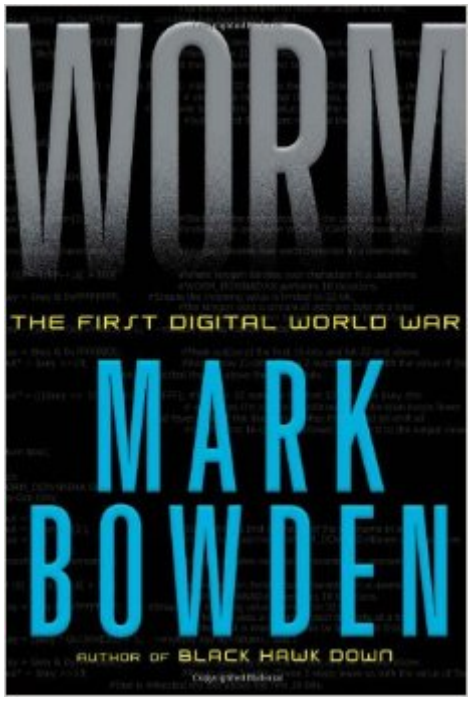
Worm: The First Digital World War



Synopsis

From the author of Black Hawk Down comes the story of the battle between those determined to exploit the internet and those committed to protect it—the ongoing war taking place literally beneath our fingertips.The Conficker worm infected its first computer in November 2008 and within a month had infiltrated 1.5 million computers in 195 countries. Banks, telecommunications companies, and critical government networks (including the British Parliament and the French and German military) were infected. No one had ever seen anything like it. By January 2009 the worm lay hidden in at least eight million computers and the botnet of linked computers that it had created was big enough that an attack might crash the world. This is the gripping tale of the group of hackers, researches, millionaire Internet entrepreneurs, and computer security experts who united to defend the Internet from the Conficker worm: the story of the first digital world war.

Book Information

Hardcover: 288 pages

Publisher: Atlantic Monthly Press; First Edition edition (September 27, 2011)

Language: English

ISBN-10: 0802119832

ISBN-13: 978-0802119834

Product Dimensions: 9.1 x 6.2 x 1.1 inches

Shipping Weight: 14.4 ounces

Average Customer Review: 3.9 out of 5 starsÂ Â See all reviewsÂ (107 customer reviews)

Best Sellers Rank: #474,929 in Books (See Top 100 in Books) #98 inÂ Books > Computers & Technology > Security & Encryption > Viruses #164 inÂ Books > Computers & Technology > History & Culture > History #800 inÂ Books > Politics & Social Sciences > Politics & Government > Specific Topics > Intelligence & Espionage

Customer Reviews

One of the greatest things about airport bookstores - they often ignore sale dates. I purchased Worm a few days ago without realizing it wasn't supposed to be released yet. Which is good, because it made that flight from Denver to Baltimore tolerable.First things first. If you are a network newbie, you will be coddled by this book. You don't need to have your MCSE or CISSP to read "Worm". Bowden does a good job of breaking down salient data - what is TCPIP, what is RPC - and creating explanations that make sense. Don't know why Port 445 is so special? Wonder why Windows is so often the target of malware around the world? (the technical explanation, not the

political answer) You will after reading this book. It won’t win you any medals at the next Cisco shareholders meeting or net you a job in IT, but at least you’ll know why Patch Tuesday is important and why malware isn’t just a problem with code - it’s a social engineering problem, too.The next best thing about this book is how much it stresses that the Internet is still in it’s adolescence. It’s a hodgepodge of ancient protocols and new-fangled protocols shoehorned into communicating with one another, and that’s a fragile animal. you’ll wonder why it doesn’t go down more often."Worm" is entertaining and informative. Personally, I think it’s too short. You’ll get a quick bio about a particular researcher, follow them through some problem solving and then, inexplicably, drop them entirely while picking up with another researcher. I think the personalities involved are as important as the science. But those quibbles are trivial.

It’s out there. Waiting. Chances are, you’ve never heard of it. Nobody knows who controls it, or why. No one knows what it will do. But its destructive capacity is terrifying.Welcome to the world of cyberwar! And, no, this is NOT science fiction."It" is the Conficker Worm, an arcane name (an insider’s joke) for the most powerful "malware" -- malicious software -- yet encountered on the Internet. First detected in November 2008, Conficker is a devilishly clever bit of programming that took advantage of a vulnerability in the Windows operating system. Microsoft immediately moved to "patch" the vulnerability, but therein lay the problem: Windows is the most-pirated software of all, so hundreds of milliions of computers were running versions of Windows without the patch -- all of them vulnerable to Conficker (and to hundreds of other malicious programs whose authors now knew how to embed their work in Windows).Mark Bowden, the very capable author of Blackhawk Down, tells the story in Worm of a group that included many of the world’s top computer security experts who privately came together early in 2009 to combat Conficker. At first, they were confined exclusively to the private sector, and their work was informal. Eventually, they managed to gain the attention of senior government officials and -- slowly, reluctantly -- obtain limited official support from the U.S. and Chinese governments. The group, known among themselves as the Conficker Cabal, even managed to get onto the White House agenda late in the game, as Conficker was upgraded once and then again - because the worm represented nothing less than an existential threat to the Internet itself.I did say the potential was terrifying, didn’t I?Bowden is a superb journalist and a capable writer, as Blackhawk Down made clear. However, Delta Force soldiers pinned down in a firefight in Mogadishu make for great copy. Geeks exchanging emails about technical material don’t. Bowden does an excellent job explaining in plain English the nature of Conficker and how it operates, and he does his best to sketch the members of the Cabal in three diimensions, but the

