Why Antivirus Software Cannot Prevent All Computer Viruses

By: Jamal Omar Mohammed

Date: ٢٨ / ٠١/ ٢٠١٦

It is clear that computer networking through using the Internet and sharing information is the cause of infections by viruses and spam because the Internet is flooded with them. According to a recent report, ٩٨% of all emails that are received by users are spam (Carolyn, Network World). The big mistake made by computer users is that they think that using antivirus software is enough to protect them from infection, since everyone has an antivirus program. One might reasonably ask why this antivirus software cannot prevent all computer viruses. Antivirus software cannot prevent all computer viruses because of the intentional purposes of viruses-makers, computer user behaviors, and the fact that viruses are a moving target.

Before discussing the reasons behind antivirus software limitations in the prevention of computer viruses, it is necessary to provide some background information about computer viruses. A computer virus is a set of codes written in a variety of system programming languages such as visual basic, Q-basic, C, C++, and Java. Essentially, computer viruses are written to enter a computer system and attach their codes to an executable system file on the operating system without the user's consent. In other words, computer viruses can attack their victim via email attachments, freeware applications, ads, computer networks, and media storage. Many computer viruses have the ability to duplicate themselves or change their code during an infection. These alterations prevent the security software from identifying the virus signature. Hence, the virus begins to launch its payload throughout the computer system. In the beginning, antivirus companies tried to develop different software to detect, prevent, and remove viruses. Since antivirus software started in the late ١٩٨٠s, antivirus software is often the subject of contentious debate. Computer viruses have become a serious issue for everyone in information technology production. Also, viruses vary according to their programming scale. Some viruses can be a simple character displaying on your screen while others can turn

into malicious code, which can format the entire hard disk. Security companies always face challenges with computer viruses because some viruses can change their code during an infection, such as the polymorphic virus. They recognized that the creators of computer viruses often come from those countries that have suffered lots of depression, unstable justice, and bitterness, and the creators have the ability to destroy others' lives in a vicious way. As a user, one may ask about the number of computer viruses existing in the digital world. It is expected that there are more than ٣٠,٠٠٠ computer viruses currently in existence, and virus makers generate ٣٠٠ viruses each month. In ١٩٩٢, the numbers of computer viruses ranged from ١,٠٠٠ to ٢,٣٠٠ viruses, and through the years these numbers increased to ٦٠,٠٠٠ viruses. This estimate includes a variety of computer viruses such as destructive viruses, Trojans, worms, and other types. Today, there are over ١٠٠,٠٠٠ in the digital world and some researchers and computer experts declare that if a computer connects to the internet, it might experience a virus in less than ٥٠ seconds (Computer Knowledge Virus Tutorial, page ١٣).

New vulnerabilities have been discovered and fixed by software vendors who provide software patches and updates. In "what is a virus," Brian Aldridge states that Bob Thomas created the first computer virus named Creeper in ١٩٧٠. Creeper's characteristic was to replicate itself along with infecting remote computers. Creeper contained a taunting message that appeared as "I'm The Creeper: Catch Me If You Can" (Aldridge).

At that time, before computer networks were becoming widespread, most viruses were transferred to other computers via removable media, mainly floppy disks. Nowadays, computer viruses commonly spread through the Internet, LAN (local area network), and WAN (wide area network) networks (Jesdanun).

Another reason why antivirus software cannot prevent computer viruses is because of the intentional purposes of virus makers. Motivation coming from malicious pleasure is one of the intentional purposes behind virus makers. Motives of virus writers have an effect on the efficacy of antivirus software because antivirus software could prevent all viruses if virus makers stopped writing new viruses through using new tactics. The role of antivirus software is to prevent all the viruses that were created before making this antivirus software or installing a new update. Inability of antivirus software to prevent new viruses is the main problem. So, it is important to know the motivation of virus makers, and work to reduce it. According to the article "Who Creates Malware and Why?," "As soon as there is an opportunity to misuse something, somebody will definitely find new technologies and use them in a way that was not intended by the inventors, but in an altogether different way — for their own interests or to assert themselves to the detriment of others" ("Who Creates Malware and Why?"). Some virus makers create a virus to demonstrate their ability. They put their action in progress, and they develop a computer virus with no pecuniary purpose. An example of a putatively benevolent computer virus is the compression virus by Fred Cohen, an American computer scientist. In ١٩٨٣, when he was a student in the engineering department of the University of Southern California, he wrote a computer virus during his preparation for a research paper. The viruses that he wrote for a parasitic application are meant to compress computer applications in order to be able to transfer from one computer to another (Cohen).

