

|  |  |  |
| --- | --- | --- |
|  | **My Drift**  **Jerry D. Petersen**  **Hackers**  **5 June 2014** | **178-2014-07** |

**Confession: I’m a computer hacker!! Yes, back in early years of computers (the 1960s, 1970s and 1980s), guys like me who knew a lot about computers, how they work, and who could program them to do almost anything were called computer hackers. Among computer programmers, it means a good programmer who can make a computer do what he or she wants—whether the computer wants to or not. Its true meaning still refers to someone with a strong technical background who is "hacking away" at the computer bits and bytes. Sometime in the early 1990’s, the term "hacker" became synonymous with "cracker," which is a person who performs some form of computer sabotage. So, now days, most people think a hacker is a sinister person who breaks into networks, servers, and personal computers to spread viruses, steal personal information, identities, destroy data, and generally cause havoc and mayhem.**

**For some reason, people don’t like to use the word “cracker” so we (the good and the bad hackers) are stuck with the word “hacker”. There are now many different types and classifications of hackers:**

**White hat**

**A “white hat” hacker is the good programmer or somebody who breaks security for non-malicious reasons, perhaps to test their own security code. I guess I fall into this category – I do wear a white cowboy hat when out riding horses.**

**Black hat**

**A "black hat" hacker is a hacker who "violates computer security for maliciousness or for personal gain. These hackers form the stereotypical, illegal hacking groups often portrayed in popular culture, and are "the epitome of all that the public fears in a computer criminal". Black hat hackers break into secure networks to destroy data or make the network unusable for those who are authorized to use the network. Black hat hackers also are referred to as the "crackers" within the security industry and by modern programmers.**

**Grey hat**

**A “grey hat” hacker is a combination of a black hat and a white hat hacker. A grey hat hacker may surf the internet and hack into a computer system for the sole purpose of notifying the administrator that their system has a security defect, for example. They may then offer to correct the defect for a fee.**

**Elite hacker**

**A social status among hackers, elite is used to describe the most skilled. Newly discovered exploits circulate among these hackers. Elite groups such as Masters of Deception conferred a kind of credibility on their members.**

**Script kiddie**

**A script kiddie is a non-expert who breaks into computer systems by using pre-packaged automated tools written by others, usually with little understanding of the underlying concept—hence the term script kiddie—an immature individual lacking knowledge and experience.**

**Blue hat**

**A “blue hat” hacker is someone outside computer security consulting firms who is used to bug-test a system prior to its launch, looking for exploits so they can be closed. Microsoft also uses the term “Blue Hat” to represent a series of security briefing events.**

**Hacktivist**

**A hacktivist is a hacker who utilizes technology to publicize a social, ideological, religious or political message. Most hacktivism involves website defacement or denial-of-service attacks.**

**Organized criminal gangs**

**Groups of hackers that carry out organized criminal activities for profit.**

**State Sponsored Hackers**

**Governments around the globe realize that it serves their military objectives to be well positioned online. The saying used to be, “He who controls the seas controls the world,” and then it was, “He who controls the air controls the world.” Now it’s all about controlling cyberspace. State sponsored hackers have limitless time and funding to target civilians, corporations, and governments.**

**Spy Hackers**

**Corporations hire hackers to infiltrate the competition and steal trade secrets. They may hack in from the outside or gain employment in order to act as a mole. Spy hackers may use similar tactics as hacktivists, but their only agenda is to serve their client’s goals and get paid.**

**Cyber Terrorists**

**These hackers, generally motivated by religious or political beliefs, attempt to create fear and chaos by disrupting critical infrastructures. Cyber terrorists are by far the most dangerous, with a wide range of skills and goals. Cyber Terrorists ultimate motivation is to spread fear, terror and commit murder.**

