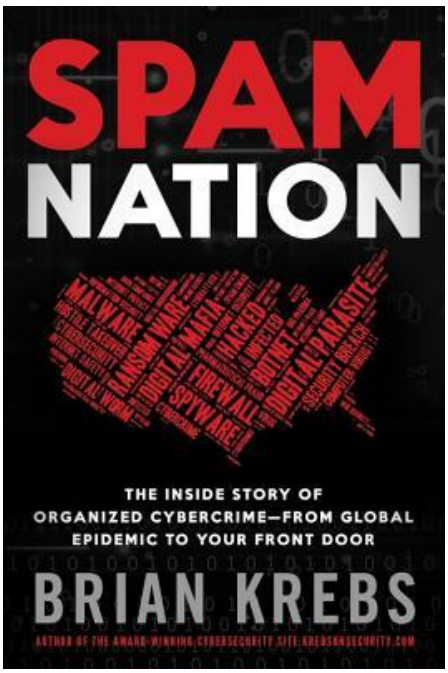

Spam Nation: The Inside Story of Organized Cybercrime — from Global Epidemic to Your Front Door

Brian Krebs

From Reader Review Spam Nation: The Inside Story of Organized Cybercrime — from Global Epidemic to Your Front Door for online ebook

Jacob says

To me, the subject matter of this totally hooked me: what is the source of spam sent worldwide? Why is it profitable for them? Why is spam not nearly the problem it used to be? Fortunately, the author provides plenty of answers to those questions. In addition, he recounts a feud that started between two of the most prominent spammers that ended up with both of them kind of destroying each other and causing significant damage to the spamming industry (not that most of us are sad about that). It's very interesting to know how spammers operate, how they make their money, and how much of the system was taken down.

The writing leaves a little to be desired, particularly towards the beginning where Krebs thrashes around a bit to try to give you a perspective of the whole spamming industry. I expect better writing, even for a journalist, and Michael Lewis is a good example here. Krebs gets onto better ground when he recounts several examples of people he tracked down who purchased things from spam emails and why. The rest would be better if he could tell it like it was a story too. Also, due to some repetition from one chapter to a next, the book has the feel of a series of blog posts or articles that got combined to form one book. It would have been better maybe with some better editing to cut out repetition, or more material written to connect one chapter to another.

Most people won't share this personal connection, but I also enjoyed the large amount of attention paid to UCSD Computer Science & Engineering department professor Stefan Savage and his efforts to identify how spamming works and how to disrupt its economics.

Rob says

Executive Summary: Interesting read, but a bit too much of Mr. Kreb's personal story in places. 3.5 Stars.

Audio book: Christopher Lane does a decent job. He has a passable Russian accent, but for some reason he didn't always use it for the Russian characters. I wouldn't have done this in audio except it was on sale. I wouldn't bother with the audio book otherwise, and you'd be better off borrowing this from the library.

Full Review
I continue to be fascinated by computer crime. This is another interesting book in that realm, though not as much as Kingpin: How One Hacker Took Over the Billion-Dollar Cybercrime Underground.

This is far from technical, and I think that's fine. Mr. Krebs gives you the basics on botnets and some of the other techniques common for spammers without going into too much detail to scare the layman off.

If I have one real complaint about the book is that Mr. Kreb's spends too much time talking about himself, especially at the start. I understand that he plays a part in the story, but he spent part of an early chapter complaining about how the Washington Post would make him sit on stories for month due to red tape and legal concerns.

I never really knew the main players in the spam game. I still really don't. That isn't Mr. Kreb's fault though.

I'm just really bad at names. He does list them out in the front of the book. Most of the people here were interchangeable to me. This likely wasn't helped by the fact that I did this in audio. It would be nice if the list of people came as a pdf for reference.

I still found it interesting. I guess I never realized just how much of spam was driven by online pharmacies. I haven't really had to deal with spam in years. I almost never wander into my spam folder looking for legitimate email.

It's interesting that there is a legitimate market for this stuff. It just goes to show the lengths and risks people will take when they can't afford proper health care and medication.

Overall I'm glad I picked this up, but it probably would have better borrowed than bought.

