TEE

An Investigation into Virus Composition and Cyber Warfare

TEE: *An Investigation into Virus Composition and Cyber Warfare*

Thao Bach
Computer Science
Mount Holyoke College
bach22t@mtholyoke.edu

Ella Holmes
Computer Science
Mount Holyoke College
holme22e@mtholyoke.edu

Eva Snyder
Computer Science and Music
Mount Holyoke College
snyde24e@mtholyoke.edu

Abstract

Cyber warfare and increasing virus potency are ever growing international concerns, threatening the security and privacy of nations and their residents. Advancing from harmless applications to costing billions in damage, viruses have affected everything from personal laptops to high clearance goverment machines. In this paper, we analyzed one of the first powerful global viruses "ILOVEYOU," current viruses, cyber attacks, and defense mechanisms employed by hacktivist organizations such as Anonymous. To gain perspective of a virus's destructive capabilities, we created a simple program of our own.

1. Introduction: Virus Composition and Cyber Warfare

"Expect massive cyber attacks. War is declared. Get prepared." This is a direct quote from a publically released video by Anonymous[1], declaring cyberwar against ISIS[2] following the recent terrorist attacks on Paris. Cyber warfare, as defined by the Cambridge English Dictionary

[1] *Anonymous is a loosely associated group of activist hackers, or hacktivists, located all around the world. They've done operations ranging from helping flood relief to uncovering information about members of the KKK.*

[2] *Islamic State of Iraq and the Levant is a jihadist militant extremist group with members located globally.*

(Cambridge English Dictionary), is “the activity of using the internet to attack a country’s computers in order to damage things such as communication and transport systems or water and electricity supplies.” The topic has been featured in many Hollywood films commonly thought of as a futuristic concept. For example, Hollywood’s “Live Free or Die Hard” is a popular movie, grossing almost 400 million dollars at the box office in 2007, whose plot is a combination of different cyber attacks against other countries. Fast forwarding to today, cyber warfare is a colloquial conflict. Technology is moving faster than humans can keep up with, and with the development of technology comes the increased ability for information breaches, privacy invasions, and thefts on a grand scale.

Microsoft defines a virus as “small software programs that are designed to spread from one computer to another and to interfere with computer operation”. Viruses began as a simple command line interruption but quickly evolved into a much more disruptive entity. With the capabilities to steal money, passwords, and personal information, people began fearing the future of viruses. Today, powerful terrorist groups conduct most of their recruitment efforts via cyberspace and viruses quickly became the modern day assassins. Moreover, those who have the capabilities to write viruses will be in popular demand if security does not continue to improve. Viruses are not always malicious, as there are groups that are writing viruses to protect. These groups are often called hacktivists,” and they can use viruses for such activities as leaking information about KKK members or declaring a cyber war on the largest terrorist group today. This is in direct contrast to those who are using viruses for harm to shut down power, control nuclear plants, and wreak havoc among civilians.

Inspired by the hacktivist group, Anonymous, their increasing visibility in the media, and their use of hacking to target ISIS, also known as the Islamic State, we decided to pursue this project to gain a better understanding of how viruses operate, how they are used in the past and present, and how the security and protection involved in detecting and eliminating viruses. We do so by researching different types of viruses, their history, and creating our own virus.

The purpose of this paper is to provide historical context to viruses, investigate current ways to write a virus, and how viruses of today affect the globe. Specifically, we focused on how an Apple Operating System can be breached by a virus written by three Mount Holyoke women.

2. Background

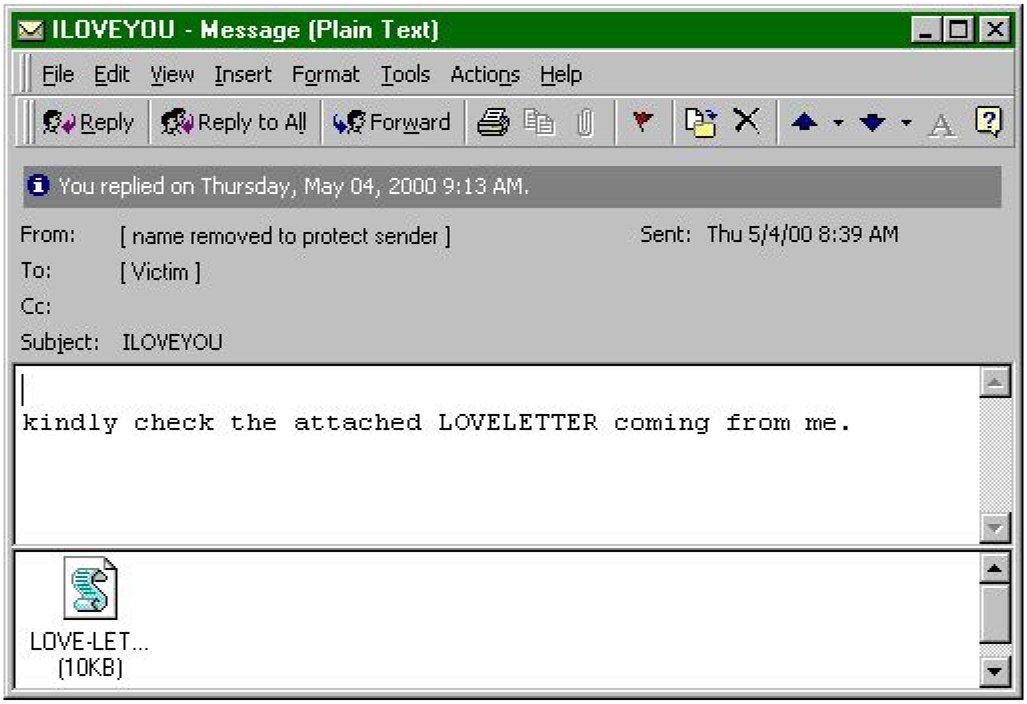
i. Relevant History

Computer virus theory was developed in 1949 by John Von Neumann, documented in the 1996 publication "Theory of Self-Reproducing Automata". Von Neumann proved mathematically that machines can reproduce other machines as long as there is enough raw material (Neumann, Burks). This exponential nature of computer reproduction is the founding principle of computer virology as many viruses today spread by recreating themselves. The first virus was created in 1959, and it was referred to as the Core Wars (History of Computer Viruses). The Core Wars was a game where each time the computer ran, a new instance of an "organism" was created, which would compromise the computer's memory. The same creators of Core Wars also invented the first instance of an antivirus. Otherwise known as the Reaper, this antivirus would destroy instances made by Core Wars. From this, many conspiracy theorists believe that malware companies also create viruses.