**HERE ARE SOME RECENT HEADLINES**

|  |  |
| --- | --- |
|  | **Millions of computer users have had their email hacked infecting their PCs with viruses and other malicious code. The most common way this happens is when you open or download an email attachment that contains infected code. This can allow hackers access to take over your computer, steal personal information, destroy data, install viruses, worms, read and send email from your accounts.**  **Hackers installed malware in Target’s security and payments system designed to steal every credit card used at the company’s 1,797 U.S. stores during the 2013 Christmas gifts buying season. This data breach continues to get worse with at least 70 million customers being impacted**  **Ebay announced recently that its database was hacked “between late February and early March, 2014” allowing cyber attackers access to customer names, encrypted passwords, email addresses, home addresses, phone numbers and dates of birth. An eBay spokesperson said that as many 145 million users may have been affected by the breach.**  **Microsoft joins a list of companies that've recently reported being hacked, including Facebook, Apple, Twitter, The New York Times and The Wall Street Journal. These companies were all targeted via a vulnerability in Oracle's Java.**  **Russian hackers have penetrated the Pentagon’s computer systems in recent attacks. The Pentagon and other US government departments face repeated attacks (more than a thousand a day), especially from Russia and China, either from individuals or indirectly from those countries' governments. There are many countries that want access to our military secrets.**  **The Chinese government has hacked into the very heart of American enterprise. The victims of the hacking are American titans: U.S. Steel, Andrew Carnegie and J.P. Morgan; Alcoa, Westinghouse Electrical Company, one of the world’s leading nuclear power developers; and the United Steelworkers, among America’s most iconic labor unions**  **The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software used by most large companies in the United States. This weakness allowed stealing information protected, under normal conditions, by the SSL/TLS encryption used to secure data sent over the Internet. This bug allowed anyone on the Internet to read the memory of the systems protected by the vulnerable versions of the OpenSSL software.** |

**I think you get the picture. Criminal hackers have pretty mush taken over the world!! Almost every day you read about the government or a bunch of companies being hacked and providing the hackers access to all of your personal data. You hardly ever hear about these criminals getting caught. Since hacking is a world-wide thing, even if you know who is doing it, making arrests and putting these crooks in jail is not easy.**

**Let me give you a brief history of computers, the Internet, the World-Wide Web, email, and a few other things that have happened in the Information Technology (IT) arena over the years leading up to where we are today.**

**The computer has not been around that long. I was born before the first computer was invented. Well, maybe they have been around for quite a while since I’m about the same age as dirt. The first computer was built at the University of Pennsylvania between 1943 and 1945 by two professors, John Mauchly and J. Presper Echert, who got the funding ($500,000) from the U.S. Army. The Army wanted a machine to support the war effort and to compute whether or not it was possible to build a hydrogen bomb. This computer was called the ENIAC (see picture below), which stood for Electronic Numerical Integrator and Calculator. It filled an entire room, weighed over 30 tons, it used more than 18,000 vacuum tubes, 1,500 relays, 70,000 resistors, 10,000 capacitors and 6,000 switches. IBM provided the card readers to input the data and Echert wrote the first computer programs. The ENIAC went operational in 1946 and proved more than worthy of the cost of its development. It had a clock speed of 100,000 cycles per second and could multiple two numbers in .2 milliseconds. After processing the data from 500,000 punch cards for six weeks, it declared the hydrogen bomb was feasible.**

|  |
| --- |
| **The ENIAC** |

**By the early 1960s, most large companies and military installations had a mainframe computer. I started working with computers in 1967 as a Computer Programmer at Tooele Army Depot in Utah. We had an IBM 1401 mainframe computer that took up about one-fourth of a large warehouse. This computer had a whopping 4,000 bytes of memory to work with. We programmed in a machine language called Autocoder and it was a real challenge to make your code fit and execute in that small memory and to get the required results. Here is an example of what a mainframe computer room looked like:**

|  |
| --- |
| **IBM Mainframe Computer** |

**Back then, there was no data networks. If we wanted to share some data with another military organization, we had to hand-carry the magnetic computer tapes or ship them by U.S. Mail. Due to the Cold War with the Soviet Union back in 1960s, the** **U.S. Defense Department was exploring ways data could still be disseminated even after a nuclear attack. This eventually led to the formation of the ARPANET (Advanced Research Projects Agency Network), the network that ultimately evolved into what we now know as the Internet. ARPANET was a great success but membership was limited to certain academic and research organizations who had contracts with the Defense Department.**

**January 1, 1983 is considered the official birthday of the Internet. Prior to this, the various computer networks did not have a standard way to communicate with each other. A new communications protocol was established called Transfer Control Protocol/Internet Protocol (TCP/IP). This protocol allowed different kinds of computers on different networks to "talk" to each other. ARPANET and the Defense Data Network officially changed to the TCP/IP standard on January 1, 1983, hence the birth of the Internet. All networks could now be connected by a universal language.**

