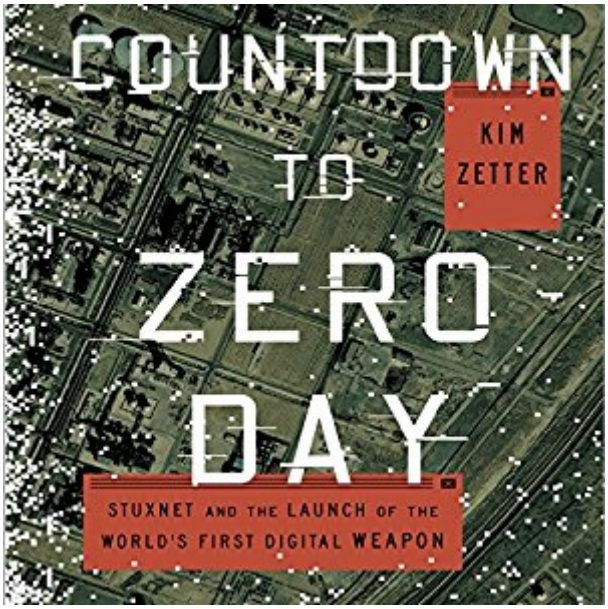
Countdown To Zero Day: Stuxnet And The Launch Of The World's First Digital Weapon



Synopsis

Top cybersecurity journalist Kim Zetter tells the story behind the virus that sabotaged Iran's nuclear efforts and shows how its existence has ushered in a new age of warfare - one in which a digital attack can have the same destructive capability as a megaton bomb. In January 2010, inspectors with the International Atomic Energy Agency noticed that centrifuges at an Iranian uranium enrichment plant were failing at an unprecedented rate. The cause was a complete mystery - apparently as much to the technicians replacing the centrifuges as to the inspectors observing them. Then, five months later, a seemingly unrelated event occurred: A computer security firm in Belarus was called in to troubleshoot some computers in Iran that were crashing and rebooting repeatedly. At first, the firm's programmers believed the malicious code on the machines was a simple, routine piece of malware. But as they and other experts around the world investigated, they discovered a mysterious virus of unparalleled complexity. They had, they soon learned, stumbled upon the world's first digital weapon. For Stuxnet, as it came to be known, was unlike any other virus or worm built before: Rather than simply hijacking targeted computers or stealing information from them, it escaped the digital realm to wreak actual, physical destruction on a nuclear facility. In these pages, Wired journalist Kim Zetter draws on her extensive sources and expertise to tell the story behind Stuxnet's planning, execution, and discovery, covering its genesis in the corridors of Bush's White House and its unleashing on systems in Iran - and telling the spectacular, unlikely tale of the security geeks who managed to unravel a sabotage campaign years in the making. But Countdown to Zero Day ranges far beyond Stuxnet itself.

Book Information

Audible Audio Edition
Listening Length: 13 hoursÂ andÂ 1 minute
Program Type: Audiobook
Version: Unabridged
Publisher: Random House Audio
Audible.com Release Date: November 11, 2014
Language: English
ASIN: B00P89SN0C
Best Sellers Rank: #6 inÂ Books > Computers & Technology > Security & Encryption > Viruses #10 inÂ Books > Computers & Technology > History & Culture > History #20 inÂ Books > Audible Audiobooks > Politics & Current Events > Freedom & Security

Customer Reviews

Being in the IT field (in particular working with OS design and administration) I took an interest when Stuxnet came to light a few years back. The last time I remembered such a stir created in the media about propagating malware was when the Morris worm surfaced in the late 1980Ã¢Â Â™s. I did not know too much about Stuxnet other than what was shared in news reports so I was eager to learn more. This book definitely delivers the goods.Instead of a dry, factual presentation that just leaves the reader bored, this book reads more like a novel Ã¢Â Â“ except that itÃ¢Â Â™s true. It starts with a fascinating account of how Stuxnet was first discovered and describes in some detail how it exploited the operating system, what mechanisms it used to replicate itself, how it targeted the systems it was designed to find and it gives a fair estimate of just how much damage it caused before it was ultimately uncovered. The book goes on from there to discuss the implications Stuxnet has had on the digital world and how it has helped to redefine modern warfare.The main text is written very much like a novel, but it makes heavy use of footnotes. These footnotes inject interesting facts relating to the point being made but would otherwise mar the chain of thought for the reader. This was a smart editing decision as it makes taking the side tracks optional.One thought kept coming to mind as I got deeper into the material and learned more about the birth of this malware and how it all came into being Ã¢Â Â“ I had absolutely no clue just how deep the rabbit hole went, both militarily and politically.For those interested in cybersecurity, those with an interest in electronic warfare or even those who are just downright curious about what is without question the most complex and sophisticated digital weapon known to date, this book is full of interesting information and because itÃ¢Â Â™s written almost like fiction itÃ¢Â Â™s a fast and engrossing read.

