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

Kevin Poulsen

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

Kevin Poulsen

Kingpin: How One Hacker Took Over the Billion-Dollar Cybercrime Underground Kevin Poulsen
The true story of Max Butler, the master hacker who ran a billion dollar cyber crime network.

The word spread through the hacking underground like some unstoppable new virus: an audacious crook had staged a hostile takeover of an online criminal network that siphoned billions of dollars from the US economy.

The culprit was a brilliant programmer with a hippie ethic and a supervillain's double identity. Max 'Vision' Butler was a white-hat hacker and a celebrity throughout the programming world, even serving as a consultant to the FBI. But there was another side to Max. As the black-hat 'Iceman', he'd seen the fraudsters around him squabble, their ranks riddled with infiltrators, their methods inefficient, and in their dysfunction was the ultimate challenge: he would stage a coup and steal their ill-gotten gains from right under their noses.

Through the story of Max Butler's remarkable rise, KINGPIN lays bare the workings of a silent crime wave affecting millions worldwide. It exposes vast online-fraud supermarkets stocked with credit card numbers, counterfeit cheques, hacked bank accounts and fake passports. Thanks to Kevin Poulsen's remarkable access to both cops and criminals, we step inside the quiet,desperate battle that law enforcement fights against these scammers. And learn that the boy next door may not be all he seems.

Kingpin: How One Hacker Took Over the Billion-Dollar Cybercrime Underground Details

Date	:	Published February 22nd 2011 by Crown
ISBN	:	9780307588685
Author	:	Kevin Poulsen
Format	:	Hardcover 288 pages
Genre	:	Nonfiction, Biography, Science, Technology, Mystery, Crime, True Crime, Computer Science, Computers

 [**Download** Kingpin: How One Hacker Took Over the Billion-Dollar Cy ...pdf](#)

 [**Read Online** Kingpin: How One Hacker Took Over the Billion-Dollar ...pdf](#)

Download and Read Free Online Kingpin: How One Hacker Took Over the Billion-Dollar Cybercrime Underground Kevin Poulsen

From Reader Review Kingpin: How One Hacker Took Over the Billion-Dollar Cybercrime Underground for online ebook

Ryan Lackey says

Great account of some of the carder underground, big carder sites, and scene drama. Particularly good because the author is from the underground and is now a journalist. Interesting too since I know a lot of the people and sites/systems involved.

Luis says

This is a quick read and it is really interesting to follow this guys story. Max Vision is fascinating to learn about, but equally interesting is learning about this huge intricate story that took place in our lives that we never knew anything about. I learned a ton about internet security through this book. It is a quick and interesting read.

Celeste Peterson says

My mom passed this book to me, along with numerous others about computer espionage and hacking. This one was a quick and fascinating read - on that nearly made by blood boil to learn how easy software companies made it to hack our personal computers and gain our credit card numbers as far back as the 1980s. It details the effort of an amazing FBI man to bring down a brilliant cyber criminal Max "Vision" Butler, also known as Iceman online. It's a fascinating look at how mag-wipe credit cards were first stolen, how the process evolved, and the first criminals to sell mass lists of data. While Europe and nearly every other country on the planet has moved past the easy to compromise mag-swipe credit cards to the highly secure pin and chip credits cards, the United States has not. Last Christmas my credit card info was hacked by the infamous Target breach. Sadly, the same month I read this book, I learned that it was compromised again by Home Depot. I called to complain loudly with my credit card company to move them to fight the cause and they sent me a pin and chip card. If every consumer called someone to complain maybe we could move the corporate giants to push forward the necessary reforms.

Jim Crocker says

This was a real compulsive non-stop read for me. I am fascinated by computer geeky stuff to begin with. However, Kevin Poulsen's writing is pretty smooth. The book focuses on the exploits of ace-hacker Max Vision. After serving nine years in prison, Max will be getting out just before Christmas 2018, which is right around the corner. Now maybe he's already out now. I don't know. But that was what I read in the book.

