Grace Tang
Mr. Wisniewski
ENGL398C
27 March 2024

# One Homemade Computer Virus? Coming Right up!

Onel de Guzman sits in front of his computer, grumbling to himself, the comments on his undergraduate thesis glaring at him. His thesis proposal was about a program he created himself to fight the injustice of paying for internet in his home city, Manila where they charge by the HOUR. The internet should be free, no? It's a basic human right, especially for the current generation in the digital era. With his extensive skill in VBScript (Visual Basic Script) and detailed knowledge of operating system (OS) structures and viruses, he laid out a simple trojan virus that can run automatically and retrieve internet passwords from the victims for others to use. Onel was extremely proud of his thesis, but his professor didn't seem to be impressed, so he rejected the proposal unanimously. They scribbled statements like how "they didn't support 'burglary'" or "this is stealing". Stealing? Onel would state his program did a lot of things, but stealing wasn't one of them. To Onel, the person who always had the password will still have that password and the internet access for the amount they paid anyway, so no stealing was occurring. The professors just didn't believe it could be done or didn't believe his cause was just, Onel reasoned. To prove them wrong, he began the process of bringing his virus into reality.

The process of writing a virus was relatively easy, it was just the details that made the process difficult. Luckily, Onel knew this process like the back of his hand.

## Step 1: Cater A Recipe For Your Guests

First, he had to determine which operating system he would attack and the weaknesses he would exploit. Different operating systems have different strengths and weaknesses, but Onel needed to choose the one that would provide him with the best results. The purpose of his virus is to infect as many computers as possible, so it makes sense to choose the most common OS. In his city, the most common operating system used is Microsoft Windows, which was perfect for this virus since it relied on the Microsoft Windows exploit that runs system code simply from just opening a file/email with code in it. With this heavily in mind, Onel quickly moves on to the next step.

## Step 2: Choose the Best Ingredients

Next, he had to decide which language to use. There are multiple to choose from, C/C++, Python, Assembly, VBScript, R, etc. (*Top Programming Languages for Malware Analysis | Cybrary*, n.d.). Onel was extremely proficient in VBScript and knew it would work well with his virus, so he opened a new VBScript file immediately.

## Step 3: Have a Mental Image of the Final Product

Grace Tang
Mr. Wisniewski
ENGL398C
27 March 2024

The third part was the brainstorming process. How was this code gonna look and how would Onel get others to download the trojan onto their computer? Onel racks his brain, what would he open with little to no hesitance? Hmmm… Oh! A love letter from a secret admirer! After all, if a person is spending all their money and time on the internet, there's a good chance they are lonely and single. With that, Onel quickly typed out the title and name for his code: "LOVE-LETTER-FOR-YOU.TXT.vbs".

**Step 4: Follow Your Recipe**

The next step in virus development is to decide what his code would do and program it. This step is the hardest one and varies the most. Luckily, Onel already knew what he wanted his virus to do from his thesis: to get the passwords from another's computer and send it back to him without the user knowing while corrupting important files on their desktop. So now, he had to program the basic functionality of the code. How was he going to do that?

Well, first he broke down what needs to be specifically done. The first step is to access and change the timeout value of the computer's registry key by using a shell. After that, Onel creates three files: MSKernel32.vbs, Win32DLL.vbs, and LOVE-LETTER-FOR-YOU.TXT.vbs. MSKernel32.vbs and LOVE-LETTER-FOR-YOU.TXT.vbs are sent to the Windows folder while Win32DLL.vbs goes into the directory, allowing the rest of the code to function properly.

The next step is to write a function that creates and updates special registry keys. Here, MSKernel32.vbs and Win32DLL.vbs are run on the local machine. Next, the code opens up around four windows of Internet Explorer to download a malicious program called "WIN-BUGSFIX.exe". This program will then be moved to the local machine so it runs every time the computer is opened.

Next is to download all the computer's important files and leave corrupted files in their place. This can be done by writing a few more new functions. Onel first gets all the folders from the computer driver. After that, the files are corrupted by being overwritten with the code itself. This is done by finding files of a certain type, like .cs, .jpeg, or even .mp3, and replacing them with the code. This leaves the files unretrievable.

After corrupting everything beyond repair, the code is ready to leave the nest and infect a new host. Onel's code will find the user's contacts through the Messaging Application Program Interface (MAPI) and draft a new email with the virus bundled up in it. Onel adds a nice touch where the email is only sent once, even if there are multiple of the same contacts. After all, it's good to efficient.

**Step 5: Taste Test**

Grace Tang
Mr. Wisniewski
ENGL398C
27 March 2024

Onel leaned back in his chair and stretched, the hardest and most tedious part was over. Now, he was in the final stretch. It was time to test his virus out.

Onel decided to test his virus out with a few of his colleagues. He quickly sent them a few emails with the virus attached. He then sits at the computer, eyes staring at an empty email box. Pop. A new email arrives and Onel quickly types in the information into his laptop. After a few seconds of buffering, the computer lights up again and opens up a new internet window. He has done it, he has internet access, all without paying a single dime.

**Step 6: Enjoy!**

He's done it, by using this simple procedure and his knowledge, he found a way to bypass the unfair system and proved to his professor that he could do it… but there was still one curious little thought that gnawed in the back of his mind. In his code, he had it restricted to the city of Manila, but what if he removed that restriction? What heights could his little trojan virus reach? Absentmindedly, he removed the geo-restriction, going to bed quickly afterward.

Waking up the next day, Onel is shocked to find out that not only was he the most wanted man in the world, but his virus also corrupted government files, bank records, and hundreds of thousands of computers, leaving a trail of chaos in its wake. According to *The History and Impact of the ILOVEYOU Virus* (2023), in total, Onel Guzmen's "little" virus ended up causing over 14 billion dollars of global damage.

Grace Tang
Mr. Wisniewski
ENGL398C
27 March 2024

## References

ONX. (2021). *ILOVEYOU/LOVE-LETTER-FOR-YOU.TXT.vbs at master · onx/ILOVEYOU*. GitHub. https://github.com/onx/ILOVEYOU/blob/master/LOVE-LETTER-FOR-YOU.TXT.vbs#L100

*The History and Impact of the ILOVEYOU Virus*. (2023, February 14). Gold Sky Security. https://www.goldskysecurity.com/the-history-and-impact-of-the-iloveyou-virus/

*Top Programming Languages For Malware Analysis | Cybrary*. (n.d.). Www.cybrary.it. https://www.cybrary.it/blog/top-programming-languages-for-malware-analysis#:~:text=As%20one%20of%20the%20older