I know quite a few of the researchers that were involved in reverse engineering Stuxnet and Flame - so I was able to watch the story unfold with a behind the scenes view - what’s presented in here is a very accurate, and insightful view of one of the most important security discoveries in recent years.Stuxnet, et. al. presented the security industry with a huge problem - and the implications are still being sorted out to this day. Government use of malware, and how the industry should handle it when discovered are topics that are still being debated on a daily basis. Kim does a great job on explaining the issues, and giving readers plenty to think about.From a technical perspective, the book goes into enough detail so that those of us familiar with the topic know exactly what is being discussed and it’s implications, while not going overboard and overloading non-technical users with incomprehensible details. The book has a good narrative style, while covering technical detail and

including details on the sources for information. Throughout the book are footnotes that list source information, additional notes that explain context, or provide additional details that don't fit in the narrative telling - I strongly suggest that you read the footnotes, as they offer very useful information.All in all, I strongly recommend the book, well worth it.

A word to describe Takedown: The Pursuit and Capture of America's Most Wanted Computer Outlaw was hyperbole. While the general storyline from the 1996 book was accurate, filler was written that created the legend of Kevin Mitnick. This in turn makes the book a near work of historical fiction.Much has changed in nearly 20 years and Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon has certainly upped the ante for accurate computer security journalism.The book is a fascinating read and author Kim Zetter's attention to detail and accuracy is superb. In the inside cover of the book, Kevin Mitnick describes this as an ambitious, comprehensive and engrossing book. The irony is not lost in that Mitnick was dogged by misrepresentations in MarkoffÃ¢Â Â™s book.For those that want to know the basics about Stuxnet, its Wikipedia entry will suffice. For a deeper look, the book take a detailed look at how the Stuxnet worm of 2010 came to be, how it was written, discovered and deciphered, and what it means for the future.The book provides nearly everything that can be known to date about Stuxnet. The need to create Stuxnet was the understanding that a nuclear Iran was dangerous to the world. The book notes that it just wasnÃ¢Â Â™t the US and Israel that wanted a nuclear-free Iran; Egypt and Saudi Arabia were highly concerned about the dangers a nuclear Iran would bring to the region.What is eminently clear is that Iran chronically lied about their nuclear intentions and actions (chapter 17 notes that former United Kingdom Prime Minister Gordon Brown told the international community that they had to do something over IranÃ¢Â Â™s serial deception of many years) and that the United Nations International Atomic Energy Agency (IAEA) was powerless to do anything, save for monitoring and writing reports.While some may debate if Stuxnet was indeed the world's first digital weapon, itÃ¢Â Â™s undeniable that it is the first piece of known malware that could be considered a cyber-weapon. Stuxnet was unlike any other previous malware. Rather than just hijacking targeted computers or stealing information from them, it created physical destruction on centrifuges the software controlled.At just over 400 pages, the book is a bit wordy, but Zetter does a wonderful job of keeping the book extremely readable and the narrative enthralling. Writing about debugging virus code, descriptions about the Siemens industrial programmable logic controllers (PLCs) and Step7 software (which was what Stuxnet was attacking) could easily be mind-numbingly boring, save for ZetterÃ¢Â Â™s ability to make it a compelling read.While a good part of the book details the