Essentially, virus creators can be classified into three categories. The first category, adolescents, often writes a simple computer virus that they release in to the wild. Similarly, college students write a computer virus as a part of their study curriculum. On the other hand, there is another kind of computer virus writer. The criminal virus writer mostly creates a very

destructive virus and releases the virus into the digital world anonymously. Writing or creating a computer virus does not require a lot of skills. Basic training in programming languages can be enough for a person to create a computer virus. Any computer user with some experience in coding or programming can write code which operates as a virus to the computer system (Ubarhande, page ٢-٤).

Some of the virus makers create a virus to show off. Virus makers intend to produce a virus that has no serious side effect. They just want to display themselves through such a simple virus type. In fact, all computer viruses are malicious software. There is not any advantage behind creating a virus. According to the world's most famous hacker, Kevin Mitnick, "I was not interested in selling the source code or doing anything with it. It was more about the challenge of getting it. I had to breach like four layers of security to get in." His goal is not monetary, just merely to challenge others (Mills). Because many virus developers are smart enough to write or develop innovative viruses, if they used their skills in useful works, the world would be changed into a better and safer place. Also, there are others who would not like to spend time on such work. They would rather gain notoriety in more resourceful ways, such as only claiming to have developed a virus without having done so. Furthermore, virus writers have different attitudes and aims when they write computer viruses. Those virus writers' behaviors vary according to their ethics and the environments in which they grow up. Through creating viruses, they all try to show their powerful ability.

Consequently, some of the virus makers create a virus as a prank or practical joke. They create a non-disruptive virus in order to make fun of their friends or colleagues. Richard Skrenta was the high school student who released a new computer virus in ١٩٨١ (Jesdanun). He already had notoriety among his friends because of sharing free computer software programs and games with his friends on Floppy disks infected with viruses. Therefore, his

friends decided to stop receiving floppy disks from him. During a summer break from Mount Lebanon high school in California, Skrenta thought about a method to alter floppy disks without touching them physically. So he wrote a virus from scratch and named it Elk Cloner. Later, Skrenta attached a short poem to the virus source code in order to use it as a prank on his friends. The first virus, which infected Apple II computers during that time, is known as the Elk Cloner virus. The virus was circulated among friends and in the high school's computer lab. An extremely destructive virus was developed from the Elk Cloner virus, which is now known as the boot sector virus (Jesdanun). However, Skrenta was a revolutionary in the creation of his virus. He was not sorry for developing a virus because he thought if he had not produced such a virus, someone else might have written it. Here is the actual poem which his virus embedded:

> Elk Cloner: The program with a personality
>
> It will get on all your disks
>
> It will infiltrate your chips
>
> Yes it's Cloner!
>
> It will stick to you like glue
>
> It will modify ram too
>
> Send in the Cloner! (Jesdanun)

Sociopolitical causes are also one of the intentional purposes behind virus makers. These individuals who create computer viruses for sociopolitical motives are called hacktivists or cyber-terrorists; they gain unauthorized access to computer systems and perform a series of destructive actions in order to achieve political goals. Most of the

computer virus creators use their skills to create a powerful and destructive virus in order to attack a governmental agency or media organization. Virus writers design a structure for the content of the virus very carefully. They write set codes for the virus and, once the virus goes into the target computer system, as a habitual characteristic of the virus it starts to copy itself inside the operating system very quickly (Top١٠hm).

The programmer of the virus creates a very good structure for the virus. The content of the virus may contain harmful commands. The virus gathers information from the logs of the user such as Outlook address book, real-time screen capture, and keystroke logs, and sends all the collected data back to the virus writer. Nowadays, it is very common to create such computer viruses. For instance, the viruses Code Red I and Code Red II have been written by an anonymous creator in China. These viruses are known as the most destructive viruses in the history of computers. When the shared computers and servers get infected by this virus, a message comes up on the screen of a computer, saying “Hello, Welcome to www.worm.com." The virus infected the White House computer systems as well, and it caused them a major loss. The estimated loss caused by Code Red I and Code Red II to the world is above $ ٢.٥ billion (Top١٠hm). This pair of viruses was propagated through huge computer networks, and the viruses left copies of themselves inside each client’s computer which was linked to the network.

