Bryan Degro
Jermaine Elliot
Oscar Ortiz
Diego Reinoso

SOFTWARE CRACKERS

Whether it is to accomplish a challenge, to protest, or maybe to just gain recognition worldwide, advance understanding of computers, networks, and systems becomes easier as more people have access to the internet. Society is exposed to many risks from the moment they connect to the internet. Without even turning on your computer, the moment your router and modem obtain an IP address and connect to the world, your whole network is at risk. This is where hackers can also become crucial in making the internet an enjoyable and safe environment. An ethical hacker (also known as a white hat) is an example of a person who has the knowledge, the power, and necessary skills to provide the community with tools which can be useful to prevent harmful attacks from malefic individuals. While a black hat hacker (cracker) is said to be a malicious kind of hacker. Although many crackers can break into software, create malwares and viruses, and bypass internet security, their harmful work can also help to create better encryption methods and better anti-virus software. Also they provide “free” or “cracked” software for those that can’t afford to buy them because of high prices. So are they really harmful to society? Should society see them as skilled experts or as threat? Is their work not valued as it should be?

We will explore both sides of hacking; comparing the benefits and harm they bring to society in our everyday life. Also we will see how they work and how similar or different they can be from each other. We will analyze how both kind of hacking can help to the other either for good or bad, and see if there could ever be a balance between both. In addition, by the end of this analysis we will gain knowledge to understand how hacking works and we will be able to differentiate between a hacker and a cracker.

Motivation

In today’s economy, the cost and demand for computer software can be high; and while programming software takes a large amount of time and money, cracking it can take from hours to days and requires no monetary spend. It is important to have in mind that cracking software requires a high

level of knowledge in programming with different languages in order to understand how the program works, but the most important part of knowledge a hacker should have is assembly language, and without it it is near to impossible for anyone to crack software. So knowing this helps to realize that a cracker is an experienced person in computing and his/ her reasons for cracking are not just vague and childish. Therefore, to understand what really makes these persons good or bad, we have to explore the motivation that drives them to target software; in many cases they have more than one reason to crack software.

Although, every cracker starts cracking for love of knowledge, to explore how secure software is, and to learn how the program coding works, there are other main motives for doing so:

- Social status.- Crackers who publish their work for others to download, like to have recognition of their work and how good it is. In many cases this is a big factor for a cracker to keep up with their work and try to get the best results in the least amount of time. They usually put their nickname in the name of the file containing the cracked software, that way when someone looking for a certain software sees their name, that person can recognize and know, because of previous released software, if it will be a working program with no problems. In downloading sites, it is easy to spot the names of some of the crackers in the field by just reading the comments, in which the users thank and praise the crackers work. These comments are used to rate the cracker in a level according to the proper work, ease of use, and amount of time that took for the release of the cracked software.
- Personal challenge.- As stated before, crackers start their work to use and gain knowledge. This is said to be one main reason for many to start hacking software. Just as in any other person, the feeling of achieving something that looked quite impossible to do, can bring that person's ego up high and gives the drive to keep on trying new and more challenging stuff. In an interview with a cracker, he explains the reason behind his work: "For me I think it's always been mainly about the intellectual challenge, studying code, or 'breaking the minds of protection authors' as one correspondent so eloquently put it." Even though, there are programs that can be really hard and impossible to crack, many crackers love that challenge and take it as a competition amongst them. This also helps get them experience and become better when working on more difficult

programs.

- Software cost and demand.- This category mostly relates to the targeted software, but it also plays a part for the motivation of many crackers. Anyone that uses a computer for work, school, or entertainment, can agree that certain software is needed in order to fully use a computer. For example, when it comes to work and school, there is a need for programs like Word, Excel, PowerPoint, etc. By doing a little research in Microsoft's website, we can see that the price range for Office 2013 ranges from 139.99 to 219.99 according to their package. So, taking in count these 2 factors (demand and price), it is easy to realize that there is a need for these programs. There is where the crackers steps in, whether is for personal use or for others, crackers take in count those factors and begin their work on the software. This is how crackers choose they target, because depending on the demand of the software in the market, means that more users are going to try to download it; therefore the cracker will gain more recognition if they do a good job.

Finally, when we talk about the motives that drive a person to become a cracker, we can conclude that the three named above, are the most important because they connect with each other and depend on each other as well.