In the 1980's, MS-DOS was the most popular operating system globally. At this point viruses increased in numbers as they targeted MS-DOS. Hackers found ways to block users from their hard disk, and soon learned that the best way to infect a computer is to target the file system. When the internet was introduced, hackers gained a whole new playground. Hackers could now spread viruses via email and website downloads to infect computers beyond physical reach. One such virus that was the first of its magnitude is the iconic ILOVEYOU virus.

ii. Case Study : ILOVEYOU

On May 4th, 2000, an email with the subject line ILOVEYOU was first sent out in the Philippines. In this email was a short message encouraging the recipient to open the innocent seeming text file titled "LOVE-LETTER-FOR-YOU.txt".


ILOVEYOU - Message (Plain Text)
File Edit View Insert Format Tools Actions Help
Reply
Reply to All
Forward
LOVE-LET...
(10KB)

You replied on Thursday, May 04, 2000 9:13 AM.

From: [name removed to protect sender]
Sent: Thu 5/4/00 8:39 AM
To: [Victim]
Cc:
Subject: ILOVEYOU

kindly check the attached LOVELETTER coming from me.

Figure 1. Email containing the ILOVEYOU virus.

Unknown to the victim, this file actually ended in ".vbs" -Visual Basic Scripting Edition (VBS)- since most Window computers at the time hid the ".vbs" extension by default. Coupled with the social manipulation nature of the email (encouraging curiosity and the appeal of being loved), this virus led many individuals to open the attachment. Once activated, the ILOVEYOU worm would begin its wide range of attacks in the following order (Bishop):

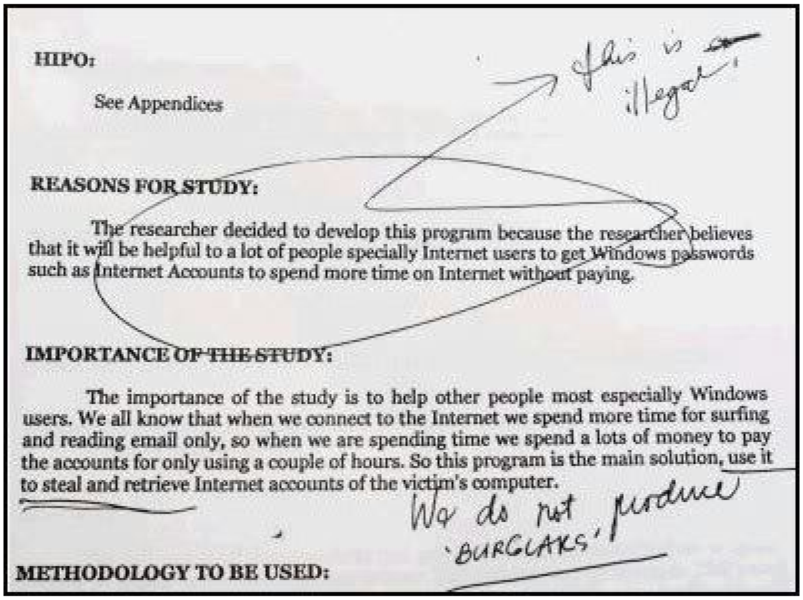
1. Create three copies of the ILOVEYOU script and add registry keys so that two of the scripts will be activated on reboot. This is to ensure that the worm can attack to any new addresses added to windows Outlook address book,
2. WIN-BUGSFIX.exe is downloaded and set to run on reboot. By the name of this file it looks like it's purpose would be to fix the bug, but actually this program searches the computer for usernames and password, and then sends them back to the creator via a website. This deceptive application is also known as a trojan.
3. ILOVEYOU then creates a web page containing the VBS source code of the virus with a wrapper. This website will eventually be sent over Internet Relay Chat (IRC) as an alternative way of spreading the worm.
4. The Virus then accesses all the email addresses that are on the Outlook application, creates a registry for each one, and then sends the same email containing "LOVE-LETTER-FOR-YOU.txt".
5. Once sent, the virus begins to do damage to the computer. On the local and remote drives the worm find all VBS, ActiveX, Java, JPG, JS,CSS DOC, HTA, ect. with copies of itself with the exception of Audio and video files which would be hidden.

6. Lastly the worm sends itself via IRC connections as an HTML file.

The virus attacked only Window machines because the virus assumed many system requirements to execute. Such assumptions were that the computer runs Outlook, Visual Basic, mIRC, Internet Explorer, supports registry keys, and that the user can write to the root and system folders. Since Macintosh computers do not support the registry concept, the ILOVEYOU virus did not contaminate Macintosh Computers.

On the morning of May 5th, ILOVEYOU spreaded to Hong Kong, Europe and lastly the United States. In the United States, the estimated cost of damage was from $5.5 to $8.7 billion dollars (Garza). In addition to the fact that 10% of all internet connected computers had the ILOVEYOU worm, similar viruses were released. Especially in large companies, servers crashed as the virus sent emails within and between companies (Ward). Anti-virus downloads were in such high demand that very few were obtained.

On this same day, Onel de Guzman and Michael Buen went into hiding after becoming the target of investigation by the Philippines National Bureau of Investigation. Guzman and Buen were both students at the AMA Computer University in the Philippines and suspected members of a secret group “GAMMERSoft,” which freelanced programming services and sold completed theses to students. Guzman had dropped out of AMA Computer University the day before graduation, after his thesis proposal, “E-mail Password Sender Trojan,” was rejected and deemed illegal (Mydans). The thesis proposed a trojan virus that could steal passwords to access the internet for free. Guzman stated that his intention was only to get free internet for an educational benefit, but investigators remained dubious after finding a floppy disk of passwords in his possession. Buen graduated after proposing a thesis about self replicating programs. In combination, their skill set amounted to the many of the characteristics in ILOVEYOU.



