Issues in Informing Science and Information Technology Volume 8, 2011

Tracking Viral Contamination through User Habits and IT Practices

Martiniano Jake Parawan Neri III
CUREXO-IDS,
Capitol University
Cagayan de Oro City, Philippines

docachmed@gmail.com

Adrian Cabangal Ranido
College of Computer Studies,
Capitol University
Cagayan de Oro City, Philippines

aranido@yahoo.com

Abstract

This study looks into the attributes of common viral infections, how these viral transmissions happen and its effects on Personal Computer systems in an academic environment and working atmosphere. Both student and staff respondents were asked about their experiences with computer viruses, along with their localized and internet-related activities that they do in a routine format. Data were also extracted from a storage scanning module designed for this study over a definite period of eighteen (18) days. This module contained anti-virus scanning software that was updated daily to capture definitions that identify and quarantine malicious codes and programs stored in drives from the respondents. Complimentary data from person's in-charge of the IT support teams assigned to heavy computer-related usage were also used to validate machine breakdowns arising from viral activities. Findings were collated and used as a basis for a policy framework designed to address the transmission of infection in a broader scope. The policies generated were then distributed to IT-related businesses (Internet/Surfing and LAN gaming cafes) in Cagayan de Oro City, which were then subjected to another study on the effect of contamination on users outside the academic environment as reminders and cues prior to computer use.

Keywords: Computer Virus, System Contamination, Viral Behavior, Policy and Framework

Introduction

In health-related sciences, it is a precautionary measure to protect oneself from infection through sustained good personal hygiene. Furthermore, infected individuals are advised to exercise other countermeasures as preventive action, not to contaminate others on existing circumstances (Jadad & O'Grady, 2008). An individual may opt to stay well and fit by doing appropriate healthy activities. The bodily defense mechanism may provide protection against certain diseases, especially those that occur in a passing manner. Resistance to diseases does not, however, guarantee protection on induced infections (HIV or AIDS). Misconceptions or inadequate knowledge of the disease itself contribute to multiplying incidences and prevalence of this (Health Promotion Board, 2008). On the other hand, extinction of a known fatal disease is possible like through breakthroughs of immunity shots, such as the case of smallpox (Pütz, Alberini, Midgley, Manini, Montomoli, & Smith, 2005) and polio. Indeed, some diseases at present times are preventable.

In the world of Information Technology, the same principle revolves around the vital existence of industry-class operating systems. With the advent of ease-of-use systems, as well as graphic user interface (GUI) functionality, robust systems are designed to address accidental misuse (deletion of system data from system folder), but have a minimal effect on the emerging threat of viral infections. To date, hundreds of thousands of known attacks have been noted and documented, and are evolving each day to challenge the systems design and exploit holes for inappropriate advantage. Countermeasures are passive in nature; they are designed after the attack has been detected (Zakorzhevsky, 2009). Malware cure and removal methods vary directly with the allotted financial aspects attached to the systems they are designed for. In a recent issue, PC magazine (Reubenking, 2010) published the top performing security suites with updated available information on performance and capabilities. Performances of these security suites ranges from malware control, phishing detection, parental control, identity theft recovery, spam filters, robust firewalls, to name a few. Free security modules provide minimal protection, prompting users to purchase an upgrade or premium edition (Bradbury, 2009). Even with paid modules or security suites, protection is still not fully secured as viruses evolve and mutate through time, and vendors would usually advise registered users to update the anti-virus signature database.

Focal Point on Viral Infections in Computers

The term “virus” in the field of Information Technology was first conceptualized by Hungarian-American mathematician, John von Neuman, in 1949, when he proposed the possibility of a computer program that can replicate itself in a confined scenario. A year later, the same idea was tested at the Bell Laboratories when a game called “Core Wars” was developed. The winning scenario of the game is demonstrated by the destruction of an opponent’s system, when players command the circumstance to create ‘tiny programs’ designed to attack, erase and propagate in a system under siege. A large scale, single game event was dragging since the computer had to deal with simultaneous multiple programs in a certain period of time, wherein very minimal action is visible in the process.