Techniques

When performing an attack on a desired target, there are a variety of techniques that a hacker can perform. Before an attack take place however, a hacker would want to perform some reconnaissance on the specified target. The first of these steps is something called Network Enumeration, in this step we find out as much as we can about the specified target. It is with this step that a hacker can begin to figure the type of attack and which tools may be necessary to perform the desired attack. An example of an attack that a hacker may want to perform on a network could be a DoS attack, injecting a virus to a network or simply hijacking a victim computer to gain unauthorized remote access to a computer. The second step that can be performed would be social engineering; this sole step if performed correctly could prevent all other of the steps from needing to be used as access would be gained simply by using social engineering. Not all the time however is this step very successful. most of the time potential

hackers will not gather the sufficient information that is needed in order to gain the access that they want to these specific computers. It is because of this as to why hackers would need to proceed to the other steps of gaining access to a network. Several tools are available for hackers to use depending on the type of attack that they want to perform. There exist programs that can be used to crack passwords such as ophcrack, or cain and abel. Other programs exist if you know certain exploits that a network may have, a program that you may use to take advantage of these exploits would be metasploit. Moreover, if you happen to have the tool of backtracker now known as Kali Linux, you have almost all of the tools needed to perform any type of attack all bundled together into one program. By using Kali Linux, you now have the platform needed to launch an attack. Let's say for example you wanted to crack some passwords to gain access to a secured computer, you could easily use ophcrack located within Kali Linux to perform the attack.

Software Targets

Black hat hackers may use many different types of software to perform their attacks on victims. Whether it is to exploit a recently found security hole on a plugin (like Adobe Flash) or from an unpatched hole in the operative system. The target point will depend on the type of attack and the purposes that the hacker has in mind.

Commercial software for example, will suffer mostly from cracked serial numbers as well as deactivated registration services to avoid them from contacting the company's' server to verify authenticity of the software. Usually, when crackers decide to crack a program, they will use a technique called reverse engineering. Reverse engineering is a technique in which crackers can discover how the program works making it possible to write their own code that will modify the program's original functions (specifically, the security parts). By knowing the structure of the program, crackers can write software known as "cracks" which will execute a code which will re-write the program to be cracked and disable functions like activation, registration and validation. This will allow the user to use the program without any restriction (as if it had been legitimately purchased). Another type of crack (known as key-generators) will generate a serial number registration which will make the program believe it is genuine and will then allow the installation of the program to continue. At the end of the installation, the program works with all

of its functions unlocked as if it was an original copy.

Reverse engineering is normally used by crackers on any software that requires a payment (software known as shareware) to unlock all of the program's features or to remove the trial period limitation. The benefits are clear, a paid program that can be used with all its functions and features fully unlocked with no time trial restrictions. However, when we consider ethics, one then comes to realize the harm done to the companies who are behind these software programs.

Some worldwide known program companies (like Corel or Adobe) have over a decade of software coding. These companies have been developing and improving their software to provide their clients with the newest features available in today's market. It is thanks to the programmers and designers who work for this companies that these tools become so useful to computer users. Unfortunately, piracy seems to strike as new versions come out causing harm to the people and companies who spend their time improving these software suites and services.

If no one paid for software, there would be no competition or motivation to create a better one. No one would bother to invest in computer programs because there would be no profit at all. Customer service would be almost non-existent as the software coder of a free software would have no way to pay someone to help users. Security exploits would take a indefinite period of time to be fixed and features would probably take a long time to make it into every new release. So, is it fair to pay for software? Should everyone be forced to pay for it?

Unfortunately, for many people around the world, what some would consider a low-cost program is far from what others can afford. As we are aware, there are people who can barely afford a computer with internet access making it virtually impossible for them to use authentic software due to high prices.

Not going too far, most college students are not able to justify the relatively high prices of programs like Microsoft Office, Autodesk AutoCAD or Adobe Acrobat. These programs are nowadays a basic need for projects, documents, spreadsheets and designs in a daily basis. Many software companies have released "Student Editions" of their software by reducing the number of features and giving a more affordable price. At the same time, some universities have been providing students with the student edition of these programs which have definitely helped students to be able to work on their assignments. The problem comes when the student finally graduates. These student licenses are only for the duration

of the student in school (which means, not upgradable). In some cases, these licenses do not unlock the full potential and features of the program compared to the full license (which could be needed in the future once the student decides to develop his/her skills as a professional). Anyone who would like a student license and is not necessarily enrolled in an educational institution will need an educational (.edu) email address in order to obtain the registration for these programs. Not having access to this discount (by not having an .edu e-mail address) or the fact that they will have less features and tools to work with gives crackers another reason to pirate software.

