It was at this point that Max realized the only way he could make money was in the carding world. He quickly climbed the food chain, first on someone else's site, then eventually his own. In a quest for power, he single-handedly swallowed the competition and became the only "reputable" site for stolen identities.

"Kingpin" is a 360 degree view of everything that was taking place in the carding community, before it was even something most people knew about. This book is a blow-by-blow account of all the dark secrets of how this world operated, the main players involved and what law enforcement did to shatter this world. It is also a frightening glimpse into the power that corporations had to keep breaches a secret. All the while millions of their customers' personal information went on auction in the black market, and the victims had no idea.

Consumers were lead to believe that in the beginning of the 21st century, the major threat to our personal identity was online; however, as you learn in Kingpin, the real threat was complacency on the part of the FBI (in not releasing names of compromised corporations) and the companies themselves for allowing their Point of Sales (POS) Systems to have little to no security. These machines continued to house data that they were not supposed to, and as such consumers who didn't even own a computer fell victim to identity theft through the gross negligence of brick and mortar operations.

Kingpin is a fascinating book, since, as an outsider to this world, I never had a great understanding of how carders operated. Throughout the book, it is apparent that there is no honor among thieves, and those that should be the most "trusted" are either back-dooring their customers and stealing whatever they can download or informing LE in an effort to either eliminate competition or reduce a sentence that is already pending. Another great feature of Kingpin is that it serves as a timeline of some of the most important/crucial occurrences in information security. In addition to covering some of the more high profile criminal cases it also shows well known exploits that were being leveraged with reckless abandon such as the Real VNC 4.1.1 vulnerability. I remember this exploit all too well as my department worked tirelessly to ensure that we took all necessary precautions to mitigate this vulnerability.

## Final Thoughts

If there was anything negative about the book, it is the lack of explanation of the various exploits, trojans and backdoors used by Max and his friends to own the carding world. Although there is some technical information including a brief explanation of PGP, this book gives a wider view of the world of identity and credit card theft. Knowing that the desired audience is broader than just us geeks, it is understandable, yet the lack of some more hacking details is still disappointing.

That being said, Kingpin by Kevin Poulsen (pictured on the right) is a great book and one of those you have trouble putting down. It is amazing that everything in the book is factual and not some piece of fiction. Kingpin joins the quickly growing list of InfoSec books that are accessible to the outside world.