research Symantec, Kaspersky Lab and others did to debug Stuxnet, the book doesnÃ¢Â Â™t list a single line of code, which makes it quite readable for the non-programmer. The book is technical and Zetter gets into the elementary details of how Stuxnet operated; from reverse engineering, digital certificates and certificate authorities, cryptographic hashing and much more. The non-technical reader certainly wonÃ¢Â Â™t be overwhelmed, but at the same time might not be able to appreciate what went into designing and making Stuxnet work.As noted earlier, the book is extremely well researched and all significant claims are referenced. The book is heavily footnoted, which makes the book much more readable than the use of endnotes. Aside from the minor error of mistakenly calling Kurt GÃ¶del a cryptographer (he was a logician) on page 295, ZetterÃ¢Â Â™s painstaking attention to detail is to be commended.Whoever wrote Stuxnet counted on the Iranians not having the skills to uncover or decipher the malicious attacks on their own. But as Zetter writes, they also didnÃ¢Â Â™t anticipate the crowdsourced wisdom of the hive Ã¢Â Â“ courtesy of the global cybersecurity community that would handle the detection and analysis for them. That detection and analysis spanned continents and numerous countries.The book concludes with chapter 19 Digital Pandora which departs from the details of Stuxnet and gets into the bigger picture of what cyber-warfare means and its intended and unintended consequences. There are no simple answers here and the stakes are huge.The chapter quotes Marcus Ranum who is outspoken on the topic of cyber-warfare. At the 2014 MISTI Infosec World Conference, Ranum gave a talk on Cyberwar: Putting Civilian Infrastructure on the Front Lines, Again. Be it the topic or Marcus being Marcus, a third of the participants left within the first 15 minutes. They should have stayed, as Ranum, agree with him or not, provided some riveting insights on the topic.The book leave with two unresolved questions; who did it, and how did it get into the air-gapped Nantanz enrichment facility.It is thought the US with some assistance from Israel created Stuxnet; but Zetter also writes that Germany and Great Britain may have done the work or at least provided assistance.ItÃ¢Â Â™s also unknown how Stuxnet got into the air-gapped facility. It was designed to spread via an infected USB flash drive. ItÃ¢Â Â™s thought that since they couldnÃ¢Â Â™t get into the facility, what needed to be done was to infect computers belonging to a few outside firms that sold devices that would in turn be connected to the facility. The book identified a few of these companies, but itÃ¢Â Â™s still unclear if they were the ones, or the perpetrators somehow had someone on the inside.As to zero day in the title, what was unique about Stuxnet is that it contained 5 zero day exploits. Zero day is also relevant in that Zetter describes the black and gray markets of firms that discover zero-day vulnerabilities who in turn sell them to law enforcement and intelligence agencies.Creating Stuxnet was a huge challenge that took scores of programmers from a nation

state many months to create. Writing a highly readable and engrossing book about the obscure software vulnerabilities that it exploited was also a challenge, albeit one that few authors could do efficaciously. In Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon, Kim Zetter has written one of the best computer security narratives; a book you will likely find quite hard to put down.

Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon The Mobility Revolution: Zero Emissions, Zero Accidents, Zero Ownership Launch!: How A Startup Made Over $100,000 Crowdfunding On Indiegogo With This Launch Strategy Day Trading Strategies: A Beginners Guide To Day Trading (Day Trading, Trading, Day Trading Strategies,Day Trading Books,Day Trading For Beginners,Day Trading Stocks,Options Book 1) Re:ZERO, Vol. 1 - manga: -Starting Life in Another World- (Re:ZERO -Starting Life in Another World- Manga) Re:ZERO, Vol. 1: -Starting Life in Another World - light novel (Re:ZERO -Starting Life in Another World-) Countdown to My Birth: A day by day account from your baby's point of view Day Trading: A Beginner's Guide To Day Trading - Learn The Day Trading Basics To Building Riches (Day Trading, Day Trading For Beginner's, Day Trading Strategies Book 1) Cryptocurrency: Guide To Digital Currency: Digital Coin Wallets With Bitcoin, Dogecoin, Litecoin, Speedcoin, Feathercoin, Fedoracoin, Infinitecoin, and ... Digital Wallets, Digital Coins Book 1) The Machine That Changed the World: The Story of Lean Production-- Toyota's Secret Weapon in the Global Car Wars That Is Now Revolutionizing World Industry Countdown to Your Perfect Wedding: From Engagement Ring to Honeymoon, a Week-by-Week Guide to Planning the Happiest Day of Your Life Day of Vengeance (Countdown to Infinite Crisis) Bomb: The Race to Build - and Steal - the World's Most Dangerous Weapon Bomb: The Race to Build--and Steal--the World's Most Dangerous Weapon (Newbery Honor Book) The 7 Day Startup: You Don't Learn Until You Launch Book Launch: How to Write, Market & Publish Your First Bestseller in Three Months or Less AND Use it to Start and Grow a Six Figure Business Photography: DSLR Photography Secrets and Tips to Taking Beautiful Digital Pictures (Photography, DSLR, cameras, digital photography, digital pictures, portrait photography, landscape photography) Selling Blueprint - How to Find and Launch Your First Private-Label Product on in 90 Days or Less Digital Painting Techniques: Practical Techniques of Digital Art Masters (Digital Art Masters Series) Photography: Complete Guide to Taking Stunning,Beautiful Digital Pictures (photography, stunning digital, great pictures, digital photography, portrait ... landscape photography, good pictures)