Audrey says

While this book was published in 2014, there’s been plenty of new cybercrime that’s popped up since then. I suggest following Brian Krebs’s blog to keep up to date. Krebs started off as in investigative reporter but left to run his own blog when his articles became too hot to handle for the paper.

The book follows the history of email spam in its heyday. It’s actually been declining in favor of phishing, ransomware, and other scams.

It turns out the vast majority of spam came from Russia from only a handful of people. They viewed spam as legitimate advertising for prescription drugs, porn, and fake antivirus programs (scareware), especially drugs. Enough people buy spammed products for it to be a lucrative business.

Researchers concluded that spam—and all of its attendant ills—will remain a prevalent and pestilent problem because consumer demand for the products most frequently advertised through junk email remains constant.

Spam was seen as more of a nuisance than a threat, even though spammers infect personal computers and use them to send spam. Krebs had an incredibly difficult time getting spam-sold pills tested. Drug companies were also to crack down on spam since some of the drugs were safe enough.

Incredibly, the [University of Alabama at Birmingham] researchers have legal approval from federal regulators and law-enforcement agencies to test and handle highly controlled and illegal substances, such as cocaine, heroin, and a methamphetamine, but they had not yet received permission from the FDA and DEA to test pills ordered through junk email.

Spam rivalry seriously hurt the spam industry, and when the credit card companies got involved, they took a big hit.

So it’s an interesting history and not quite what I expected. I was most interested in who was buying from spam and why. I would have liked to hear more about the anti-spammers and their efforts. The spammers themselves were not that interesting.

Recommended for anyone interested in computers and cybercrime. Editing is pretty well done. There is some strong language in quoted material.

Book Blog

Gwern says

(2h; ~73k words) Journalistic account of Brian Krebs's (Wikipedia, blog) experience with some Russian spammers & associates.

Krebs has been engaged in a little war with Russian spammers: getting onto their forums, looking for weak points like abuse-friendly ISPs or payment processors, and blowing the whistle on them; he's been heavily aided by the feuding community leaking lots of information and vouches to him, and the book revolves around one he's hyped up as the 'Pharma Wars'. All the leaks means he can do an unusually thorough job of documenting it and the principals, and the involvement of the Russian government in the e-crime scene. My own interests are mainly in the Western darknet markets like Silk Road, and in the pharmacy affiliate networks which were one of the main routes for buying modafinil up until recently, so while Krebs doesn't go into nearly as much detail as I would like, it's still a fairly illuminating read. Few Westerners have as much experience with the area as he does, which makes it worth reading for anyone interested in this niche, and certainly it's easier to read the book than try to piece together everything from his blog posts.

One downside is that the book comes off as a bit stream of consciousness and disorganized: there seems to be a rough chronological order, but not much of one; and a few diagrams of all the overlapping people and organizations (as well as a flowchart of the spam process) would probably be helpful. And I used the word 'journalistic' deliberately: Krebs's writing is purple and sensationalistic. Something is not 'terrifying', it is 'truly terrifying'; spammers are not a nuisance, but they become "potent threats"; in describing the fall of a small plurality source of spam (~20%, I believe he estimates), "consumers all over the world were enjoying a brief reprieve" from "the spam email empire". His overheated writing aside, his own sources make the case that spam is not that important; eg towards the end:

> Vrublevsky and Gusev's Pharma Wars were extremely costly for the spam industry, and their internecine war cost everyone in their business plenty. The two are now widely reviled on cybercrime forums for costing spammers tens of millions of dollars in profits, and for focusing attention from law-enforcement officials and security experts on individual spammers. "These two fuckers killed the spam business," Vishnevsky said in a May 2012 interview. "It was never super profitable for most guys; maybe five to ten guys earned really good money with spam. But after Pavel and Gusev started their war, everyone started thinking that every spammer is a millionaire and started hunting for spam and spammers."…Legitimate high-tech and well-paying programming jobs are increasingly available to talented coders in Moscow, and many of his longtime employees have been hired away to legitimate jobs in Moscow's young but promising tech sector. "Many representatives of the underground can't find good coders now, because their salaries in Moscow are much more than you can earn with spam," Vishnevsky said. "This business went to shit when Pasha [Vrublevsky] got busted. If Pasha and Gusev [had] not start[ed] that stupid war, everyone would be much happier." Vishnevsky's criticism may be harsh, but it is hardly an exaggeration. The spam industry has indeed taken a huge hit in the past few years. Prior to SpamIt's closure in October 2010, the volume of spam sent