**So, basically, the Internet is a global system of interconnected computer networks that use the standard Internet protocol suite (TCP/IP) to link several billion devices worldwide – including your personal computer (PC) and smartphone. But, hold on just a second! We have not invented the first microcomputer or the PC yet. And remember, no computer works without the appropriate Operating System.**

**Enter stage left - Microsoft. The history of Microsoft began on April 4, 1975, when it was founded by Bill Gates and Paul Allen in an Albuquerque garage. In 1980, Microsoft formed a partnership with IBM that allowed them to bundle Microsoft's operating system with IBM computers, paying Microsoft a royalty for every sale. In 1985, IBM requested that Microsoft write a new operating system for their computers called OS/2. Microsoft wrote the operating system, but also continued to sell their own operating system, which proved to be in direct competition with IBM’s OS/2. Microsoft Windows eventually overshadowed OS/2 in terms of sales. When Microsoft launched several versions of Microsoft Windows in the 1990’s, they had captured over 90% market share of the world's personal computers**

|  |  |
| --- | --- |
| **The Apple II series was the first highly successful mass-produced microcomputer. It was designed primarily by Steve Wozniak, manufactured by Apple Computer (now Apple Inc.) and was introduced in 1977. The original Apple I was difficult to use and didn’t sell well.** | **Apple II** |

|  |  |
| --- | --- |
| **The term “Personal Computer” was not used until IBM got into the microcomputer making business. The first IBM Personal Computer, commonly known as the IBM PC, was model number 5150 - it was introduced on August 12, 1981. Because of the success of the IBM Personal Computer, the generic term PC came to mean more specifically a desktop microcomputer compatible with IBM's PC products.** | **IBM PC Model 5150** |

**The Computer Revolution had started for real and along with it, came the computer coding heroes - the hackers. This new breed of computers needed software (computer programs) to make them work and do things to be productive. Us computer programmers (hackers) were a different but fascinating group. There was nothing we liked to do more (at work) than sit in a corner and write code. We didn’t like to be bothered by other humans. This was probably why many people thought of us as nerdy and social outcasts. I think a better description of us “old-time” computer programmers would be – “imaginative, adventurers, visionaries, and risk-takers.” I did notice over the years that my co-workers seemed to like me a lot better when they had a problem with their computer.**

**The World Wide Web, or WWW, was created as a method to navigate the now extensive system of connected computers. Tim Berners-Lee, a contractor with the European Organization for Nuclear Research (CERN), developed the first hypertext program called ENQUIRE. The program was designed to make information readily available to users, and to allow them to explore relationships between different web pages. In 1989, he partnered with Robert Cailliau to develop the first Web browser and Web server. They insisted that the Web should be available to the public for free and with no patents. To this day, nobody owns the Internet or the World-Wide Web. This is great!! But don’t expect it to last forever – the government eventually taxes all things that people like and use a lot.**

**A brief history of email - Mankind has always had a compelling desire to communicate with each other. In ancient times this could be verbally or in some form of writing. If remote communication was required, then messages had to be physically carried or sent by a messenger. Examples of early forms of remote transmission of messages not requiring a person to actually move between the sender and the receiver would be the African 'jungle drum' or the Indian 'smoke signal'. These were somewhat lacking in security and privacy, however.**

**The first messages transmitted electronically started in the last century with the telegraph (by wire) and Morse code transmissions (via airways). The telex network was used extensively by business on a world-wide basis from the mid-1920's to the mid-1980s. The telex network was independent of the telephone network and telex machines could connect with and communicate with any other telex machine on a global scale.**

**During the 1960's and 1970's many companies who were using mainframe also used email facilities on those systems. This enabled users of terminals attached to those systems to send messages to each other. As companies began to connect their central systems (hosts) to branch offices and subsidiaries, then employees were able to send email to other employees of that company on a world-wide basis. The same was true with government and military systems.**

**In the 1980's, the phenomenal growth of personal computers created a whole new type of email technologies. Some of these systems were proprietary 'dial-up' systems such as MCI Mail, EasyLink, Telecom Gold, One-to-One, CompuServe, AppleLink, etc. For two people to exchange messages remotely on these systems, they had to both be subscribers. The proprietary systems did not interoperate or transmit messages from one system to another and were notoriously unreliable.**