In addition to the above issue, these individuals who create computer viruses for sociopolitical reasons also do so for revenge. Some people may be getting angry over what other countries might have done to their nation. So, they will write a computer virus intentionally to take revenge. It is plausible that a virus named Stuxnet, designed to attack Industrial Programmable Logic Controllers (PLCs) was developed by the United States of America and Israel. Kim Zetter explains:

> Stuxnetwas launched in ٢٠٠٩ and ٢٠١٠, and possibly ٢٠٠٨ as well, and targeted cascades and centrifuges at the Natnaz uranium enrichment plant in Iran. The cyber weapon was reportedly designed by Israel and the U.S. in an effort to set back Iran's ability to produce a nuclear weapon, though the U.S. has not officially acknowledged its role in the attack. Until the attacks occurred, intelligence agencies speculated that Iran would be able to produce a nuclear weapon by ٢٠١٠. The attacks by Stuxnetare believed to have set back the program by an estimated three years. (Zetter)

The virus was created in order to slow down the process of the Iranian nuclear system. After five months, the Iranian government declared that they were attacked by the Flame virus that belongs to Stuxnet. Later, two security firms that worked separately on that issue, refused to explain who developed the virus.

Current and former national security agencies confirmed that the USA has played a big role in creating the Flame virus. Also, another world news agency has reported that Israel was also involved. During past years many websites were attacked by hackers, especially online news websites. When some of them published some news about a religious or political activity, hackers immediately attacked those websites by ceasing their broadcast on the Web and changing their content. Sometimes a governmental agency may try to use a powerful computer code, which acts as virus, to monitor some certain countries' interior issues (FactMonster).

Antivirus software also cannot prevent computer viruses because of computer user behaviors. Clicking on links to dodgy websites is one of the self-harming behaviors of computer users. Virus makers or hackers write other types of viruses like adware and spyware. Many hackers attack their target by using an advertisement. They create ads and put

them on the homepage of many websites as a means of advertising. When a user mistakenly opens up a link without having information about it, the virus, which is known as adware can start to search the target computer for banking information, and it collects all the necessary usernames and PINs (Personal Identification Number) the user saved on the computer system. Also, many victims of adware suffered bankruptcy when they got a spam email that hacked or stole information. Clicking links to dodgy websites could be one of the reasons that the antivirus industry repeatedly blames users. While antivirus software will develop continually, they cannot prevent computer viruses that result from user behaviors.

Computer users click on pop-up windows because they cannot recognize the risks involved with fake pop-ups. Even thought antivirus companies update antivirus software frequently, they cannot force user to avoid clicking on fake links. According to Peter Stavroulakis, "Many phishing kits contain the requisite pages, which can be loaded by point and click"(page ٤٣٥). Through clicking the links that hackers used as a technique for phishing, once a victim enters her credentials by clicking it, they might be stored on a separate egg-drop server. Just one click is enough for hackers to input some files that they have for doing their work. When users are clicking on links randomly or by mistake when browsing Web pages, they may be running programs. While running this program, the antivirus software does not do its job because this program was chosen by user to run. From time to time, antivirus companies try to write programs that add this protection. The problems are that most of the time when a pop up window shows, users do not know about the consequences of opening this page. When users open this page through clicking on it, this guarantees opening the page without action by the antivirus software, this is why antivirus software fails to fully protect its users.

Other problems with clicking on fake links are the use of social networks by a variety of people. Most users of social networks do not have enough information about phishing attacks; according to Tom Jagatic they showed that over ٧٠% of successful phishing attacks are done on social networks. This behavior of computer users is another reason that antivirus programs cannot examine suspect programs on their own. Since social networks are used widely, virus creators try to attack victim's computers through them. Through finding personal information from your account, simple details like your phone number, or your birthday, or your name, hackers can often crack the "account recovery" features of any other online accounts that users have. Recently, hackers are using a common malware scheme through sending a message to all their friends with a link using their Facebook account. Most of the time Facebook users might be trusts the safety of this malicious link that is shared by the hackers. It is one way that hackers try to use phishing scams, fake login sites, or other deadly threats that look like they come from a friend. Obviously, this is the main reason that as Facebook's popularity grows; computer attacks through social networks will grow too.