My opinion is that all these hackers have pretty much destroyed the Internet, which many claim to love, with their dirty deals and dirty tricks. Why they think they are being so cute certainly beats me. Computers and the Internet offered me a great time working on database development projects all over the US and the UK. Now I build websites for fun and write books, all thanks to computers and the Internet. Otherwise, I have no

idea what I would have been doing. Probably nothing good.

This book should be a real eye-opener for those who don't understand the extent to which the Internet has been corrupted. Most recently, Net Neutrality has gone down the tubes. Policing and use restrictions will become the future and folks will gripe and complain about that.

Thank a hacker! What a shame and waste of talent and perseverance, just to show the world that you are a smart-ass.

Nathaniel says

It's a little weird to file a book on my "history" shelf when the primary subject of the book was born less than 10 years before me and is still 2 years away from finishing his prison sentence, but things change fast in the Internet Age, and this book is a great example of that.

It's the story of a Max Butler, the kind of person that makes people use words like "troubled." I really did recognize an awful lot of Max's high-school days from my own circle of friends. I was a tame kid, but there were definitely boys in my high school circle who exhibited Max's distinctive blend of manic intelligence and abysmal impulse-control. It was just one more way that reading this book felt, for lack of a better word, almost nostalgic.

Kevin Poulsen didn't really ever go into this, but the rise of credit card scams and identity theft through the 1990s and into the 2000s was also, in a way, the history of the rise of the mainstream Internet. Every time the story moved forward a year, I would think about the types of computers that were cutting edge that year, the Internet sites that were big that year. The book even mentioned quite a lot of definitive events in the Internet Age--like when Metallica's "I Disappear" leaked online, leading the band to sue Napster--that I remembered vividly.

On the other hand, there was an awful lot of information in this book that I didn't know anything about. That's not a coincidence, either. Poulsen mentions in passing how industry trade groups deliberately suppressed data about the extent and nature of credit card theft, pretending to the world that theft was a minor problem and relegated primarily to online shopping when in fact fraud levels were skyrocketing and were primarily a result of brick-and-mortar stores being hacked, not online sales getting compromised.

I wouldn't say the story was exactly riveting--credit card theft is not exactly high-stakes, as world events go-- but it was definitely engrossing. The constant squabbling among the various thieves--and especially their territorial disputes over masculine reputation games--was interesting and also kind of sad. It felt, in a way, like a primatologist's field notes on a particularly quarrelsome band of chimpanzees.

I guess, in the end, it was mostly just a story that I already knew too well to find really revelatory. I'm not an Internet security expert by any means, but I am familiar with how shockingly irresponsible most companies are when it comes to IT security, and so the news that hackers could easily use know-exploits to seize control of computers around the world is not remotely surprising. The problem is: most people don't like their day job (shocking, I know) and so they only do the minimum amount required. Contrast that mediocrity with the fiendish delight some hackers take in simply going where they're not supposed to be allowed, and there really is no contest. Hackers--dedicated, zealous, and innovative--are going to win out over underpaid, bored employees any day of the week. And then the rest of it--the way that what we do on the Internet can become

divorced from our real lives, and how our personalities can bend and morph and even detach completely from our real-world personas as they stretch and distort to suit digital environs--is also not shocking. It's the same thing everyone who grew up at the dawn of the Internet Age learned.

And so I guess that's why I'm going with three stars. It was moderately interesting, but the events and the personalities themselves are just not compelling or surprising or significant enough for someone already familiar with the basic subject matter. Everything and everyone is basically exactly what you'd expect. What a book like this needs, I think, to really become something special is some kind of analysis or insight to tell us what these events mean about society, or how they tie in to geopolitical tensions between the US and Russia or China, just something *more* than a recitation of the fact that bad guys like to steal your credit cards.

Max is an interesting character. His white hat / black hat personas are interesting, but--there again--not really surprising. He wasn't ever a bad guy, really. He was just good at rationalizing, bad at impulse control, and found a medium--the Internet--that's uniquely suited to dissociation. Telling his story like he's the exceptional case isn't the right move, I think. Telling his story as emblematic of all of us in a digital age might have been a better approach to take. Because he's not unique. He is who we all are, with our multiple online identities, our curated and context-dependent personas, and our cyborg inner lives.

