

r00ting the hacker: An Interview with Dan Verton

Von Spangler

"...With every technology there are unintended consequences. And in the case of computer technology, the unintended consequence was that inherently bad people could use the new technology to do bad things."

- Dan Verton, author of *The Hacker Diaries*

Hacker headliners over the years

Hackers deface Air Force Web site, *Computer World*

Teenager admits \$100,000 credit card rip-off, *Associated Press*

Ontario boy, 14, charged as hacker for breaking into more than 500 sites in less than a year, *Vancouver Sun*

Thousands of passwords accessed by cyber prowler, *Associated Press*

FBI mounts big crackdown on small-town teens, *ZDNet News*

FBI on offensive in "cyber war," raiding hackers' homes, *CNN*

Five arrested for hacking into high school system, *Flagler Palm Coast News Tribune*

Fed ID hacker who allegedly stole more than 485K credit card numbers, *Computer World*

Hackers, not terrorists, major concern, *InternetWeek*

Internet survives massive DDoS attack, *eWeek*

Who are they?

They make international headlines for all the wrong reasons and everyday we read about the increasingly large-scale havoc they cause: the hacking into corporate computer systems, the theft of credit card numbers, and the defacement of Web sites with vulgar, disturbing and sometimes hate-filled messages. But still - teenage hackers - who are they?

Social misfits? Loners? Pimpled face geeks? Dangerous and deceptive brainiac-villains? That is in fact the public's perception and how the media stereotype them.

Yet real teenage hacker culture is a patchwork of different personalities, backgrounds, motivations and experiences. In other words, there is no one picture of the average teenage hacker.

Dan Verton, the author of *The Hacker Diaries: Confessions of Teenage Hackers* is a former intelligence officer in the U.S. Marine Corps who currently writes for *Computerworld* and *CNN.com*, covering national cyber-security issues and critical infrastructure protection.

For his *Hacker Diaries*, he interviewed well over a dozen real life hackers and explored beyond the myths and stereotypes surrounding these teenagers. He describes many of them as being the kids bagging your groceries at the supermarket; working in the community service on the weekends; playing in the school orchestra or singing in the choir; struggling with their grades in math, science and English; getting good grades and planning for a bright future; hanging out with their friends after school and sometimes getting into trouble; and almost always feeding their obsession with computers and the Internet late at night.

A far contrast to the monsters we read about.

How did they originate? What's their purpose?

The hacking scene today consistently seems to be becoming more about mischief, crime, status, money, media attention... and destruction. Trends that are at odds with the essence of the hacking culture; the original role that hackers saw themselves play.

In the beginning, according to Verton, hacker explorers were rarely prosecuted because nobody had any idea about what was legal and what wasn't. At the same time, most hackers back then were into hacking as a means to explore and discover, and enable information sharing.

"The first hackers were the pioneers of the computer revolution and the Internet," explains Verton. "They were in it for one thing: pursuit of legitimate scientific knowledge and the betterment of mankind through science, knowledge etc.... The programming shortcuts that they invented to make large mainframe computers run faster and more efficiently became known as "hacks" and the programmers of those shortcuts as "hackers." But with every technology there are unintended consequences. And in the case of computer technology, the unintended consequence was that inherently bad people could use the new technology to do bad things."

The massive distributed-denial-of-service attacks against *Yahoo!*, *ZDNet*, *EBay*, *CNN* and *Amazon* are of the many examples that assert this. The series of attacks occurred early 2000; the first victim - *Yahoo!*, one of the Web's biggest information portals and e-commerce sites, was crippled enough to go offline. It involved their network (or precisely their main routers) being flooded with massive amounts of data at speeds higher than 1 gigabit per second, the equivalent of more than 3.5 million average e-mail messages every minute.

Recently, a similar assault was launched against the Internet's root DNS servers. These root DNS servers perhaps can be considered the heart of the Internet. Another story involved *Creditcards.com*, which was hacked, and 55,000 card numbers were held hostage for \$100,000. When the extortion attempt failed, the hacker posted the card numbers on the Web...