HIPO:

See Appendices

REASONS FOR STUDY:

The researcher decided to develop this program because the researcher believes that it will be helpful to a lot of people specially Internet users to get Windows passwords such as Internet Accounts to spend more time on Internet without paying.

this is illegal!

IMPORTANCE OF THE STUDY:

The importance of the study is to help other people most especially Windows users. We all know that when we connect to the Internet we spend more time for surfing and reading email only, so when we are spending time we spend a lots of money to pay the accounts for only using a couple of hours. So this program is the main solution, use it to steal and retrieve Internet accounts of the victim's computer.

We do not produce 'BURGLARS'

METHODOLOGY TO BE USED:

Figure 2. Guzman's rejected thesis proposal.

Although Guzman admitted that he may have released the ILOVEYOU bug by accident, charges were dropped due to lack of strong computer-crime laws (Creator of the 'Love Bug'). The result of this virus changed the perspective of how intrusive a virus can be. Spam e-mail became more common, and cyber crime ever more relevant. ILOVEYOU was the first of its kind to infect a large magnitude of computers, and it changed the virus culture from being a harmless prank to a costly crime. We originally wanted to use ILOVEYOU as an inspiration to our virus without harmful features. However, current operating systems have strong security and privacy settings to prevent even simple applications to access small features.

3. Viruses of Today

There are four prominent methods employed by viruses that have risen in 2015. One type is a ransomware trojan called “cryptolocker.” Using RSA encryption, the virus is spread via email attachments and botnets. From the perspective of the user, a cryptolocker would ask him to pay a ransom to relinquish the encryption key, and it would destroy the key, if the ransom had not been paid off in bitcoin or in cash after 96 hours (Computer Tech Tips).

The second method is breach of data at point-of-sale (POS), which has risen due to the increased transaction of online shopping. It attacks the POS terminals used by online merchants to process customer payments and steal credit card information. An example of this type of malware is “Dexter,” which was reported to have infected hundreds of POS systems across 40 countries in 2012. It works by injecting itself into the file iexplore.exe in Windows servers before hijacking process lists, staying active through rewriting in the registry key to scrape sensitive credit card data from the server, before transferring it through a remote Command and Control (C&C) system. After this, the cyber attackers would use this information to clone credit cards that have been used in the system, which could be any retailer from a store to a hotel to a restaurant (Osborne).

The third method is adware, programs that display unwanted advertisements without the user’s consent. Upon downloading the malware, it redirects search requests to advertised websites and collects data without consent about the user such as the types of websites they frequent to customized displayed advertisements. Through a USB, the virus can covertly create a backdoor to override DNS settings on an unlocked computer by mimicking a mouse or keyboard and randomly type things, flair pointer around, and weaponize mouse clicks. A typical adware looks like this (Malware-Detective.com):

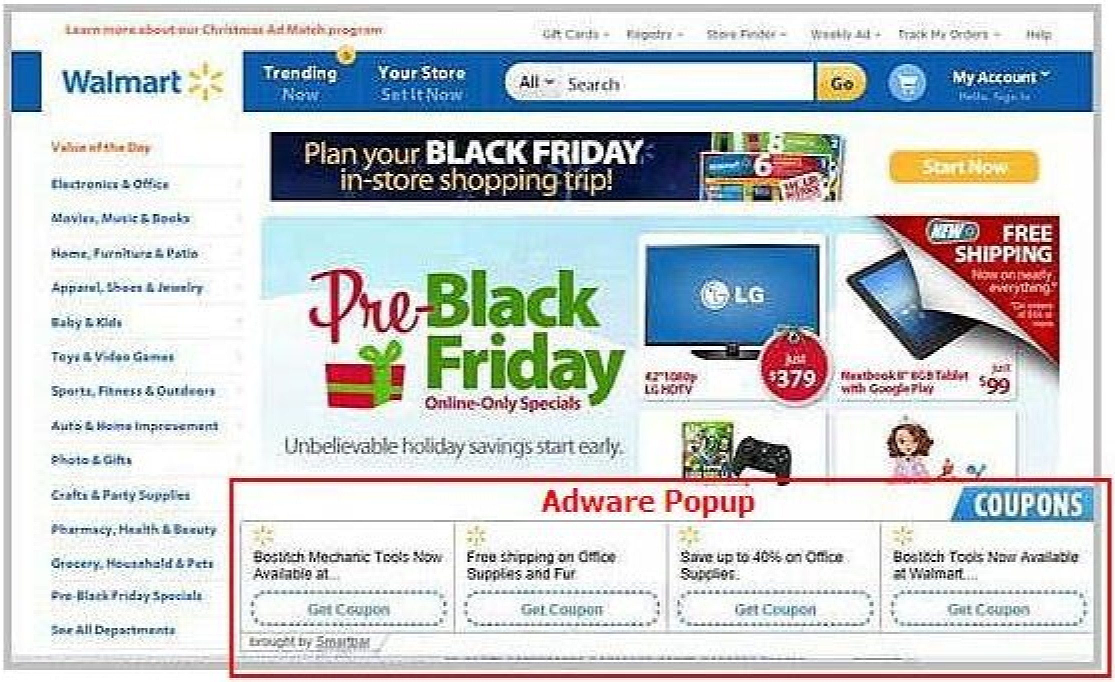


Figure 3. Adware for black friday coupons

i. How Antivirus Softwares Detect Viruses

There are two ways that antivirus software detects viruses: on-access scanning and full system scan. On-access scanning occurs when an antivirus software run in the background of the computer, checking every file upon opening to compare it to known viruses, worms, and other types of malware. It can also do heuristic checking, where the antivirus programs identify new or modified malware without virus definition files. Even though this increases chances of virus detection, it may also flag legitimate software as a virus. In addition to scanning files as they are downloaded and opened, a full system scan is used to make sure no viruses lie dormant on a computer. Most antivirus programs have a full system scan once a week, which ensures that the virus detection files are updated to detect possible dormant viruses (HTG Explains). Typically computers that are infected by a virus will have these following symptoms (Gibbs):