The term “virus” was attributed to Fred Cohen, a graduate student back in the year 1983 while he was describing a self-replicating computer program. Two years later, Trojan Horses (from the Greek story ‘the Homer’s Odyssey’, representing the wooden horse strategy used to successfully invade Troy) appeared, posing entrance to computer systems as a graphic enhancing program known as EGABTR, as well as a game called NUKE-LA. The success of these attacks led to an onslaught on new strains that increase the complexity of its variants with the same objective: malicious intent to jeopardize a system (Herrmann, 2002).

Viruses in Action: A World-wide Phenomenon

There are numerous ways to quantify the damaging effects of noted viral activity. Loss of productive time can be calculated using the following definition:

Let X = hourly rate of an employee
Y = repair cost

Suppose a person can finish encoding a magazine in 8 hours of productive time, the company will pay him 8X. Now, if another employee is experiencing, say a WinWorm incident (see first bullet on the following page), the time it takes him to finish the same magazine is 16. Therefore, on the same hourly rate, the same output is produced with a much larger labor cost (16X). Further down, the management takes notice of the incident, and takes the computer for repair for an indefinite number of days. No work then is done without the computer, and add to that the expense of fixing the computer, the cost now is $(8X * \infty) + Y$.

Sometimes, work lost due to viral damage is unquantifiable, especially in incidences that require deadlines. To illustrate, a book writer is on the verge of finishing a 700-page book. Working on this project, he did not employ a backup system. His only file is in his computer. During his idle time, he decided to open his e-mail, and got carried away when he spotted a subject of him winning a million dollars in an unidentified lottery. Seconds after he thought he was claiming something he did not even have any inkling about as directed by the e-mail, he got a surprise. A macro-script for his word processing software took effect, infecting all of his .doc files, including his book draft. With no recovery options and no backup storage, it is then impossible to quantify a time-span of hard work lost in a mere moment of viral attack.

To initially present the destructive effects of viruses, the following samples are presented:

- **First Macro Virus -** The 1990's started a new trend in viral activity as computer nuisances grew in sophistication and effect. In the middle of the decade (1995), the first macro virus came to surface. Known as WinWorm Concept, it exploited 3 holes in Microsoft's basic word processor. Infection starts at contamination, wherein the virus is loaded into action when a document is loaded into the program (hole 1). It then infects the word processing scenario by copying its macros into the pre-loaded global macros environment, effectively positioning itself as a resident virus. The second hole is exploited each time a user creates a new document and upon saving, the new document becomes a carrier. When the word processing software exits, the virus automatically saves any changes in its global environment, thus infecting future documents made by the word processing software. Viral macros are usually resident on universal documents and will remain active in future sessions unless cleaned. Its destructive effects include the popping of a prompt box with the text "1" and the ok button every 2 minutes. Users cannot work efficiently on typing documents since the virus always intercepts encoding activities during the prompt.
- **First Bootstrap Virus** - In 1986, a virus known as Brain appeared and by 1987, it circulated worldwide through its distinct effect on systems. It had the impression of a life form, as it evolved into the first bootstrap virus known as the Stone, and its kin, the Internet Worm, crossed the US continent overnight through the computer networks that businesses infrastructures stand on.
- **First Fast-Infector** - The phenomenal Dark Avenger posed as the first fast-infector of 1989, paving an effective evolution of the first polymorphic virus of 1990.
- **Most Prolific Virus -** The year 1995 marked the entry of the first macro language virus, WinWord Concept. It stalled productivity with annoying prompts that disturbed document processing users. In 1999, the Melissa macro virus propagated by spreading into e-mail systems. Its payload disabled e-mail servers it encountered around the world, some for several hours, others several days. During that time, it earned the title of the most prolific virus ever. It cost business corporations that relied on email as a communication medium millions of dollars due to computer downtime and lost productivity.
- **Highest Financial Damage** - The VBS_LOVELETTER script virus, also known as the Love Bug and the ILOVEYOU virus, placed the Philippines in the map of viral notoriety. Designed by students to test a script, it unseated Melissa as the world's most prevalent and costly virus when it struck in May 2000. The test went haywire and spread like wildfire with computers as combustible agents. Financial losses were estimated at USD 10 billion when the contamination was brought down to manageable levels. The Love Bug is said to have transpired an infection rate of 20% in all the PCs worldwide.