Analyzing and Drawing Conclusions

Software cracking comes in many ways. As mentioned, software crackers help individuals not able to afford a particular software product. The effects of software cracking is releasing of fully operable proprietary software without any copy protection. Software companies charge a huge amount for their product. As a result, it encourages crackers to override their systems. Software will be cracked and placed on torrent websites for users to download for free to save money. The advantages of cracked software are commercial profit, understanding how the system works and increase publicity. Software companies are concern because crackers are able to take the software illegal. Next, sell the software online to everyone. Achieving these cracked versions are challenging because company increased their security each year. However, a skilled cracker can easily break through any security by using sophisticated tools that emulate the computer environment such as allowing them to quickly find and remove security code. Although increasing security features will make some crackers excited to work on it. Companies are not educated sufficiently to know that software privacy is not a crime. Software user are affect by software crackers on daily bases. Computer hacking is a breach of computer security. It exposed sensitive user data and risk user privacy. Software users enjoy free software. It saves them on money and peace of mind as long they are able to download it and cracked it correctly. Advance software users can manage to install correctly as compare to novice user. Some instructions may be confusing to novice users. Crackers can get software users in trouble by downloading torrent software. They damage everyone during the process. Crackers send many ignore computer users in jail. Internet users found cracked software on the net. The risk of crack software will get a person in trouble.

In conclusion, the use of cracked software have its advantage. It saves money for software users,

increase commercial profit for crackers and increase publicity for crackers. The disadvantages are software users can risk going to jail for downloading illegal software, increase security will not prevent crackers to break in their software and software companies lose money. We need to know how to prepare ourselves.

References

Corporation, Symantec. "Security News." *Security News*. PCTools.com, Mar.-Apr. 2010. Web. 17 Jan. 2014. <http://www.pctools.com/security-news/crackers-and-hackers/>

Cyber Coyote. "Happy Trails Computer Club." *Hackers & Crackers*. CyberCoyote.org, Aug.-Sept. 2009. Web. 19 Jan. 2014. <http://cybercoyote.org/security/av-hacker.htm>

Armor2net Software. "The Most Common Methods Used by Hackers." *The Most Common Methods Used by Hackers.* Armor2net Software Ltd, Aug.-Sept. 2002. Web. 19 Jan. 2014. <http://www.armor2net.com/knowledge/hackers_methods.htm>

The Twenty Twelve Theme Blog at WordPress.com. "Successful Software." *Successful Software*. SuccessfulSoftware.Net, 7 Apr. 2011. Web. 15 Feb. 2014. <http://successfulsoftware.net/2011/04/07/interview-with-a-cracker/>

Tech-Faq. "How Do Keygens Work?" *Tech-FAQ*. Tech-faq.com, 22 May 2012. Web. 15 Feb. 2014 <http://www.tech-faq.com/how-do-keygens-work.html>

Scribd. "Hack How to Create Keygens." *Scribd*. Infobits, June-July 2013. Web. 21 Feb. 2014. <http://www.scribd.com/doc/3042847/Hack-how-to-create-keygens>

Mindsprings "Online Argument." *Cracks*. Mindspring.com, 3 May 2013. Web. 23 Feb. 2014. <http://www.mindspring.com/~win32ch/Crackit.htm>

The Silicon Realms Toolworks. "Software Protection, Licensing and Copy Protection." *Software Protection, Licensing and Copy Protection with SoftwarePassport for Windows Applications; Story about*

Hackers, Crackers, Script-Kiddies, and Pirates. Digital River, Feb.-Mar. 2009-2014. Mindsprings "Online Argument." *Cracks*. Mindspring.com, 3 May 2013. Web. 24 Feb. 2014. <http://www.siliconrealms.com/articles/hackers_crackers.php>

Yamauchi, Hiroki. (January 23-25, 2006) Software Obfuscation from Crackers' Viewpoint. "Advances in Computer Software and Technology." IASTED International Conference. [PDF]. <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.102.652&rep=rep1&type=pdf>

InformIT, The Trusted Technology Learning Source. "Introduction to Software Security." *Hackers, Crackers, and Attackers.* Gary McGraw and John Viega. 2 November 2001. Web. 25 Feb. 2014. <http://www.informit.com/articles/article.aspx?p=23950&seqNum=3>