1. Loading time is longer for computer programs
2. Hard drive constantly runs out of free space
3. Floppy disk or hard drive runs even when not in use
4. Unrecognized files appear
5. Files with unrecognizable names appear
6. Constant change in program sizes

ii. Virtual Machines

Virtual Machines are defined as "a software program or an operating system that not only exhibits the behavior of a separate computer, but also capable of performing… like a separate computer"(Technopedia). Virtual machines are useful for running multiple operating systems on a single computer without any interruption. They are easy to manage, maintain, and offer application provisioning and disaster recovery options. Although VMs are not as efficient as a physical computer, they are cost effective solutions, if you are working on a project that is specific to an operating system you do not own. VMs are also good tools to practice virus writing. Because VMs provide access to many operating system, a hacker can learn how best to write a virus that exploits flaws in specific or many machines.

Since previous versions of operating systems have less security preferences, we explored a VM as an option to access older operating systems and write a virus that will specifically target their weaknesses. Below are the steps takes to download Virtualbox and run the RedHat operating system (The CS Help Site).

1. Download and install VirtualBox hosting envisonment for your operating system at <https://www.virtualbox.org/wiki/Downloads>
2. Download the pre-configured Cloudera virtual machine (via link provided in the tutorial) and decompress the file
3. Open VirtualBox and in the Machine menu, select "Add…" and then navigate and select "cloudera-quickstart-vm-5.4.2-0-virtualbox.vbox"
4. In the VirtualBox Manager, double click on the Cloudera VM
5. Log into the Cloudera operating system. The password and username are "cloudera"

To emulate a Microsoft or Apple operating system, VM environments can be purchased to run on VirtualBox. There are ways to download these environments free of charge but it is illegal. Because of our low budget, we could not access an earlier version of the Microsoft or Apple operating system.

iii. Basics of Computer Viruses

Most viruses are written in assembly language. They can also be written in high level languages like Basic, C, and Pascal, which are designed to generate stand-alone programs. A virus is comprised of 4 structural parts: search, copy, anti-detection, and payload.

Search is a routine that locates files or disks in a computer to target for infection (Dunning). This routine determines the rate of virus reproduction (i.e. how quickly it spreads, the extent to which it spreads).

The second routine is *copy*, a routine in which the program copies itself in the location the search routine discovers. The smaller the copy routine, the less detectable the virus is to antivirus softwares. The size of the copy routine depends on the structure of the program that is intended to be infected. For example, executable files with the ".exe" extension have a complex file structure that requires larger copy routines than other files (Dunning).

The third routine is *anti-detection*, a routine that keeps a virus from being detected by antivirus software. It does so by keeping the date on a file the same when a virus infects it. By doing so, it camouflages viruses and tricks particular anti-virus programs into thinking the viruses are not there. Additionally, it can also turn the antivirus program into a logic bomb, a malicious program that remains dormant until its intended trigger time.

Finally, *payload* is a routine that is unrelated to the reproduction of viruses, aimed at deleting data or creating annoyance. Viruses are usually classified based on the types of programs they infect and the method of infection (Dunning). There are four distinct types (VX Heavens):

- Boot sector infectors - viruses that take over when the computer is first turned on. These can be further categorized into the programs they infect: COM (i.e. DOS EXE, Windows EXE, OS/2 EXE, etc.), EXE, or SYS files.
- File infectors - viruses that infect ordinary program files on a disk
- Multi-partite - a combination of the above two
- Script - viruses written in a script language. These scripts can be hidden inside a web page, a program, or simple files.

4. Our Virus: TEE

i. Description of the Virus

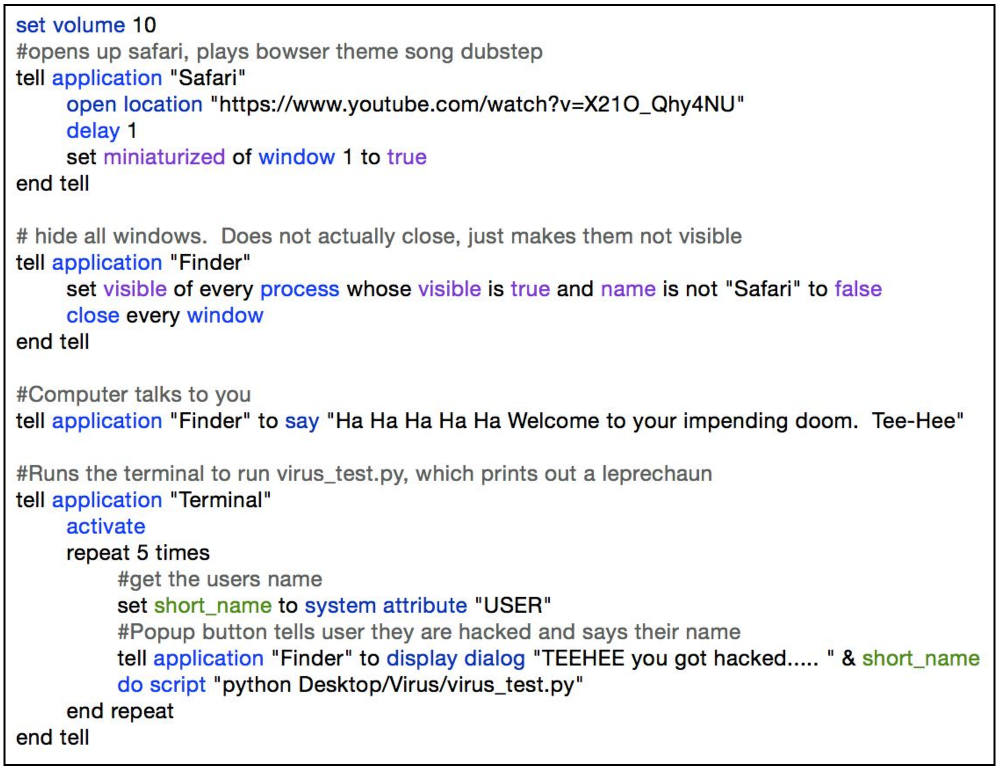
The virus we created is a simple program that explores different manipulations to various Mac applications. We used AppleScript, a scripting language written by Apple in 1993 for their System 7 operating system, to facilitate the execution of Inter-Application Communication, the act of sharing data between different processes. We decided to use AppleScript for our virus because it is powerful and easy to read.