- **Operating System Exploit**-Three years after the Love Bug, a much celebrated incident of viral infamy took place. First, the Blaster Worm emerged and infected more than 10 million computers worldwide by exploiting a common flaw: machines that have the Microsoft's Windows Operating System (OS). Simply said, this flaw exploited as it bypassed security measure in a simple circumstance where mere connection to the internet provided the connection to a heavily-contaminated network. MS security engineers scampered to provide a patch for the security hole for free in a fortnight manner.
- **Network Virus** - Later on in the same year, the SoBig worm infected millions more in a worldwide phenomenon. Its payload was designed to transform systems into network relay nodes capable of creating and sending massive amounts of junk e-mail. These unsolicited e-mails were later referred to as "SPAM". SoBig's favorite transmission is via e-mail. A few hours after its conception, SoBig was reported by an e-mail filtering company with more than a million SPAM messages and it earned the title of the first fastest-spreading virus in history. By 2004, however, the MyDoom virus unseated SoBig, spreading even faster, and by most accounts, causing even more technical and financial harm than the latter.

Work Plan

The first phase of the data gathering procedure was to exactly locate a time frame that can be replicated in terms of the degree of computer use. This phase covered 18 days in the determination of sufficient data necessary for the formulation of a digital contamination epidemic.

Figure 1 shows the components of the observable clusters grouped according to how the computers are used inside the institution. These groups include laboratories, internet use, special purpose use, and general clerical use. From these clusters, we gathered information regarding how the transmission of viruses takes place and what observable consequences are seen in the system, using data from 2 sources: a) questionnaire and b) interview transcripts.

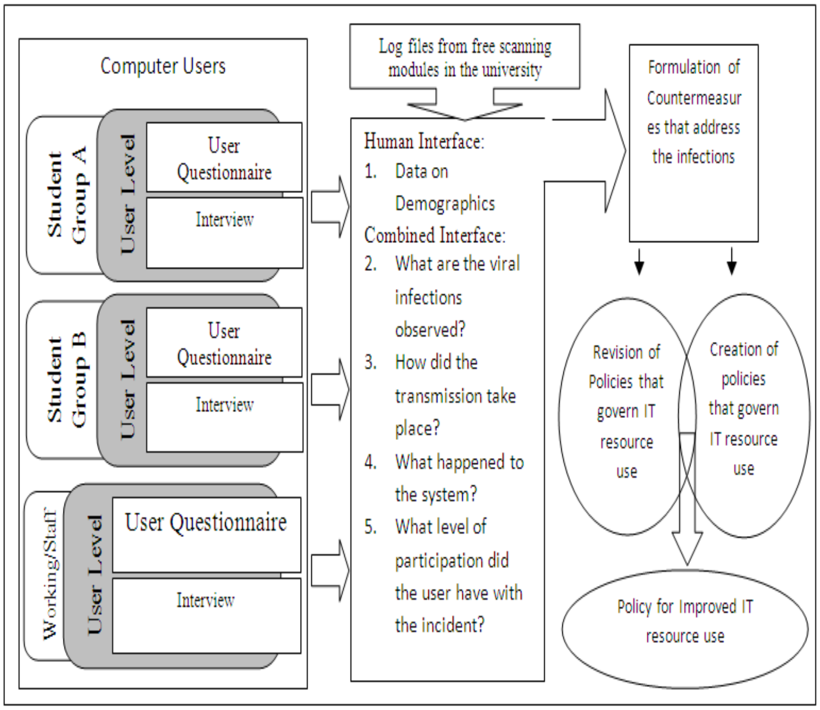

Computer Users
Student Group A
User Level
User Questionnaire
Interview
Student Group B
User Level
User Questionnaire
Interview
Working/Staff
User Level
User Questionnaire
Interview
Log files from free scanning modules in the university
Human Interface:
1. Data on Demographics
Combined Interface:
2. What are the viral infections observed?
3. How did the transmission take place?
4. What happened to the system?
5. What level of participation did the user have with the incident?
Formulation of Countermeasures that address the infections
Revision of Policies that govern IT resource use
Creation of policies that govern IT resource use
Policy for Improved IT resource use