> worldwide each day hovered at around 5.5 billion messages. Since SpamIt's closure, however, the volume of global spam sent daily has been in marked decline. According to Symantec, by March 2011, spam levels had fallen to just over one billion junk messages per day, and the total has hovered at or very close to that diminished level ever since.

(If spam is at 1/5 peak and even at the peak it was 'maybe five to ten guys'…)

In other spots, Krebs makes mistakes or does not exhibit as much critical thinking as one would like: the illustration of the horrors of designer drugs is the infamous 'causeway cannibal' (except that that wasn't bath salts, that was marijuana - and Krebs even acknowledges his mistake in a footnote! So why on earth does the main text confidently say he "turned into a real-life zombie after ingesting prodigious amounts of "bath salts""?); when discussing the online pharmacies, he repeats idiotic pharmacorp talking points like "8% of the bulk drugs imported into the United States are counterfeit, unapproved, or substandard" without pointing out that no one actually cares about the fraction that are "counterfeit [or] unapproved", and mentions that Marcia Bergeron's poisoning death is "almost always recited in some form whenever experts allied with the pharmaceutical industry talk" without asking the obvious question if the online pharmacies are so dangerous, why is only that story 'almost always recited'?; it's interesting that there's no mention of Kaspersky Lab's connections to the FSB and why Krebs was being wined and dined by Kaspersky personally; there is a bizarre lack of mention of Bitcoin except for a throwaway line about Russian forums, which is particularly bizarre given that he discusses the rise of ransomware (now often Bitcoin-using) and seems to agree with the interviewed Russian spammers at the end that going after credit-card payment processors has effectively killed the industry (which would be an unwise prediction if they can move to Bitcoin, as many of the online pharmacies have begun to).

Further reading:

"PharmaLeaks: Understanding the Business of Online Pharmaceutical Affiliate Programs"
"Pick Your Poison: Pricing and Inventories at Unlicensed Online Pharmacies"
"Structuring Disincentives for Online Criminals"
"The Partnerka—What is it, and why should you care"
"Click trajectories: End-to-end analysis of the spam value chain"
"An analysis of underground forums"
"Folex: An analysis of an herbal and counterfeit luxury goods affiliate program"
"Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace"

Some key authors:

Nicolas Christin
Nektarios Leontiadis

Mo says

Very interesting story about two spam kingpins destroying each other. Definitely shows you another side of spam that I don't think most people know or understand. The story was captivating, but the author struggled with sounding egotistical, though I don't think he is, having read his blog for a while now. I think he made a good attempt at making the story exciting. Had he simply retold information, it would have been boring, but he didn't find the right balance between telling an excting story that he plays a major roll in and sounding self-aggrandizing.

Definitely worth a read if you're interested in cyber security or the internet underworld.

Atila Iamarino says

Um livro um tanto ultrapassado (muito por obra do autor) contanto como começou e como foi o auge do spam de medicamentos por e-mail. Um assunto um tanto específico, mas bem contado e escrito por alguém que realmente entende sobre o que está falando.

Legal para quem quiser entender um pouco do cenário de cybercriminals russos, botnets, spam e quais são as demandas de mercado que geram spam de medicamentos. Vulgo, o preço dos remédios nos EUA.

Will says

Overall, this was pretty good, 3.5 stars, but I'll round up.

I think it fell a bit into the pitfall that some non-fiction writers fall into in terms of following the narrative of such a small number of people; I would have liked to see more about other folks involved in the spam wars (including anti-spammers), but I understand why the book was structured the way it was.

For the most part, Krebs does a good job of not getting bogged down with technical details, but still explaining technical matters in a way that's correct, but also understandable to non tech sorts.