Clicking on links to open email attachments from unknown senders is also another behavior of oblivious computer users. Clicking on a link is also a reason for infection by viruses. This will happen when a specific program is run by users by clicking on a link.According to a survey done by Messaging Anti-Abuse Working Group (MAAWG), the results of the group's second year survey of email security practices offers an interesting insight into the various interactions end users tend to have with spam emails (Danchev). This survey shows that it is important for us to know how often people will open things from someone that they do not know. People just click it to see what happens, and many people do not know to double check the messages they read. Those spam emails usually scam new computer users by sending them an email in the name of a bank, in which the email asks the

user to provide some primary information regarding their bank accounts such as first name, last name, password, date of birth, security information, or bank account number.

According to "Consumer Fraud Reporting" in ٢٠٠٥, the Max Theater Company released a product and advertised it as anti-spyware software. The Federal Trade Commission (FTC) took action against that company which released a false product on the Internet. The FTC stated that "Unbelievably, there are products for sale that claim to block and remove adware and spyware, yet these products either do nothing, or are actually spyware themselves!" Users assumed that the product might remove spyware or adware on computers, but instead of removing spyware the product was a virus by itself (Consumer Fraud Reporting). It is a good idea if people tell their friends what their email looks like. This will help others who receive emails from these users which do not follow those rules; recipients should delete them and contact the senders. This is the other reason that antivirus software cannot be the only defense. More important than having antivirus software is the need to be aware of what is going on with one's own email. By downloading an attachment through email from someone they do not know, some users made a mistake to allow malware infections or theft of their credit card information.

Mostly, spyware and adware enter a computer through a form of security software. Occasionally, computer users want to use free security software, or freeware. Hackers or computer virus writers upload spyware software on many websites. Those victims get infected after downloading the program with the intention of protecting their computers. When the spyware is successfully installed on the system, it instantly begins recording information and collecting logs and then sends all the data collected to the writer of the virus. Usually, those security software programs have some definite errors such as misinformation about the software, misspelling of the program name, and fake or unknown company names

and copyrights. Those companies that advertise their goods on the websites will regularly pay for their advertisements and there are dozens of advertisements with unknown or strange names. Those ads can be activated by just a click of the mouse, which leads to extremely harmful consequences. Identity theft happens when other hackers steal and use a real person's name and email address. After gaining all the required personal information, they use it in political, personal, religious, and commercial matters, which leads to social chaos. Identity theft is common nowadays. As technology improves, hackers can steal more personal data. Furthermore, virus writers or hackers write other types of deceptive software such as Click Fraud. In "Click Fraud," Helen Martin explains:

> Click fraud is a criminal offence in many areas. The main profit-makers from click fraud, the owners of the page whose traffic is being fraudulently increased, are not necessarily the perpetrators - in some cases rival sites or advertising systems have been found to have set up click fraud to incriminate or damage the profits of their competitors, while other more personal motives have also been suggested to be behind instances of click fraud. (Martin)

Obviously, the primary reason for creating a virus is to trace someone's computer information. The zombie network is an enormous world of viruses that includes spam, click fraud, and money mules. Creators of viruses build up a network of thousands of computers, and they send spam and advertisement emails ceaselessly. The spam emails damage the computer system unit and corrupt hardware parts, and they frequently steal secret information. The infected computer shows denial of service during operation mode, after that the spam will erase the media totally (Brian, Fenlon).

Sometimes spyware can bind itself to a Trojan or virus file in order to get into cookies which are usually helpful. The cookies mostly save user identities and passwords which helps the user to retrieve that information at a later time. A good example of spyware is the "ILOVEYOU" virus (Shneiderman and Plaisant ٤٢٦ - ١٣).

The name of the virus is very lovely, but the structure was designed to destroy a whole computer system. When the "ILOVEYOU" virus infects a business company's computer system, all important data and information about the company reached unauthorized hands which caused them to lose money. Regardless of the time they lost, they shut off all computer systems until they fixed it. The best way to keep viruses out of computers is to use licensed operating system software, and security software, and keep the computer up-to-date. Also users should be aware of ads and promotions while surfing on the internet.