Figure 1: How infection works and formulation of countermeasures and policy generation

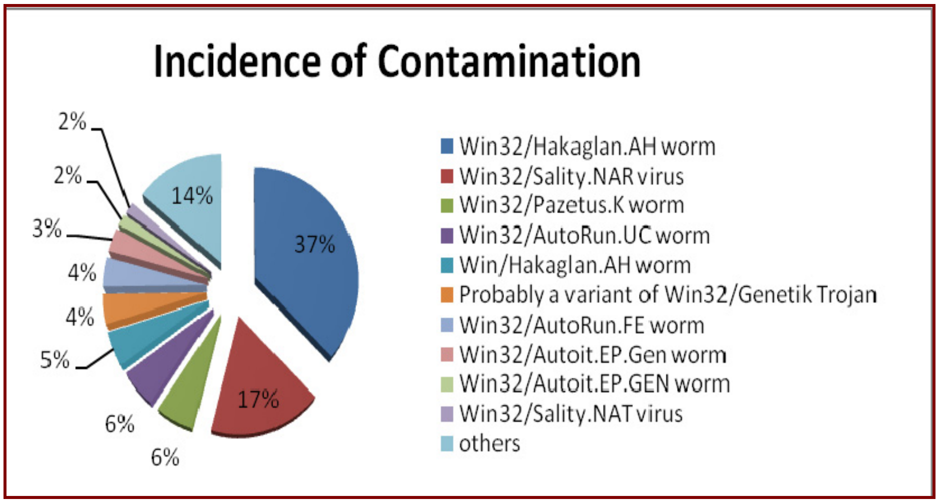
Standard countermeasures (update of AV modules, information drive, used education from stud findings, etc) were then applied to address the problems from these infection activities. These countermeasures will serve as the framework for the revision of existing policies as well as the creation of new IT policies which will be tested in the 2nd phase of the study.

Findings

The following findings were derived from the first step of the data-gathering activities ofthis research. The respondents were tallied at 2,500 entries, broken down into 2,000 respondents for regular random participation, 250 respondents for those individuals with at least a built-in computer subject for the current semester, and 250 respondents for individuals doing routine work with computers. These findings also generated information gleaned from the scanning modules part of the research plan.

Common viral infections

A total of 2,268 infections were detected over the span of 18 days during the monitoring procedure. Of the 2,268 detected, there were only 103 strains of viral incidences observed. The top ten infections are as shown in Figure 2 with their corresponding counts:



1.	Win32/Hakaglan.AH worm	(842)
2.	Win32/Sality.NAR virus	(389)
3.	Win32/Pazetus.K worm	(131)
4.	Win32/AutoRun.UC worm	(126)
5.	Win/Hakaglan.AH worm	(112)
6.	A variant Genetik Trojan	(96)
7.	Win32/AutoRun.FE worm	(95)
8.	Win32/Autoit.EP.Gen worm	(76)
9.	Win32/Autoit.EP.GEN worm	(38)
10.	Win32/Sality.NAT virus	(38)
11.	Others	(325)

Figure 2: Virus/Infection identities with summary of incidence

User profile

The research classified the user into two groups, namely: 1.) Regular students' enrolled, and 2.) staff/working individuals. Majority indicated daily computer use. Student users spend around 1-4 hours a day. Majority of the working population surveyed spent around 2-8 hours or more a day. Figure 3 summarizes the daily average use of both respondent groups in a graph.