To the right is a brief outline of the virus's actions upon execution. TEE infects a computer once downloaded from a fake website that looks identical to "Isis," Mount Holyoke College's internal site. Once logged into what looks like your normal account, you are notified that there has been a security update, and you have to download new software to protect your computer. Unknowingly, the user then downloads TEE. They are then instructed to open and install the software, and thus, executing TEE, which then briefly takes control of their computer.

1. Sets the volume of the computer to maximum level
2. Says "Ha ha ha, welcome to your impending doom. Tee-Hee"
3. Opens Safari and navigates to YouTube to play the Bowser Theme Song
4. Opens the Terminal
5. Executes a Python program downloaded with the virus which prints to the command line 5 times
6. In between printing to the terminal, makes a window pop up telling you that you've been hacked.
7. Puts the computer to sleep upon clicking "I'm Tired" in a popup window
8. Calls 617-710-0055 on Facetime

Upon taking control of the computer, TEE hides all of the windows that are open to display your desktop, simultaneously speaking in a computerized voice. Then, it secretly opens Safari to play the menacing "Bowser Theme Song" from Super Mario. While the theme song is playing, the virus executes a Python program downloaded to the computer at the time TEE was download, which prints an ASCII art of a leprechaun and the words "Top of the mornin' to ya" to the command line 5 times, each in a new terminal. In between each print, a popup appears saying you've been hacked with your name.

After this, a dialog pops up, prompting the user to choose "Yes," "No," or "I'm tired" to answer the question, "Did you have fun?" If "Yes" or "No" is chosen, the program commences to calling 617-710-0055 on Facetime. If "I'm Tired" is chosen, the computer goes to sleep. Only upon waking the computer up does the program continue to call 617-710-0055 on Facetime.



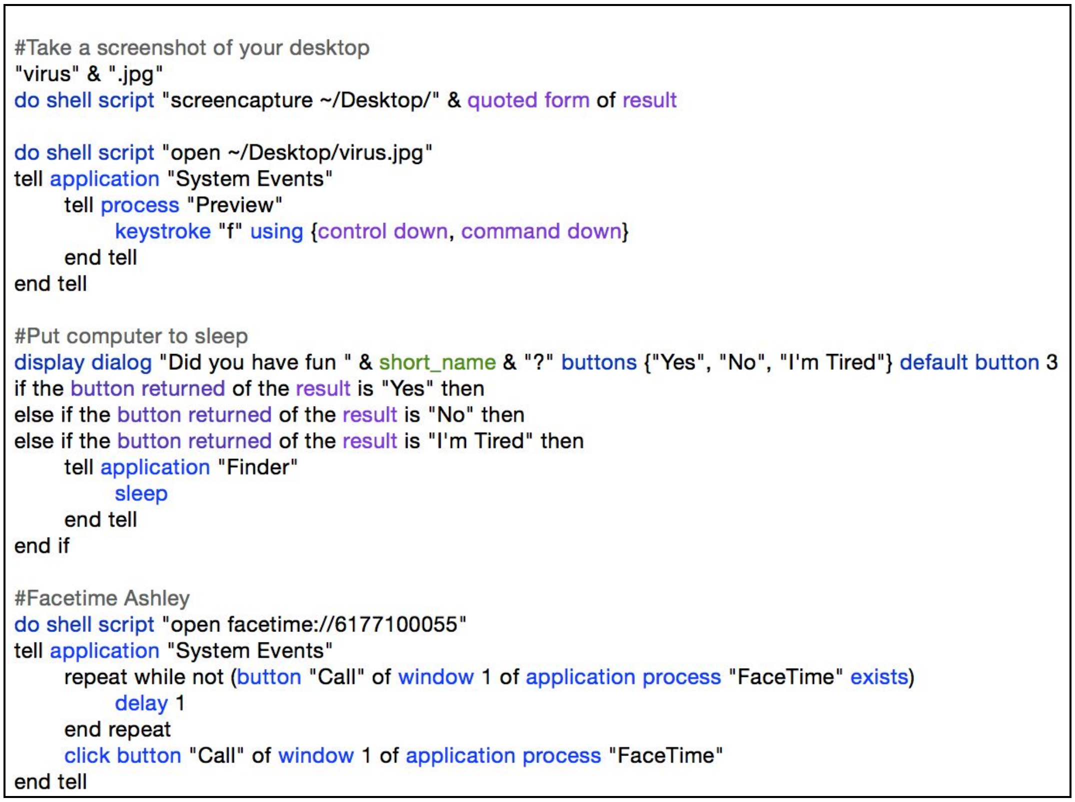
```
set volume 10
#opens up safari, plays bowser theme song dubstep
tell application "Safari"
	open location "https://www.youtube.com/watch?v=X21O_Qhy4NU"
	delay 1
	set miniaturized of window 1 to true
end tell

# hide all windows.  Does not actually close, just makes them not visible
tell application "Finder"
	set visible of every process whose visible is true and name is not "Safari" to false
	close every window
end tell

#Computer talks to you
tell application "Finder" to say "Ha Ha Ha Ha Ha Welcome to your impending doom.  Tee-Hee"

#Runs the terminal to run virus_test.py, which prints out a leprechaun
tell application "Terminal"
	activate
	repeat 5 times
		#get the users name
		set short_name to system attribute "USER"
		#Popup button tells user they are hacked and says their name
		tell application "Finder" to display dialog "TEEHEE you got hacked..... " & short_name
		do script "python Desktop/Virus/virus_test.py"
	end repeat
end tell
```