"Today," says Verton, "many who use the title *hacker* are into stopping information flow or worse, destroying information as a way to demonstrate their technological prowess and *discovery*." But many hackers' motives and actions are not limited to those alone. As in the case of *Creditcard.com*, Verton agrees their major objective can be simply money. Credit card data is cash.

What is being done?

At the opposite end are the law enforcement agencies and Verton, who frequently converses with the top heads, believes that in recent times they - particularly the FBI - are becoming much more organized and prepared to combat and suppress these cyber criminals.

"Director Robert Mueller has ordered a massive overhaul of the FBI structure and mission focus," says Verton, "so that not only are there more resources being dedicated to cyber-crime and cyber-terrorism, but those two areas are now within the top 3 priorities for the entire Bureau as set forth by Director Mueller. That's a significant change."

Yet recently, President Bush's cyber-security adviser stated a fact when he declared that cyber-crime is costing the world economy billions of dollars and is on the increase.

Why is cyber-crime not being effectively controlled? What is fuelling the rampancy?

- Parental apathy & the public education system - Kids are not being thought responsibility and responsible use of computer resources in the school and at home. To begin with, parents and teachers may not be computer literate and au courant enough to understand the frightening dangers and consequences involved with computer hacking.
- The increased ease of hacking - Now, not only hackers who have taken years in garnering and honing their

skills can hack. Take for example the assault on *Yahoo!*, *ZDNet*, *EBay*, *CNN* and *Amazon*. This was done by a 14 year old Canadian boy; an unskilled hacker according to the FBI's conclusive reports.

Freely distributed, easy-to-use yet malicious toolkits (published throughout the Internet by programmers / expert hackers) fall into the hands of unsophisticated / novice hackers who - as a *CanWest Interactive* report described - "...are unaware of the capabilities of the hacker tools they use, unaware of the implications of their hacking or unconcerned about the consequences of their actions."

- The private-sector cooperation yet to make cyber-crime a top priority -
 - Companies are not investing enough to train their administrators or seek expert assistance, resulting in poorly configured environments.
 - Administrators do not keep up with updates and patches released by their software vendors.
 - The "2002 Computer Crime and Security Survey" by the FBI and the San Francisco-based Computer Security Institute shows that only 34% of companies said they reported cyber-crime incidents to law enforcement agencies. Most said they didn't report incidents out of fear of negative publicity and the potential for competitors to use the information against them. According to FBI Director, Robert Mueller, it is a serious hindrance in the fight against cyber-crime if companies don't come forward.

Verton adds to this. "Well, one other reason that maybe I didn't focus on in my book would be corporate complacency. I recently sat in an invitation-only dinner meeting of Wall Street executives in New York, where the discussion was off the record so that everybody would speak candidly. One CEO actually said that his company was so small that nobody would be interested in hacking his network, so why should he spend so much time and money worrying about staying on top of the changes in vulnerabilities and security technologies.

"Well, we know now that everybody is potentially somebody else's weakest link. It's no longer enough to worry about only your networks. Today you have to worry about everybody you do business with, everybody you give access to (physical and cyber access). The push toward corporate transparency has a fatal drawback: it allows bad people to more easily identify and see undiscovered vulnerabilities."

Ethics in hacking?

Though, not all "illegal" hacking is bad, according to Verton. "Sure, it's illegal, but Web site defacements that are specifically targeted and focused on critical social or political issues could be seen, and in fact are by many people, as a legitimate form of peaceful dissent."

In Verton's book, he mentions the *EHAP*, *Ethical Hackers Against Pedophiles*, a group that helps law enforcement officials to track down adults who exploit children online. Over the last several years they have helped rid the Internet of those who traffic and profit in child pornography. Such ethical hacking is commonly termed as hacktivism.

Verton goes on to give another example of this. "If a company is known to be an environmental offender, for example, hacking their Web site and placing the truth about that company in front of the world may actually do some good. I'm not necessarily against minor infractions of the law for critically important social causes. People do that all the time when they picket without a license, or try to block entry into a courthouse while not resisting arrest. Hacking or hacktivism has a place in that respect."

Resources

<http://www.infosecwriters.com> - The Information Security Writers

<http://www.danverton.com> - Dan Verton's National Security Journal

<http://www.sans.org/rr/hackers> - The SANS Institute's Reading Room