There was a bit of repetition, and I felt some parts dragged on a bit.

RC1140 says

A really well structured and informative book into the underground dealings that are always happening but we are not aware off. The coverage was excellent and thought provoking giving you all the information you need even if you are not intimately informed about spam or cyber crime. It is always motivating that after reading a non fiction book like this that I find myself motivated to research more on the topic since it shows just how well the author captured my attention and allowed me to fill some of the slightly less detailed areas with my own research (this is for obvious reasons as the book would have needed to be extremely long to cover everything in detail).

The style of writing was also really enjoyable with the only reason it didnt get a 5/5 was because remembering some of the character names are kinda hard (they are all russian so its not really the authors fault), this issue is also probably only an issue in the audiobook since its easier to visually recognize some of the names and attach meaning to them , than it is to hear the names and attach meaning.

Scott Baxter says

Fascinating subject, less than stellar execution.

This book illustrates just how difficult it is to write a first book, even if the author has a long career as a writer writing short pieces. Krebs has trouble deciding which things require longer explanation and which can be glossed over. For example, at one point he points out the importance of understanding what IP addresses are, but Krebs would have done well to spend much more time going into detail about what an IP address is, why it is important to understand their meaning, how they can be spoofed, and how much time security researchers spend trying to discover the true IP address of a server. I also thought that Krebs would have done well to greatly expand his final chapter in which he describes what one as an individual computer user can do to be safer.

There are other, less important problems, that marred the book. These include:

* trouble using metadiscourse to signal things coming in future chapters or to refer to earlier chapters. Krebs is less than elegant here.

* trouble referring to himself consistently and elegantly.

* trouble referring to published literature. Krebs seems to never be quite sure if his audience is a technical computer science security community or a more general audience.

* related to the last point, I found Krebs endnotes annoying and, at least in my opinion, the book would have been better if Krebs had integrated them into the main text. Part of my problem may have been related to reading the text in ebook format, although it was not that difficult to toggle between footnotes and main text on my kindle paperwhite.

Despite these issues, I did enjoy the book. Krebs is well positioned to inform the world of casual computer issues about a critically important subject. I , for the most part, did enjoy the book.

Jean says

Even though we have good filters on our e-mail programs these days and no longer see all the spam, the author maintains it is a critical problem. Krebs claims the crooks are no longer content with standard commercial fraud, e-mail criminals infect millions of computers worldwide with toxic digital parasites, designed to extort our wealth and steal our personal data.

Krebs states that Russia is the key spam Nation with skilled hackers and corrupt police and is now the global epicenter of cyber crime. Krebs says Visa and MasterCard are starting to successfully shut down spammers. The author says Microsoft and other such companies are becoming successful shutting down “botnets.” Krebs tells of the frightening world of cyber criminals and reveals some of the success in fighting it.

The information is interesting but the author had problems staying focused on the main topic. The writing was jerky at times making for a difficult read but the topic was interesting enough to overcome the writing difficulties. I read this as an audiobook downloaded from Audible. I am glad I listened to this book rather than read it because of all the Russian names. I would not know how to pronounce them. Christopher Lane narrated the story.

Rick Howard says

Executive Summary

In Spam Nation, Brian Krebs covers a key portion of our cyber security and cyber crime history: 2007–2013, that period when we started to learn about the Russian Business Network, bulletproof-hosting providers, fast-flux obfuscation, criminal best business practices, underground cyber crime forums, and strange-sounding botnet names like Conficker, Rustock, Storm, and Waledac. This period just happens to coincide with Krebs's rise in popularity as one of the leading cyber security journalists in the industry. His relationship with two competitive pharmaceutical spammers—Pavel Vrublevsky and Dimitry Nechvolod—is a big bag of crazy and is the key storyline throughout the book. The competition between Vrublevsky and Nechvolod escalated into something that Krebs calls the Pharma Wars and Krebs gives us a bird's-eye view into the details of that escalation that eventually destroyed both men and the industry they helped to create. Krebs's weird symbiotic relationship with Vrublevsky is worth the read by itself. Spam Nation is definitely a cyber security canon candidate, and you should have read this by now.