Figure 4.a: AppleScript code of TEE



```
#Take a screenshot of your desktop
"virus" & ".jpg"
do shell script "screencapture ~/Desktop/" & quoted form of result

do shell script "open ~/Desktop/virus.jpg"
tell application "System Events"
	tell process "Preview"
		keystroke "f" using {control down, command down}
	end tell
end tell

#Put computer to sleep
display dialog "Did you have fun " & short_name & "?" buttons {"Yes", "No", "I'm Tired"} default button 3
if the button returned of the result is "Yes" then
else if the button returned of the result is "No" then
else if the button returned of the result is "I'm Tired" then
	tell application "Finder"
		sleep
	end tell
end if

#Facetime Ashley
do shell script "open facetime://6177100055"
tell application "System Events"
	repeat while not (button "Call" of window 1 of application process "FaceTime" exists)
		delay 1
	end repeat
	click button "Call" of window 1 of application process "FaceTime"
end tell
```

Figure 4.b: AppleScript code of TEE

ii. How We Wrote TEE

There were two parts to writing the virus: the website and the virus program. The website was written in HTML, CSS, and JavaScript to model after Mount Holyoke's "Isis" page. Hosted on https://viruss.herokuapp.com/, the website features a login page identical to "Isis's."

To write the virus program, we referenced Apple's *Applescript Language Guide* for instructions on operators, applescript fundamentals, script objects, and commands (AppleScript Language Guide). In addition to the guide, we also looked at some sample code on Stackoverflow to familiarize ourselves with Applescript.

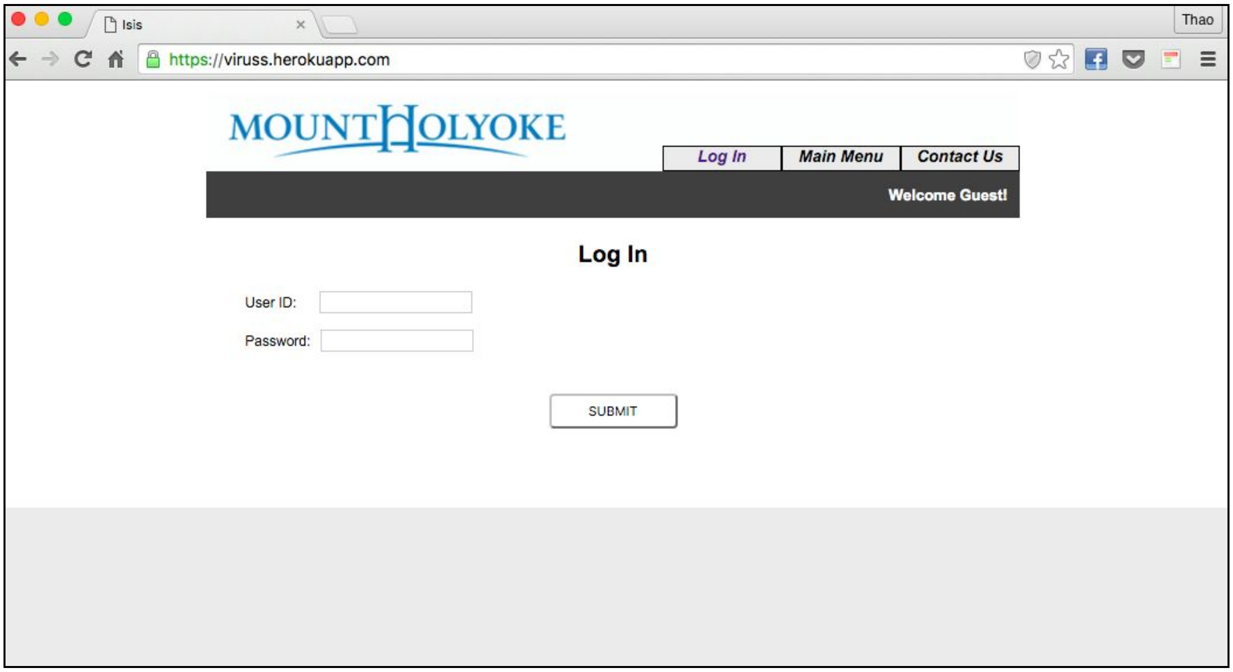
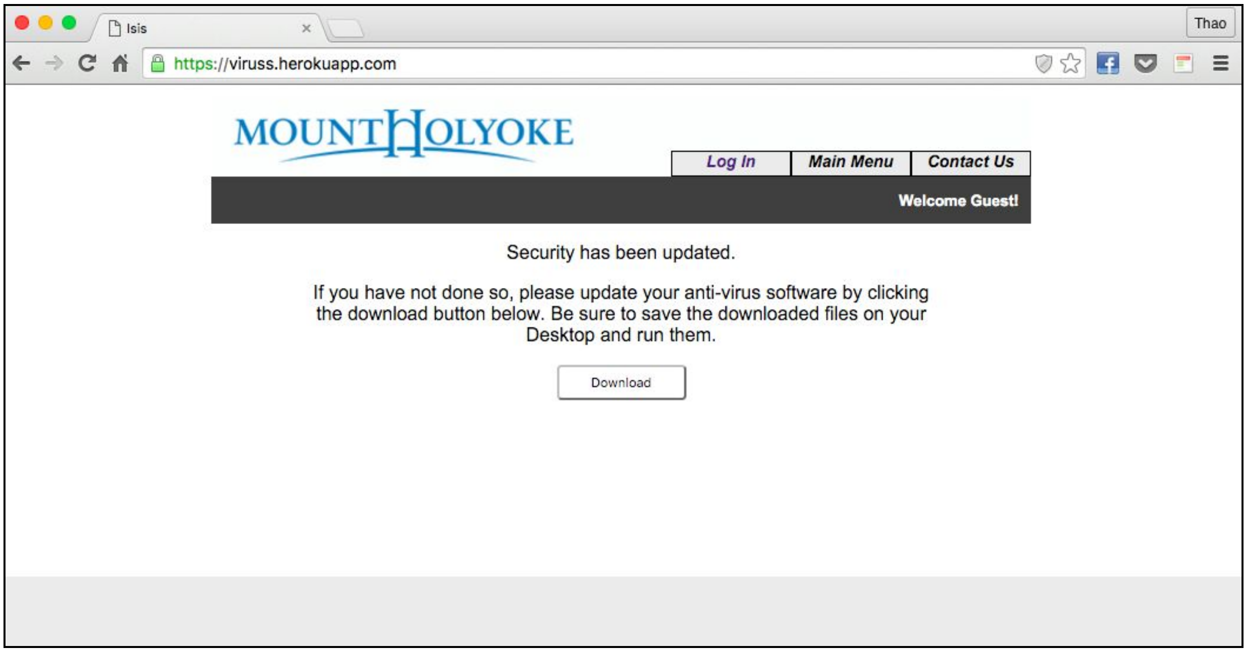