Antivirus software cannot prevent computer viruses because a virus is a moving target. Viruses are a moving target in consequence of the fundamental flaws in the security architecture of PC operating systems. While antivirus companies learn how to spot a set of virus programs, at the same time the virus makers learn how to write the latest virus that cannot be spotted. In a new piece for Wired, security expert Bruce Schneier wrote about the Storm botnet:

> Not that we really have any idea how to mess with Storm. Storm has been around for almost a year, and the antivirus companies are pretty much powerless to do anything about it. Inoculating infected machines individually is simply not going to work, and I can't imagine forcing ISPs to quarantine infected hosts. A quarantine wouldn't work

> in any case: Storm's creators could easily design another worm -- and we know that users can't keep themselves from clicking on enticing attachments and links. (Wired)

According to the description of the writer, “Storm represents the future of malware.” Uneducated computer users and experienced virus writers are the reason that the security architecture of user PC operating systems is fundamentally imperfect. This is the reason that viruses will not be beaten until operating systems are changed. While viruses are a moving target, the reason that Mac and Linux systems are more secure than Windows is not because those computers have a better technology. Those computers have on similar safety models to Windows. They get viruses less often than Windows because they are less popular. Apart from this fact, they are equally at risk.

Viruses are a moving target because of the “arms race” going on between security companies and virus programmers. As a result of this arms race, antivirus companies showed that people cannot isolate systems and users from each other completely because the connection is necessary for doing all the work, required. They think that erecting partitions to limit the spread of malware is possible. Using the Bell-LaPadula model might help limit the spread of viruses, but Cohen reports that “viruses demonstrated the ability to cross users’ boundaries and move from a given security level to a higher security level” (AllNet). The way that antivirus programs work is by making a list of all possible malicious programs. After installing defense software, this antivirus will download a list of malicious programs and try to update it regularly. After that, they daily check users’ computer systems for any viruses. This list that they have is a “blacklist” of the viruses that they have found up to this date. These are the reasons that a virus may appear on a user’s computer before the antivirus program knows about it. After new viruses are made and placed into users’ computers without setting off any alarms, antivirus companies can figure out a solution. These are the

reasons that virus makers are winning the race against the antivirus companies. Virus makers know how to directly attack the security software on a user's machine without getting caught by users' antivirus software.

It has been demonstrated that one of the reasons that antivirus software cannot prevent computer viruses is the different motivations that push people to create computer viruses. Some people want to create computer viruses for malicious pleasure. They create a virus in order to demonstrate their talent. Specifically those types of virus makers are not capable of producing powerful viruses. On the other hand, some virus writers aim to write a computer virus for sociopolitical purposes. Sometimes, computer viruses are created by those persons who views opposing their country's government. In addition, some virus writers have a particular purpose in writing a computer virus, such as financial gain. Computer user behavior is also another reason why viruses can attack a computer system, as a result of clicking links to dodgy websites or clicking links to open email attachments. As a result of fundamental flows in the security architecture of PC operating systems and because of the arms race going on between the virus programmers and the antivirus companies, virus makers are moving targets as they attack their victims.

Viruses cannot do more than damage computer systems, but the writers can include destructive instructions to get personal and other important information. Computer users should always keep their computer programs up-to-date in order to avoid virus infection. They also should be aware of using thumb drive storage. Certainly, nowadays everyone has memory drive storage, but they should not exchange it with a friend or someone else. They have to consider scanning the flash drive with licensed security software prior to opening the flash drive. Overall people have on incentive to create more powerful computers, but viruses will continue to grow with rapid progress in technology.

Works Cited

Aldridge, Brian. "What is a Virus?." *The First Virus. Bite of Tech*. n.pag. (٠٥ Aug. ٢٠١١).Web. ١٦ March. ٢٠١٤. <http://www.biteoftech.com/٢٠١١/٠٩/٠٥/what-is-a-virus/>.

Brian, Marshall, and Wesley Fenlon. "How Computer Viruses Work?" *Howstuffworks.Howstuffworks*, Inc, n.d. Web. ١٣ Mar. ٢٠١٤. <http://computer.howstuffworks.com/virus.htm>.

Carolyn, Duffy Marsan. "CAN-SPAM: What Went Wrong*?" Network World (Online)* (٢٠٠٨): ٥٥. *ProQuest*. Web. ٢٤ Mar. ٢٠١٤.