Introduction

I have been a fan of Brian Krebs for many years. His blog, Krebs on Security, has been a mainstay of my recurring reading list since he started it in 2010 and even before when he was writing for The Washington Post. Since he struck out on his own, he has carved out a new kind of journalism that many reporters are watching to see how they might duplicate it themselves as journalism transitions from dead-tree printing to new media. Krebs's beat is cyber security, and he is the leading journalistic authority on the underbelly of cyber crime. Spam Nation is a retelling— with more detail and more color—of some of the stories he covered from 2007 until about 2013 on a very specific sub-element of the cyber crime industry called pharmaceutical spam.

Many security practitioners will hear the phrase "pharmaceutical spam" and immediately start to nod off. Of all the problems they encounter on a daily basis, pharmaceutical spam is pretty low on the priority list. While that may be true, this subset of cyber crime is responsible for starting and maturing many of the trappings that we associate with cyber crime in general: botnet engines, fast-flux obfuscation, spamming, underground forums, cyber crime markets, good service as a distinguisher of criminal support services, and bulletproof-hosting providers.

The Story

The story really begins with Krebs's weird symbiotic relationship with Vrublevsky (a.k.a. RedEye and Despduck). Vrublevsky was a Russian businessman and cofounder and former CEO of ChronoPay, the infamous credit card processing company that initially got started in the rogue anti-virus industry. I think it is safe to say that in his heyday, Vrublevsky was a bit of an extrovert. He followed Krebs's blog religiously and would instigate long conversations with Krebs on stories that were fantastical, true, and everything in between. Vrublevsky would feed Krebs half-truths about what was going on in the industry and left it to

Krebs to sort it out. Vrublevsky's downfall was his deteriorating relationship with his former partner, Dimitry Nechvolod (a.k.a. Gugle).

Vrublevsky and Nechvolod founded ChronoPay together in 2003, but by 2006, Nechvolod had left the company to pursue his own interests. He started two pharmacy spam operations called GlavMed and SpamIT. Because of the competition between these two men, the situation escalated out of control to something that Krebs calls the Pharma Wars, which ultimately scuttled the entire pharmaceutical spam industry, not just Vrublevsky and Nechvolod's operations, but everybody else's too.

Krebs's main sources of information for this book came from leaked customer and operational databases from these two men. Although Vrublevsky and Nechvolod never admitted it, they both stole the other's data and leaked it to Krebs. Krebs had many conversations with both Vrublevsky and Nechvolod about their side of the story, and Krebs even traveled to Moscow to interview Vrublevsky personally. From these conversations and other research done by Krebs, we get an inside view of how cyber crime operates in the real world.

Krebs set himself seven research questions:

• Who is buying the stuff advertised in spam and why?
• Are the drugs real or fake?
• Who profits?
• Why does the legitimate pharmaceutical industry seem powerless to stop it?
• Why is it easy to pay for the drugs with credit cards?
• Do customers have their credit card accounts hacked after buying?
• What can consumers, policy makers, and law enforcement do [about this cybercrime]?

For the most part, he answers all these questions. I will not spill the answers here, but I will tell you that I was surprised by every single one. I thought I knew this stuff, but Krebs provides the insight and research to make you re-evaluate what you think you know about illegal pharmaceutical spam operations.

Spam Nation is about the Brian Krebs's story too. Traditional journalists reading this book are going to hate the fact the he plays a key role in most everything that he talks about in this book. His original reporting on bulletproof-hosting providers operating in the US and elsewhere—the Russian Business Network (RBN), Atrivo, and McColo—became that catalyst that eventually got them shut down. This got him noticed by Vrublevsky and started that weird relationship that ultimately led to Krebs receiving the databases from Vrublevsky and Nechvolod. It also led him to leave The Washington Post and to start his Krebs on Security blog.