Figure 5: Screenshot of virus website's landing page

Upon clicking "Submit," the login subpage is replaced by a download page.



Security has been updated.

If you have not done so, please update your anti-virus software by clicking the download button below. Be sure to save the downloaded files on your Desktop and run them.

Figure 6: Screenshot of download page

As for designing the program, the process was straightforward. Besides determining the logical progression of actions to maximize surprise to the user, minimal design choices were discussed, mainly because our program did not demand it.

5. Anonymous: The Growth of Hacking as a form of Warfare

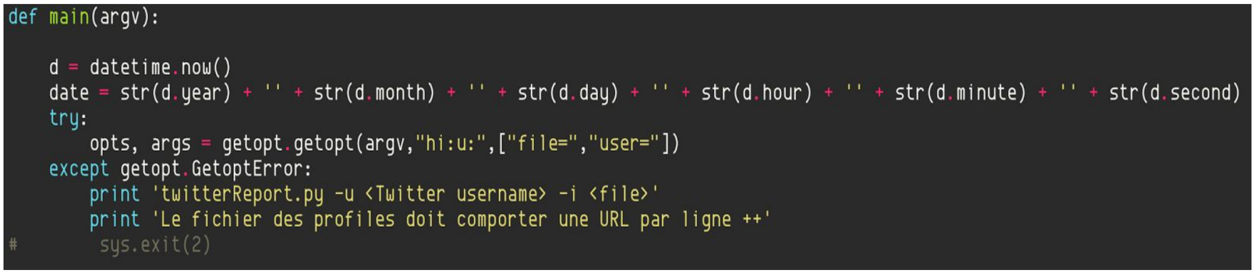
TEE might not steal personal information or disable a security system, but it's very closely related to the work of large scale hacking organizations. A leader in cyber warfare is the hacktivist group, Anonymous. The size of the group is unknown, but it's estimated to be in the thousands. Anonymous sees the power of technology and tries to use it as protection and a form of defense to help put a stop to corrupt organizations that are using technology for villainous purposes. Warfare has evolved from territorial fighting as seen in World War 2 and the Civil War to today's cross-continent drone strikes. In addition to drones evolving from the technological revolution, terrorist organizations are writing viruses and trying to hack into government controlled facilities such as the U.S Power Grid. According to Business Insider, ISIS attempted attack on the U.S power grid in October of 2015 (Bender, Business Insider). Thankfully, they were unsuccessful, but the threat of an attack is still present every day with upwards of 80 attacks in 2014 (Pagliery, CNNMoney). Throughout roughly 11 years, Anonymous has been an organized coalition that has fought in dozens of 'operations' to take a stance against many wrong-doings.

Anonymous first hit the scene in 2003 after convening on an anonymous posting platform, 4chan[3]. All members remained incognito, except for a select few whose identity has

[3] *An image-based early form of social media launched in 2003 where users could post images and respond to comments anonymously.*

been made public by spending time in jail. For all other members, you can recognize them only by their iconic Guy Fawkes masks from the popular comic, V for Vendetta. The mask first came into play in 2008 when the Church of Scientology removed videos of Tom Cruise from the video sharing platform, YouTube. Protestors were instructed to hide their face to discourage photos being taken after which the guy Fawkes mask became a symbol for the hacker organization.

Looking at Anonymous's current pattern of operations, one notices that their efforts have been largely honed in on Operation Paris, also known as #OpParis on all social media outlets. Directly following the ISIS terrorist attacks in Paris on Friday, November 13th, Anonymous declared war against the Islamic State in a YouTube video[4] that quickly went viral.



```python
def main(argv):

    d = datetime.now()
    date = str(d.year) + '' + str(d.month) + '' + str(d.day) + '' + str(d.hour) + '' + str(d.minute) + '' + str(d.second)
    try:
        opts, args = getopt.getopt(argv,"hi:u:",["file=","user="])
    except getopt.GetoptError:
        print 'twitterReport.py -u <Twitter username> -i <file>'
        print 'Le fichier des profiles doit comporter une URL par ligne ++'
#        sys.exit(2)
```

Figure 7: A snippet of Python code from Anonymous's "Twatter Report"

In this video, Anonymous says they will stop at nothing to take down the terrorist organization that uses social media and encrypted apps for most of their communication to both the outside world and members within their fighters. So far, Anonymous has managed to take down over

[4] https://www.youtube.com/watch?v=ybz59LbbACQ. *The link to the video Anonymous released a few days after the November 13th, 2015 terrorist attacks in France by the Islamic State. In this video, a member of Anonymous who speaks french declares war against the terrorist organization saying they will stop at nothing to take them down.*

5,000. Pro-Islamic State Twitter accounts and have provided toolkits and how-tos[5] for everyday computer savvy people to attempt taking down ISIS.

These how-to documents, Figure 7, consist of pre-written python code that anybody can download and then execute as well as a text document with thousands of flagged twitter accounts. The code which is then executed by any user takes in the text document and starts stepping through each twitter account. For each flagged account it looks to see if it's already been suspended or taken down completely and then if it has not, it looks through the followers recording them and adding any new ones to the list of suspicious accounts.