"Computer Knowledge Virus Tutorial." *Cknow. ValueClick*, ١٣. n.d. Friday. ٧ March ٢٠١٤. <https://coa.edu/assets/IT/vtutor.pdf>.

Cohen, Frederick. "A Case for Benevolent Viruses" *AllNet*. n.pag. (١٩٩١). Web. ٢٠ Feb. ٢٠١٤.<http://www.all.net/books/integ/goodvcase.html>.

Danchev, Dancho. "Survey: Millions of Users Open Spam Emails, Click on Links" *Zdnet.com*. ٢٥ March, ٢٠١٠. Web. ٣ March, ٢٠١٤.

"http://www.factmonster.com/ipka/.html." *Fact Monster.*© ٢٠٠٠–٢٠٠٧*Pearson Education, Publishing as Fact Monster*. n.pag. n.d. Web. ٢٠ Mar. ٢٠١٤. <http://www.factmonster.com/ipka/A٠٨٧٢٨٤٢.html>.

Jesdanun, Anick . "High School Prank Began Era of Computer Virus." *Association Press*. n.pag. (٣١ Aug. ٢٠٠٧).Web. ٥ Mar. ٢٠١٤. <http://usatoday٣٠.usatoday.com/tech/news/computersecurity/wormsviruses/٢٠٠٧-٠٩-٠٢-computer-virus-anniversary_N.htm>.

Jagatic, Tom N., et al. "Social Phishing." *Communications of the ACM* ٥٠.١٠ (٢٠٠٧): ٩٤-١٠٠. *Academic Search Complete*. Web. ٣ Mar. ٢٠١٤.

Mills, Elinor. "Q&A: Kevin Mitnick, From Ham Operator to Fugitive to Consultant." *CBS Interactive Inc.* n. pag.(٢٢ Jun. ٢٠٠٩). Web. ١٠ Mar. ٢٠١٤. <http://news.cnet.com/٨٣٠١-١٠٠٩_٣-١٠٢٦٩٣٤٨-٨٣.html>.

Martin, Helen, ed. "Click Fraud." *Virusbtn. Virus Bulletin Ltd* . Web. ١٧ Feb ٢٠١٤. <http://www.virusbtn.com/resources/glossary/click_fraud.xml>.

Stavroulakis, Peter, and Mark Stamp. *Handbook of Information and Communication Security*. Heidelberg: Springer, ٢٠١٠.

"Spyware, Adware and Other Malware." *Consumer Fraud Reporting. CFR ٢٠٠٨A*, n.d. Web.١٣ Mar. ٢٠١٤. <http://www.consumerfraudreporting.org/spyware.php>.

Shneiderman, Ben, and Catherine Plaisant. *Designing The User Interface*. ٥th ed. Boston, MA: Pearson Higher Education, ٢٠١٠. ٤٢٦ - ١٣. Print.

Schneier, Bruce. "Gathering Storm Superworm Poses Grave Threat to PC Nets." *Wired ٤ Oct.* ٢٠٠٧. Web. ٢٨ Feb. ٢٠١٤. < https://www.schneier.com/essay-١٨٤.html>.

"Top ١٠ Computer viruses." *Top١٠hm*. n.p., n.d. Web. ١٥ Mar. ٢٠١٤ <http://top١٠hm.com/top-١٠-computer-viruses/>.

Ubarhande, Sachin. "International Journal of Scientific & Engineering Research." *International Journal of Scientific & Engineering Research.* ٢.١٢ (٢٠١١): ٢-٤. Print. ٧ Mar. ٢٠١٤. <www.ijser.org/researchpaper\Computer-Viruses.pdf>.

"Who Creates Malware and Why? - Securelist." *Securelist.com*. N.p., n.d. Web. ٢٥ Apr. ٢٠١٤ <http://www.securelist.com/en/threats/detect?chapter=٧٢>.

Zetter, Kim. "Legal Experts: Stuxnet Attack on Iran Was Illegal 'Act of Force'." *wired.com. Condenast,* ٢٥ ٠٣ ٢٠١٣. Web. ٢٠ Feb. ٢٠١٤. <http://www.wired.com/threatlevel/٢٠١٣/٠٣/stuxnet-act-of-force/>.