In the background, Krebs introduces us to the key players involved in the development and operations of some of the most infamous botnets that have hit the Internet community in recent history:

• Conficker worm (author: Severa; infected 9-15 million computers)
• Cutwail botnet (authors: Dimitry Nechvolod (Gugle) and Igor Vishnevsky; 125,000 infected computers; spewed 16 billion spam messages a day)
• Grum botnet (author: GeRA; spewed 18 billion e-mails a day)
• Festi botnet (operators: Artimovich brothers; delivered one-third of the total amount of worldwide spam)
• Rustock botnet (author: COSMA; infected 150,000 PCs; spewed 30 billion spam messages a day)
• Storm botnet (author: Severa).
• Waledac botnet (author: Severa; spewed 1.5 billion junk e-mails a day)

From my reading, Krebs's unintentional hero of his story is Microsoft. While Vrublevsky and Nechvolod

were tearing each other apart and Krebs was trying to sift through what was true and what was not, Microsoft and other commercial, academic, and government organizations were quietly dismantling the infrastructure that these and other illicit operations depended on:

• June 2009: 15,000 illicit websites go dark at 3FN after the Federal Trade Commission convinced a northern California judge that 3FN was a black-hat service provider. NASA did the forensics work.
• November 2009: FireEye takes down the Mega-D botnet.
• January 2010: Neustar takes control of the Lethic spam botnet.
• March 2010: Microsoft takes down the Waledac botnet.
• October 2010: Armenian authorities take down the Bredolab botnet.
• March 2011: Microsoft takes down the Rustock botnet.

• July 2011: Microsoft offers a $250,000 reward for information leading to the arrest and conviction of the Rustock botmaster.
• July 2012: FireEye and Spamhaus take down the Grum botnet.
• July 2013: Microsoft and the FBI take down 1,400 botnets using the Citadel malware to control infected PCs.
• December 2013: Microsoft and the FBI take down the ZeroAccess botnet.
• June 2014: The FBI takes down of the Gameover Zeus botnet.

One takedown masterstroke came out of academia. George Mason University, the International Computer Science Institute, the University of California, San Diego, and Microsoft determined that 95 percent of all spam credit card processing was handled by three financial firms: one in Azerbaijan, one in Denmark, and one in Nevis (West Indies). They also pointed out that these financial firms were in violation of Visa's own Global Brand Protection Program contract that required fines of $25,000 for transactions supporting the sale of Viagra, Cialis, and Levitra. Once Visa started levying fines, the financial firms stopped processing the transactions. The beauty of this takedown was that this was not a legal maneuver through the courts and law enforcement. It merely encouraged Visa to follow its own policy.

Cyber Crime Business Operations

For me, one of the most enjoyable parts of Spam Nation is the insight on how these criminal organizations operate. For example, Krebs highlights why pharmaceutical operations have great customer support: they want to avoid the penalty fees associated with a transaction when a buyer of illicit pills charges them with fraud. These are called chargebacks, and pharmaceutical customer support operations avoid them like the plague. These support operations require teams of software developers and technical support staff to be available 24/7.

Pharmaceutical operations have mature anti-fraud measures—equivalent to any legitimate bank's anti-fraud measures—because they need to keep law enforcement and security researchers out of their business.

Most spammers do not make a lot of money. The top five do, but not everybody else. Krebs points out that it takes a multibillion dollar security industry to defend against a collection of criminals who are making a living wage.

In terms of botnet management, operators rent out top-earning botnets to other operators who do not have the skill to build a botnet themselves. Renters purchase installs and seed a prearranged number of bots with an additional malicious program that sends spam for the affiliate. They pay the rent by diverting a portion of their commissions on each pill sale from spam. Sometimes, that commission is as high as 50 percent. That is why the small-timers do not make any money.

Operators launder their money in a process called factoring. They map their client transactions into accounts on behalf of previously established shell companies. They tell the banks that the shell companies are the true customers. Then the operators pay the clients out of their own pockets.

Russian law allows FSB agents (Federal Security Service, the successor to the Soviet Union's KGB), while remaining in the service, to be assigned to work at enterprises and organizations at the consent of their directors. Twenty percent of FSB officers are engaged in this protection business called "Krusha" in Russian, which means "roof" and pharmaceutical spam operations use them as much as possible.