Joe says

This book explores part of the world of modern cybercriminals.

I tend to think of the "old school" of computer "criminals" as mostly people that were interested in technology, wanted to explore, and just didn't care laws -- but generally not interested in directly stealing money from people. At worst, they would profit by doing things that they didn't consider stealing: for example, taking over a radio station's phone lines to guarantee that they would win a call-in prize.

The newer versions of cybercriminals really are just interested in stealing money: getting lists of credit cards, and turning those into actual dollars. People have been abusing credit cards for as long as they've existed, but recently the criminal activity surrounding them -- stealing the numbers, producing fake credit cards, buying products, turning that into laundered money -- has become very organized.

And thus, this book: it describes some of the central players that helped set of some of the largest discussion forums and computer-based credit card fraud marketplaces: people could buy or sell cards, equipment, and services.

The book theoretically focuses on one, or a few, characters ("how one hacker took over...") but in reality, many of the people involved in organizing smaller criminals knew each other, and interacted on a regular basis, and this book describes many of them.

The topic is pretty incredible: the way that the criminals would wait for a new security flaw to be discovered, and then take a shotgun approach to snagging as many people as possible. If virtually all of the potential targets evaded the attack, no matter -- the net was cast so wide, a few would get taken in. Then, it's sort of fascinating to see how the people would operate: given that their career was theft, it's not surprising that they would turn on one another, but they do it so quickly -- even going so far as to attack each other's computers.

The book itself is not bad, but it does seem a little disorganized. The author was involved in the computer

underground previously, and recently involved himself in the computer deception that eventually caused Bradley Manning to be arrested for involvement with Wikileaks, so he's got the right background -- I just wish the book itself had a little more focus.

Katherine Tomlinson says

Poulsen's name may be familiar to those who follow cyber-crime. He was a notorious hacker in his own right before serving time and emerging a WIRED correspondent. He knows the sub-culture of hacking, and that really makes this story feel "inside." This is not the most "active" story, but it is one, like SOCIAL NETWORK, that takes us inside the minds of some brilliant people; introduces us to an intriguing world; and plays out cops and robbers in an entirely new way. And in a time of wikileaks, the story is totally current.

Peter says

If you're interested in cyber crime, hacking, online and banking security, this is definitely an interesting read. It mostly tries to be a biography of one of the more prominent hackers who ended up organizing a large group of cyber criminals. So if you enjoy biographies, this is also a quite well written one in my opinion. However, if you're like me, who doesn't enjoy biographies much and is only moderately interested in cyber crime, then it's just a decent book that tells a decent story with some cool anecdotes here and there.

The biographical nature of the book makes sense, since it allows the reader to have an anchor while traversing the three decades worth of cyber crime. So it kind of irked me that towards the end, it started going all over the place, detailing exploits of numerous other cyber criminals that only loosely connected to the main character. I think the inconsistency was more of an issue than the actual content, since I actually preferred the latter part of the book.

On the technical side, the writing was solid and the length was spot on: not too long that it felt boring and not too short that you were left wanting more. The story was quite predictable, but it's hard to be too critical of that since it is a true story after all. I didn't really care about any of the characters and their problems, but that might also be a personal bias since the stuff they do is quite annoying to most people. I also felt the book was a tad biased towards law enforcement and a bit naive in general on the state of cyber crime which I felt was a bit dishonest.

Overall, it was a good book that I generally enjoyed and which had only minor, mostly nit picky issues. If you like biographies and cyber crime themed books, this will probably earn a higher rating from you, but I don't, so it gets a fair three stars from me.

♥Xeni♥ says

Wow... what a powerful book! I noticed this on my friend's book update feed yesterday, searched around for an ebook, found one, started reading, and practically didn't even stop for much else. (Although there was a 16 hour break in between reading there :P)

Normally I don't like nonfiction books: they are dry, not engaging and just don't deal with subject matter in an interesting way that I can absorb readily. This book reads more like an action novel filled with tons of real life tidbits. I think the tidbits are what I enjoyed most. Travelling through the decades of hacking took me back to my own misbegotten youth (especially when Back Orifice was mentioned being released at DefCon!) but it was also a bit of a look into the movie Hackers, Hackers 2 and so forth. Just that this book continued up until right now (it even included a footnote at the very very end about the recent Wikileaks hack.)