**In the 1990’s, as company and government networks slowly evolved from terminal-based host-access, the Internet was becoming more widely used for access to information. Firstly for military use, then academic and commercial communications. As the Internet became available to more people, both privately and through company connections, the email facilities available to users have evolved from the proprietary email systems available only within company networks to the Internet email system we have today that is available to everybody world-wide.**

**How in the world did we ever get along without email?**

**Also during the 1990s, computer servers and server data farms replaced most mainframes. I worked on IBM mainframes for most of my Federal Government career (1967 to 1999). I wrote computer programs and maintained the IBM operating system for the Army’s four mainframe computers located at Fort Shafter, Hawaii; Camp Zama, Japan; Yongsan, Seoul, Korea and Camp Walker, Taegu, Korea. It was a great job and a very sad day when the Army took out the last mainframe computer in September 1999, which was the one in Taegu. It was also my last TDY trip to Korea which is a country I enjoyed going to very much. Come to think about it, I could use a nice little vacation to Korea right now.**

**Next came mobile “wireless” pagers, cell phones, and finally the smartphone.** **You know – that thing everybody walks around in a hypnotic state staring at like a bunch of zombies. Given how common smart phones are now days, it is shocking just how recently they were introduced. The first BlackBerry smart phone was developed in 2003 although the company did produce other devices before that – mostly pagers. The Apple iPhone was introduced in 2007. More recently, we got the iPad and the Tablet. It is amazing how small and how powerful these devices have become. Who knows what the next BIG thing is going to be?**

|  |
| --- |
|  |

**The Internet, the World-Wide Web, and all this technology has led the world into a hacker’s paradise. All computers and other devices connected to the Internet are targets for hackers including your PC and smartphone. Computer hackers break into computer systems in order to steal, change or destroy data, often by installing dangerous malware without your knowledge. Their clever tactics and detailed technical knowledge help them access information you really don’t want them to have like your bank account and credit card numbers.**

**How do computer hackers and predators find me? Anyone who uses a computer connected to the Internet is susceptible to the threats that computer hackers and predators pose. These online villains typically use phishing scams, spam email or instant messages and bogus websites to deliver dangerous malware to your computer and compromise your computer security.**

**What can computer hackers do to me? While your computer is connected to the Internet, the skilled hacker can install malware on your PC which can quietly transmits your personal and financial information back to the hacker without your knowledge or consent. Or, a computer hacker may capture private information you unwittingly revealed on a social website. In either case, they may:**

* **Hijack your usernames and passwords**
* **Steal your money and open credit card and bank accounts in your name**
* **Ruin your credit**
* **Request new account Personal Identification Numbers (PINs) or additional credit cards**
* **Make purchases and max out your credit cards**
* **Add themselves as an authorized user so it’s easier to use your credit**
* **Obtain cash advances**
* **Use and abuse your Social Security number**
* **Sell your information to other parties who will use it for illicit or illegal purposes**

**How will I know when I have been hacked? Here are a few signs of a possible hacking:**

* **Anything out of the usual that is happening on your computer such as:**
* **Your standard programs won't open or work correctly**
* **Files that you didn't delete appear to have disappeared**
* **File contents have been changed and not by you**
* **You cannot access programs using your usual password**
* **There are programs on your computer that you didn't put there**
* **Your computer connects itself to the internet frequently**
* **Your mouse cursor moves around all by itself**
* **Your printer may behave strangely - It may not print at all or it will print different stuff than what you wanted**
* **When you go on the Internet, more strange things seems to be happening such as:**
* **One or more sites refuse you access because of password failure**
* **Your internet searches are being redirected**
* **Extra browser screens appear for no apparent reason**
* **If you have your own website, you can’t get to it or when you do, it shows something other than what you expect**

**COMMENT: When my Internet Service Provider and my website was recently hacked, the hacker kept adding malicious files to my root directory. Then sometimes when I or other people went to my website, they would see dirty pictures or a bunch of swear words and racial slurs. I finally changed to a more secure Internet Service Provider.**