Partnerships, called partnerkas, between spammers and dodgy advertisers that act as an intermediary for potential sponsors are essential. In this way, sponsors keep their distance from the illicit aspects of the spam business and can unplug from one partnerka in favor of another whenever they want. Some refer to this as organized crime (think The Godfather), but it is more like a loosely affiliated network of independent operators.

With all of these best business practices, you can see why the operators do not see themselves as criminals. They are just businesspeople trying to run a business.

The Tech

Cyber crime runs on technology. In the pharmaceutical spam business, some tech is unique, and other tech is shared with other kinds of cyber crime operations. Unique to pharmaceutical spam is a technique called black search engine optimization (Black SEO). Pharmaceutical spammers hack legitimate websites and insert hidden pages (IFrames) with loads of pharmaceutical websites links. The more links that the common search engines like Google and Bing index, the higher the pharmaceutical sites get in the priority list when normal users search for pills online.

Also unique to the pharmaceutical spam business is a good spam ecosystem. It must have the ability to keep track of how many e-mails the system delivered and how many recipients clicked the link. It must scrub e-mail addresses that are no longer active or are obvious decoys and harvest new e-mail addresses for future operations.

Not unique to pharmaceutical spam are the forums. Forums are the glue that allows the loosely affiliated network of independent operators to communicate with each other. Forums are a place that allows newbies an opportunity to establish a reputation and lowers the barriers to entry for a life of cyber crime. There are forums for every language, but most are in English. Members enforce a strict code of ethics so that members who are caught cheating other members are quickly banned. Social networking rankings give members a way to evaluate potential partners. A single negative post may cost an individual thousands of dollars. Because of that, most amicably resolve issues. Sometimes newbies get labeled as a "deer," members who unintentionally break one of the forum's rules. More-serious infractions might find a member in the blacklist subforum defending himself or herself from fraud allegations.

New forums start all the time, but some have been in existence for more than a decade, indicating process maturity for self-policing, networking, and rapid information sharing. New forums allow open registration, but mature forums set up various hurdles for membership that are designed to screen out law enforcement and hangers-on. Most have sub-rooms for specialization such as the following:

- Spam
- Cyber banking fraud
- Bank account cash-out schemes

- Malicious software development
- ID theft
- Credit card fraud
- Confidence scams
- Black SEO

Forums have many members (tens of thousands in some), but they exist to make money for the administrators. Admins offer additional services to improve the user experience. They offer escrow services—a small percentage of the transaction cost held until both sides agree that the other held up its end of the bargain—and stickies—ads that stay at the top of their sub-forums that range in price from $100 to $1,000 per month.

Conclusion

In Spam Nation, Brian Krebs covers a key portion of our cyber security and cyber crime history: 2007–2013, that period when we started to learn about the Russian Business Network, bulletproof-hosting providers, fast-flux obfuscation, criminal best business practices, underground cyber crime forums, and strange-sounding botnet names like Conficker, Cutwail, Grum, Festi, Rustock, Storm, and Waledac. This period just happens to coincide with Krebs's rise in popularity as one of the leading cyber security journalists in the industry. His story, and the story of two competitive pharmaceutical spammers who eventually destroyed the lucrative moneymaking scheme for all players, is a fascinating read. It is definitely a cyber security canon candidate, and you should have read this by now.

Sources

"Spam Nation: The Inside Story of Organized Cybercrime - from Global Epidemic to Your Front Door," by Brian Krebs, published by Brilliance Audio, 18 November 2014, last visited 13 November 2014, https://www.goodreads.com/book/show/2...

References

"Blue Security folds under spammer's wrath," by Robert Lemos, Security Focus, 17 May 2006, last visited 13 November 2014,
http://www.securityfocus.com/news/11392

"Click Trajectories: End-to-End Analysis of the Spam Value Chain," by Kirill Levchenko, Andreas Pitsillidis, Neha Chachra, Brandon Enright, Mark Felegyhazi, Chris Grier, Tristan Halvorson, Chris Kanich, Christian Kreibich, He Liu, Damon McCoy, Nicholas Weaver, Vern Paxson, Geoffrey M. Voelker, and Stefan Savage, last visited 13 November 2014,
http://cseweb.ucsd.edu/~savage/papers...