All in all, this is a great book for learning about the huge world carding scams out there (descriptive enough to make you never want to use a credit card in America again until they change the system), about the main hackers on the scene and in between filling in your tech knowledge gaps (for instance, it explained SQL in a few short, very easy to understand paragraphs. Anyone want to change the Wikipedia article to make more sense??)

All in all, a very well written book, that I felt really covered the whole area of hacking while still maintaining a somewhat unbiased point of view. I thoroughly enjoyed it!

Greg says

Inside look at the cybercrime underworld, specifically carders (people who steal credit card information). Book is really well written and hard to put down, and additionally it actually manages to cover the technical parts in enough detail to be interesting without being boring. Book follows the life of Max Burton and how he came to rule the carding world. Interestingly, he started out with light stuff, got in trouble, and went white hat for a while. But when the FBI wanted him to inform on one of his friends, he refused and got put in the slammer. It was there that he turned black hat once more, and once out of jail started getting into carding.

It was surprising how technically inept the supposed other hackers who made up the carding population were. Most were running skimming operations (stealing magstripe data by literally swiping cards, usually with an inside person at a restaurant), but otherwise were not skilled at computers. Max was able to easily hack those people and steal their card information before they could resell it. Even the guys who were running the carding forums where all these people met were no better. After Max was able to hack into some of their computers/accounts, it was pretty easy for him to take over their forums as well. In fact, of all the characters in the book, only a couple of people, Max included, actually sounded like they could legitimately break into other peoples computers.

It was also pretty alarming how widespread this kind of crime seems. There are break-ins and thefts of credit card data all the time. The people who buy the stolen credit card information then buy lots of goods at stores, and resell them on eBay in order to make a profit. Their favorite items are things like expensive handbags and electronics - basically big ticket items. So now I wonder how many outrageous deals I see on Craigslist or eBay are actually just carded goods. It's also sad how many break-ins and thefts of credit card data happen. Most of it is just due to how poorly secured most corporations are (even some big ones), that once you break into their corporate network (and many have B&M branches that are wired into that network) it's possible to steal credit card data. I guess it's just insane to me that they have credit card data in the clear, stored on their network. That should never happen.

But it was due to poor security practices that Max was able to find most of his card data. The main exploit the book details is how small restaurants like pizza places, who really can't afford to hire anyone technical, use a POS that stores credit card information accumulated during the day, and waits to transmit it all at night

to the processing center. The full magstripe data is stored in the clear in text files on those computers. Many of them also do not delete old text files after they're no longer needed. Max was able to find and break into these computers, giving him lots of fresh card information. Part of the exploit detailed was a VNC vulnerability that sounds so silly it's hard to believe anyone could be so incompetent to actually have implemented it. Basically, the handshake between a VNC server and client involves the server telling the client what protocols it wants, and the client picking one of those protocols to actually use. However, the implementation used on most of the POS's (VNC was installed to allow remote administration) didn't check that the protocol the client passed back was actually on its list of accepted protocols. Therefore, you could hack a client to pass back protocol 1, which requires no authentication, and the server would gladly open a password-less connection.

One other thing from the book that stood out to me was how vulnerable client machines are to being hacked. There were multiple exploits detailed in the book, mostly on old Windows software, that would allow an attacker to take control of a machine, and all that was required was that it visit a compromised webpage.

There are lots more details in the book about Max's multiple identities, different vulnerabilities, and just loads more detail, but it'd be too much to try and capture here. Needless to say, this was an easy read and a really enjoyable book.

Rob says

Executive Summary: A fascinating and terrifying look at the darker underbelly of the internet and identity theft.

 Full Review
I consider myself fairly knowledgeable about computers and the internet. Computer Security has never really been my thing though. Yet for whatever reason I find reading books about computer crime fascinating.