* **Additional toolbars appear in your browser**
* **Random and frequent pop-ups appear on your computer.**
* **Everybody in your email address directory list get fake emails from you**
* **Your anti-virus software is not working properly or is turned off**

**NOTE: If any of these things are happening to you while you are on the computer, disconnect from the internet immediately. Check the accuracy of your personal accounts, credit cards and important documents. Are there unexplained transactions? Questionable or unauthorized changes or charges? If so, dangerous malware, installed by criminal hackers, may already be on your computer. You need to have a technical professional take a look at your computer and get it fixed.**

**What can I do to protect my computer from hackers?**

* **Continually check the accuracy of personal accounts**
* **Only buy online from secure reputable companies**

**NOTE: Check for the closed padlock or key symbol in the browser window when entering your credit card details and other personal information online.**

* **Use “strong” passwords and change them every 30 days**
* **Don't store important passwords on your computer**
* **Use extreme caution while on Facebook and other social media websites**
* **Limit the personal information you post on online**
* **Carefully monitor requests by online “friends” for predatory behavior**
* **Keep personal and financial information off of your computer**
* **Make sure your antivirus software is installed and working correctly**
* **Install a firewall**

**NOTE: A firewall is a software program and/or a hardware device that helps screen out hackers, viruses, and worms that try to reach your computer over the Internet.**

* **Install latest updates to your operating system and web browser**
* **Avoid questionable websites**
* **Only download software from sites you trust**
* **Don't open messages from unknown senders**
* **Immediately delete messages you suspect to be spam**

**I think computer companies, credit card companies, banks, our government, and all commercial companies selling things online need to do a better job in stopping these “black hat” hackers. Here are a few ideas I can think of that might help:**

* **All computers sold need to have antivirus, spyware, and a firewall software already installed when the customer buys it. No computer should be allowed to access the Internet without these.**
* **Credit card companies and U.S. stores need to start using credit cards with an embedded microchip - immediately. The embedded chip makes the card extremely difficult to counterfeit or copy. The embedded chip stores information required to authenticate, authorize and process transactions.**
* **Companies need to use more secure servers to store credit card numbers and other customer personal data.**
* **Banks and credit card companies need to alert card users more quickly when where are unusual or suspected fraudulent charges on the card. If they wait until the card user gets their monthly statement, it is too late.**
* **Companies selling stuff online need to make sure that the buyer is who they say they are. Items should not be sent to third party addresses without additional verification. Customers should use PayPal or similar method to make an online payments, receive or send money or to set up merchant accounts. This way, you don’t have to enter your credit card number online every time you buy something.**

**Why can’t the FBI and/or other authorities catch more of these criminal hackers? Cyber attackers use viruses, worms and other malware to take control of Internet servers or personal computers, creating a network of "zombie" or “proxy” computers under their control that they can use to launch their attacks on the real targets like the Pentagon or Microsoft. As a result, an attack may appear to come from a particular server or computer, but this does not mean the attack originated at that device. Hackers will setup a string of proxy servers located in different countries prior to launching an attack which greatly complicates the legal process of trying to catch these bad people. It seems like only the inexperienced and dumb hackers get caught.**

**Even Microsoft who has some of the smartest computer professionals in the world couldn’t catch the hacker who hit their installation last year. Microsoft security experts knew that a hacker had access to one of their systems and were working closely with law enforcement trying to catch the criminal. But after more than a weeklong game of electronic cat and mouse through the computer software giant’s vast computer systems, they failed to capture the hacker.**

**Yes, the hackers are out there “laughing” at law enforcement and all of us law abiding citizens. They have formed Facebook groups where they can all get together for a good laugh and exchange ideas on how to better hack and steal and cause mayhem to computer users around the world.**

**Governments, “White Hat” hackers, and the military need to work together to establish an International Cyber Police Task Force to track down and deal with these criminal hackers before the problem gets any worse. I think they need to be treated the same as terrorists. Maybe after they pinpoint exactly where the hackers are located, our military should use armed drones to wipeout a few of these international “Black Hat” hackers. Then, maybe, they won’t be laughing so hard!**

**From now on, please refer to me as only a Computer Programmer – I don’t want to be known as a hacker any longer. Good luck with your computer and other online devices – and be careful.**

[**bigdrifter44@gmail.com**](mailto:bigdrifter44@gmail.com)