"Experts Warn of New Windows Shortcut Flaw," by Brian Krebs, Krebs on Security, 10 July 2010, last visited 13 November 2014
http://krebsonsecurity.com/2010/07/ex...

"Krebs on Security: In-depth security news and investigation," by Brian Krebs, last visited 14 November 2014,
http://krebsonsecurity.com/

"PharmaLeaks: Understanding the Business of Online Pharmaceutical Affiliate Programs," by Damon McCoy, Andreas Pitsillidis, Grant Jordan, Nicholas Weaver, Christian Kreibich, Brian Krebs, Geoffrey M.

Voelker, Stefan Savage, and Kirill Levchenko, Usenix, August 2012, last visited 13 November 2014, http://www.cs.gmu.edu/~mccoy/papers/p... and https://www.usenix.org/conference/use...

“Russian Business Network Study,” by David Bizeul, 11 November 2007, last visited 12 November 2014, http://www.bizeul.org/files/RBN_study...

“Shadowy Russian Firm Seen as Conduit for Cybercrime,” by Brian Krebs, The Washington Post, 13 October 2007, last visited 12 November 2014, http://www.washingtonpost.com/wp-dyn/...

“The Partnerka – What Is It, and Why Should You Care?” by Dmitry Samosseiko, Sophos, Virus Bulletin, September 2009, last visited 13 November 2014, http://www.sophos.com/medialibrary/PD...

“The Sleazy Life and Nasty Death of Russia’s Spam King,” by Brett Forrest, Wired Magazine, August 2006, last visited 13 November 2014, http://archive.wired.com/wired/archiv...

“The Underground Economy of Spam: A Botmaster’s Perspective of Coordinating Large-Scale Spam Campaigns,” by Brett Stone-Gross, Thorsten Holz, Gianluca Stringhini, and Giovanni Vigna, last visited 13 November 2014, https://www.iseclab.org/papers/cutwai...

“Top Spam Botnets Exposed,” by Joe Stewart, SecureWorks, 8 April 2008, last visited 13 November 2014, http://www.secureworks.com/cyber-thre...

Rich Miller says

I was turned on to this book after reading the author's blog at http://www.krebsonsecurity.com and becoming intrigued to learn about the sources of and reasons for the torrent of spam that we are hit with in our inboxes each and every day. The author is obviously well-versed on this topic, and his story about the competing cybercrime factions made for a compelling story. There is some technical jargon sprinkled throughout this book, but the author made the topic approachable for any reader by providing clear explanations of most if not all technical terms and concepts. Overall, the book is very readable for any audience that is fascinated by this topic or those just wanting to become more informed. Unfortunately, I could only give the book 3 stars because the material, while well researched and thorough, could probably have been presented in a more organized and concise manner to get the point across more effectively. At times the book reads like a collection of independent blog posts, and some information is presented repeatedly. The cast of characters was also hard to follow and needed to be better managed. Still a recommended read in these times when we spend a good part of our lives online and the risk of hacking threats grows higher every day.

Vasil Kolev says

It's a very good and mostly in-depth look into the world of spammers, especially the ones that deal with selling drugs. It concentrates mostly on some Russians, but still paints a petty good picture of most of the business, and the advice in the end seems good enough for beginners and most people.

The parts on why people buy from spammers were really interesting, which point to why most of the big pharma companies don't really want to investigate them, as it mostly seems that they sell the same stuff, just cheaper.

Monica Willyard says

This book offers a clear, easy to read introduction of spam, the people behind it, and the reason for its rise in prominence.

Isa K. says

Brian Krebs's favorite word is miscreant. >.>

An interesting, richly detailed account of the cyber crime ecosystem. I must admit I was slightly bemused by the fact that the author doesn't know that Livejournal was an American company sold to a Russian one, not the other way around (at one point he says that Russian Livejournal bought Six Apart and I was like ORLY? Also remember when having a MovableType install as a blogger was like buying a BMW? *sigh*) ... but this is just olds on the internet talk.