This book is no different. Kevin Poulsen has turned himself from one-time hacker into a leader in covering computer security. I occasionally read some of his articles on Wired. I like getting the take of someone whose been there before on things. It seems like he's good about not just presenting the facts, but the reasons behind them. He really gets into Max Butler's head a little and presents a more complete picture than you might get from a different author.

I had read a little here and there about carding over the years, and I had vague recollections about the Dark Market, but I never really knew any of the details behind that bust. When comparing law enforcement in this book to that of The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage it's like night and day. Of course 20 years have passed, but they really had some clever approaches to tracking and eventually capturing some big players in the cyber crime world.

It's scary to learn just how easy it was and continues to be for people to steal your credit card information, and that the credit industry in the US refuses to change magnetic strips simply because of the upfront cost to replace the machines is so high they prefer to deal with the cost associated with the theft instead. I don't know what it will take to finally force a change, but meanwhile innocent consumers continue to have their lives upended by it.

I didn't find this book too technical, though given my background, I'm usually a bad judge of these things. I

think anyone who understands the basics of the internet would be able to follow along. It's really more a character study of Max Butler and others than it is a detailed account of how he did it.

Overall another fascinating read.

Nick Black says

still too pissed off about my lost hour reviewing Hitch-22 to properly write; suffice to say that this is the best true hax0r crime book written as of April 2011 -- yes, i have read them all (previous title holder: The Hacker Crackdown. it pleases me to no longer need praise anything by confirmed mountebank Bruce Sterling, though he's been replaced by charlatan Kevin Poulsen....whom I think I must reassess).

so much nostalgia. i knew two characters, peripheral but named, personally, and half-expected to see my first, favorite and most successful startup mentioned on any page. poulsen gets it all right (ahh, the MSR206, how many lives did you change for better and worse?), from details historial to cultural to psychological. great book, save that game time's no more than about one hour.

----
http://garwarner.blogspot.com/2011/03... very solid review here, and i dig poulsen's "THREAT LEVEL" blog on wired. it's always amusing if nothing else. poulsen might be a big douchebag (see The Fugitive Game), but he did give us this awesomeness:

Sam_Hamrick says

Fairly intersting book. The work done by Kevin Poulsen to find all the necessary materials for the basis of the book is really impressive. He tells about fraudulent life, which takes place right in front of common user's life - on the screens of our PCs. There are no classical war between mafia or gangs in this book. Instead, we see, how hackers keep doing their dirty deeds simply sitting on front of the screen. Nonetheless, the effects of this deeds some times cost much more, than any others. In addition, the sty?e of the book looks similar to another investigation by Wired - the one about the Silk Road (https://www.wired.com/2015/04/silk-ro...) - which took place a few years after the events, described in this book.

Jacques Bezuidenhout says

This would be 3.5 Stars.

Although I really enjoyed the book, they seemed to have over simplified some things.

I'm not sure if it was the narrator or the biography form of the book, but the way it was told didn't quite grab and keep my attention, I found myself drifting away a lot.

Some things getting explained in the book like the Bind hack that didn't have a checksum and you could

append extra bytes to the end of you post to run code, and the way they explained SQL injection was really well written. Short paragraphs explaining the just of the technicalities.
(view spoiler)

It was interesting to see that it doesn't really matter how secure/safe you try be with your own cards, the bridge in security will most likely not happen on your side, or with your online usage.
(view spoiler)

Some of the hacking also seemed over simplified, although some of the initial phases of security probably was that easy to compromise.
(view spoiler)

I liked some of the white-hat initiatives of warning people about security loop holes before publishing it.

This book really makes you think whether you are doing enough to safeguard your own data, and keeping up to date with security.

(view spoiler)

All in all a worth while read.

Ron Quartel says

Good read. Gives you insight into how fragile the swipe system of credit cards is. The USA was the only country left using it - because the cost of changing the system his higher than the losses in fraud. Thank you American banks - please may I have another. The US has finally moved to chip and sign. Hopefully, they will move to chip and pin soon to help further protect its citizens from identity and financial theft. Then again - the US is still on Imperial measurements...