result is hardly a page-turner. Still, Worm is a very important book, because it brings to light just how vulnerable is the infrastructure of the world we live in.And, oh yes, the Cabal managed to fight Conficker to something of a standstill. But they couldn't destroy it, and to date they've never found the hackers who created it. Conficker is still out there.[...]

Author Bowden does a great job of summarizing malware in general, and the Conficker worm in particular. He begins by explaining that there are three types of malware - Trojans, viruses, and worms. A Trojan is a piece of software that masquerades as one thing to get inside a computer, then attacking. A virus attacks its host computer after entering its operating system - it depends on the operator opening an e-mail attachment or clicking on a lilnk. A worm works like a virus, but doesn't attack once it enters - it's primarily designed to spread, then wait for instructions delivered later.Some computer malware is intended to damage or destroy one's computer, and victims quickly realize the problem. A computer worm, by contrast, is a packet of computer code designed to infiltrate a computer without attracting attention and then scans for others to invade, spreading exponentially. The Conficker computer worm emerged in November, 2008 and infiltrated 1.5 million of the world's computers in the first month. By January, 2009 it had spread to at least 8 million computers, exploiting flaws in Microsoft Windows that it closed after entering. They constantly check with its unknown creaters at their unknown location for directions. Frustrated cyber-security experts at Microsoft, Symantec, SRI International, etc. have merged forces to try and defeat it - so far they've been unsuccessful. Bowden's 'Worm' tells how hackers, entrepreneurs, and computer security experts are trying to defend the Internet from Conficker - what the author calls 'the first digital world war.'In the 'good old days,' infected computers slowed down because user commands had to compete with viral invaders for processing power. Computers would slow down, and programs would freeze. Worm-linked computers ('botnets') can be used to steal information, assist fraudulent schemes, or launch denial-of-service attacks. So far, Conficker (35 kilobytes of code - less than a 2,000-word document) has done none of those things, and been activated only once to perform a short, simple spamming operation that sold a fake anti-spyware program for two weeks, then stopped.The Microsoft operating system has over 65,000 ports designed to transmit and receive certain kinds of data. Conficker exploited Port 445, which Microsoft had tried to repair 10/23/2008. Firewalls are security programs that guard these ports, but Port 445 was vulnerable even when protected by a firewall if both print-sharing and file-sharing were enabled. However, many fail to apply new patches promptly, and others run pirated Windows systems which Microsoft doesn't update. Thus, reverse-engineering patches allows attackers to create targeted

worms.Experts trying to disable Conficker have learned that it tries to prevent communication with security providers, it avoided Ukrainian IP addresses, and disabled system restore points that allowed users to reset infected machines to a date prior to infection. To prevent IT-defenders from predicting how the infected computer would try to communicate home by setting the computer's clock ahead and then watching what happened (it generates 250 random-codes/day for each of 8 domains - eg. .com, .edu, .uk, etc.). Conficker-infected computers use system clocks (eg. Google, Yahoo) that can't be set ahead. The 'bad guys' only have to pay $10 to register one address, and wait for botnetted computers to make contact. Unfortunately for computer defenders, that communication used coding techniques employed in the latest standard, MD-6, revised.Defenders, however, were flooded by 50,000 domain names/day needing investigation. Each requires checking to ensure it belongs to a good guy, and their spread out all over the world. Worse yet, a newer version introduced peer-to-peer communication, meaning that all infected computers no longer needed to call home for instructions, and defenders no longer have any way of telling how many computers are infected.Another insidious Conficker attribute is that it could also be spread by USB drives - thus, systems not connected to the Internet were also vulnerable.Most of the world's 'best' malware comes from Eastern Europe, drawing on high levels of technical expertise and organized criminal gangs. That's a very big area within which to search.

How to Set Up and Maintain a Worm Composting System The Tequila Worm The Worm Family (Bccb Blue Ribbon Picture Book Awards (Awards)) Photography: NOW! - The Ultimate Guide to Take STUNNING Photos And Change the Way You See the World - Master The Art of Digital Photography With Your Camera ... Digital Photography, DSLR, Creativity)