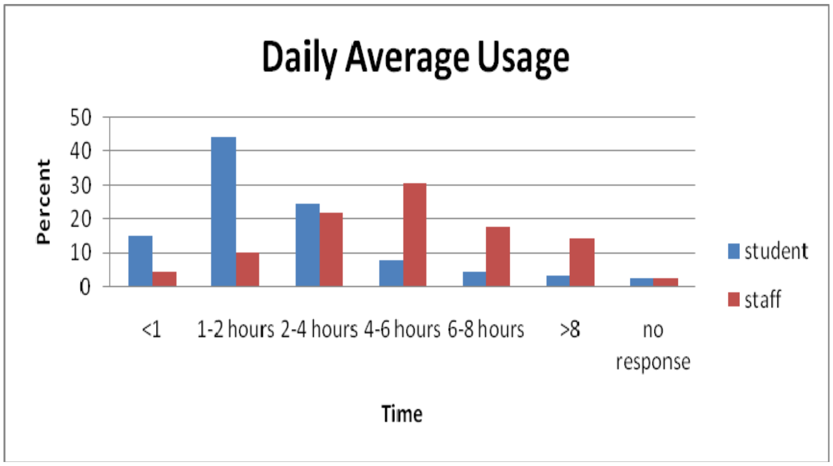


Figure 3: Daily usage

Drive contents

The major reasons for computer use are net surfing, communication and file storage. Most of the students indicated access of computer services at school, while for the working population, at work. Around three quarters of both groups have a flash disk. Inside these drives, we usually find productivity documents, images and music files. Figure 4 indicates the usual contents (in file types) of the respondents in their storage devices.

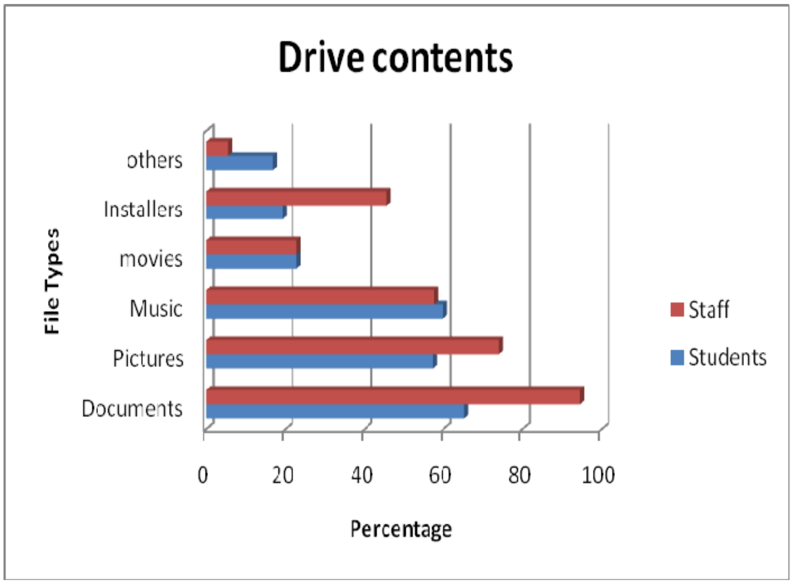


Figure 4: Drive Contents

Anti-Virus software usage

More than half of those surveyed have an idea about anti-virus (AV) programs, and used them. Students have more access to updating the features of these AV programs, less than half of the working group indicated the same access. Both groups surveyed indicated high awareness (>75%) of computer virus incidences and update operating system files for security reasons. Around 2/3 of the surveyed perform drive scans before using the drives; although only a third know about auto-run programs attached to the drives. Students prefer the following AV programs in order of preference: AVG, Avira and Norton. The staff/working surveyed indicated the same.

Almost 90% of the staff had an actual experience with viruses in their computers, only 2/3 of the students experienced the same. The usual effects of these viruses are the following: very slow loading time, slow browsing and shuts down unexpectedly, and these incidences sum up to more than half of the experiences. In Figure 5, the graph shows the Anti-Virus brand preferences of the respondents.