Anonymous is focusing on exposing Islamic State supporters to infiltrate the terrorist organization more than what one might consider to be traditional 'hacking'. However, one of the largest obstacles is ex-Anonymous member, Hussain, who taught ISIS everything he knew before he was killed in a U.S drone attack in August of 2015. Since then, every backdoor employed by Anonymous has been used by ISIS to prevent an invasion of cyber attacks.

Hacking into personal computers and retrieving confidential information, or shutting down power grids, is the future of wars around the world. Anonymous, while located around the world, use technology to unite members in times of 'combat'. This coalition of online hackers evolved from a single hacker wreaking havoc with a simple virus written in their basement. The virus written for this project is similar to the viruses most operating systems will protect against nowadays however the same concepts can be found in modern day viruses and hacks. Anonymous, for example, work on developing viruses that are secretive and undetectable as well

[5] *https://ghostbin.com/paste/jrr89. 'The Noob Guide' released by Anonymous on November 17th containing instructions for the basics on how to hack. Also released was the 'Twatter Reporter' (https://ghostbin.com/paste/vt5zz) which instructs computer savvy individuals on how to locate and then report Pro-Islamic State twitter accounts.*

as fast spreading to other similar machines.

6. Conclusion: The Future of our Virus

If we obtained older hardware, we would have added more advanced activities to our virus TEE. Windows 95 and Mac Snow Leopard were two operating systems that we attempted to use. We successfully installed VirtualBox to run the Cloudera operating system however, due to lack of budget, we could not obtain older virtual operating systems. Due to this, we decided to continue writing a virus for the current Mac operating system that we have local to our computers: Yosemite. If Mac Snow Leopard 10.6 was obtained on a computer other than our own, we would have added additional damaging programs such as deleting files off of the computer's hard drive. The operating system of Mac OS 10.6 does not protect against certain attacks, such as modifying visual displays without granting security permission and does not require permission before passing control to a foreign file.

Despite being restricted by the stiff access permissions required by Yosemite, through writing a virus of our own, we gained a better understanding of how a computer can damaged with only a few lines of code. Moving forward, we are interested in learning more about how advanced viruses are written, and additionally, writing a new virus in different languages like assembly language or C, which are capable of more dangerous activities to the computer on a lower level closer to hardware.

7. References

1. Barkham, Patrick. "Hackers Declare War on Scientologists amid Claims of Heavy-handed Cruise Control." The Guardian. N.p., 4 Feb. 2008. Web. 29 Nov. 2015.
2. Bender, Jeremy. "'They'd Love to Do Damage': The FBI Says ISIS Wants to Go after One of America's Biggest Vulnerabilities." Business Insider. Business Insider, Inc, 19 Oct. 2015. Web. 05 Dec. 2015.
3. Bishop, Matt. "Analysis of the ILOVEYOU Worm." *University of California at Davis* (2000): 12. Print.
4. Borchers, Callum. "Operation Isis: Anonymous Member Reveals How They Are Waging War on the Militant Group." The Independent. Independent Digital News and Media, 28 Nov. 2015. Web. 29 Nov. 2015.
5. "Computer Tech Tips For Everyone!" *Computer Tech Tips For Everyone*. N.p., n.d. Web. 02 Dec. 2015.
6. "Computer Viruses Explained." *Computer Viruses Explained*. N.p., n.d. Web. 28 Nov. 2015. Dunning, David. "What Are the Three Structural Parts of a Computer Virus?" *EHow*. Demand Media, n.d. Web. 27 Nov. 2015.
7. "Creator of the 'Love Bug' Finds Fame Isn't So Sweet." *WSJ*. The Wall Street Journal, 7 May 2001. Web. 3 Dec. 2015.
8. "Cyber Warfare Definition in the Cambridge English Dictionary." Cyber Warfare Definition in the Cambridge English Dictionary. N.p., n.d. Web. 06 Dec. 2015.
9. Garza, George. "Top 10 Worst Computer Viruses." *Catalogs*. Web. 2 Dec. 2015.
10. Gibbs, Beth. "Computer Viruses." *Computer Viruses*. N.p., n.d. Web. 28 Nov. 2015.
11. Hellord00t. "Building a Hack Lab For Free: Part 1. "*Http://hackmethod.com/building-hack-lab-free-part-1/*. Hacker Method, 23 Jan. 2015. Web. 23 Nov. 2015.
12. "History of Computer Viruses." *History of Computer Viruses*. AntivirusWorld. Web. 3 Dec. 2015.
13. "HTG Explains: How Antivirus Software Works." *HowTo Geek RSS*. N.p., n.d. Web. 28 Nov. 2015.
14. John Von Neumann, and Arthur W. Burks. "Theory of Self-Reproducing Automata." *Mathematics of Computation* (1966): 745. Print.
15. "Kaspersky Personal & Family Security Software." *Kaspersky Lab United States*. N.p., n.d. Web. 02 Dec. 2015.

16. Mydans, Seth. "Student Sought In Virus Case In Philippines."*The New York Times*. The New York Times, 10 May 2000. Web. 3 Dec. 2015.
17. "Naked Security." *Naked Security*. N.p., n.d. Web. 04 Dec. 2015.
18. Osborne, Charlie. "New 'Dexter' Malware Strikes Point-of-sale Systems - CNET." *CNET*. CNET, 14 Dec. 2012. Web. 04 Dec. 2015.
19. Pagliery, Jose. "Hackers Attacked the U.S. Energy Grid 79 times This Year."*CNN Money*. CNN, 29 Dec. 2014. Web. 5 Dec. 2015.
20. VX Heavens; "The Giant Black Book of Computer Viruses"; Mark Ludwig; 1995
21. Ward, Mark. "A Decade on from the ILOVEYOU Bug - BBC News." *BBC News*. 4 May 2010. Web. 2 Dec. 2015.
22. "What Is Adware? - Malware-Detective.com." *Malware Detective.com*. N.p., 22 Feb. 2014. Web. 04 Dec. 2015.
23. "What Is a Virtual Machine (VM)? - Definition from Techopedia." *Techopedias*. Web. 4 Dec. 2015.
24. "AppleScript Language Guide." *Introduction to*. N.p., n.d. Web. 06 Dec. 2015.