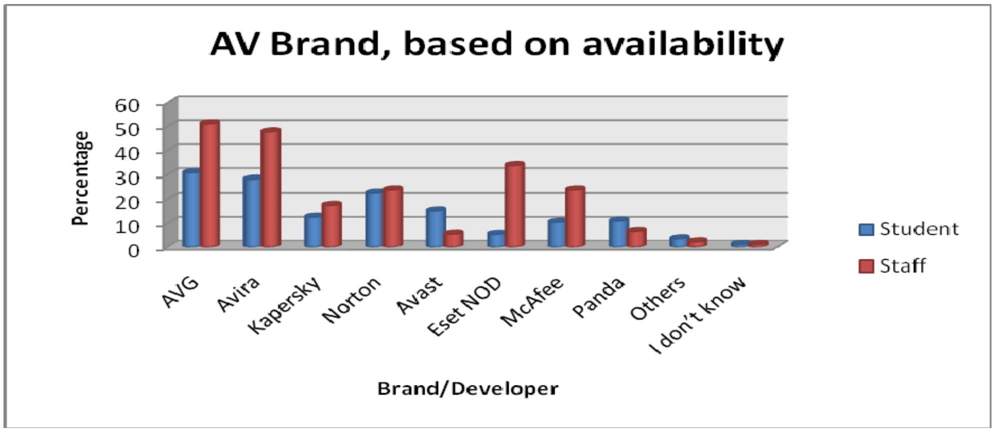


Figure 5: Anti-virus software usage

Common transmission methods

In Figure 6, the graph shows that majority of those who responded to the survey indicated ownership of a digital media drive with a capacity of 2 gigabyte (GB) or more. These drives are usually for the storage of digital files that serve different purposes according to user preference. A portion also of the respondents also pointed out that this transmission medium could be the cause of their infections because of its ease of use. They indicated that these devices are conveniently used whenever they have some files to copy from any computing station.

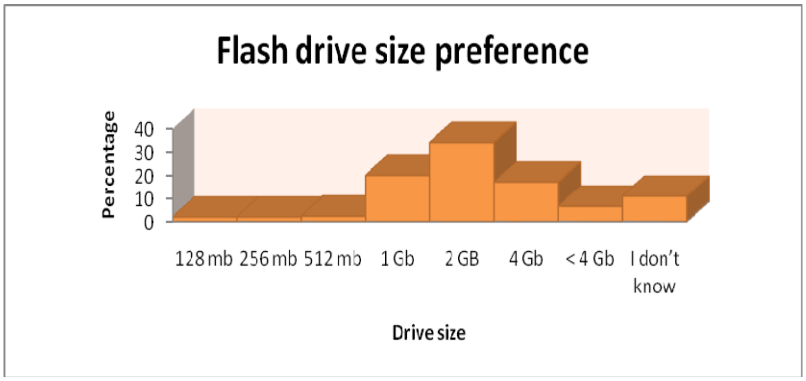


Figure 6: User drive ownership size of preference

Effects of contamination

Unusual computer behavior was noted as the primary effect of the infection. In some cases, the respondents never had an idea of what transpired. It was only on the virus-scanning module that they learned that their current mobile disk drive is carrying a virus that infected each host station it was plugged into. In severe cases, a large portion of the respondents indicated that the home page of their browser takes them to a pornographic (e.g. redtube) website without their permission. Time-triggered events such as unusual shutdowns and restarts are noted during prompts of operating system and virus updates. Other instances reported include the mass-broadcast of foreign-sounding messages on installed chat/messaging clients to all registered recipients with a link at the end. Clicking the link will contaminate the recipient of the message with the same virus. The most damaging effect observed is the deletion of system files of the operating system, which leads to total computer breakdown. The user usually takes out the computer for repair, and the usual recommendation from the service provider is the reformat of the hard disk, which destroys both the virus and essential files not backed up by the user. Some respondents reported the presence of garbled data, in what used to be folders they created for a specific file. The virus changes the file type and makes the file inaccessible by its default program. Images are no longer viewable, and productivity documents are no longer editable. Figure 7 summarizes the perceived effects of viral infections as indicated by the respondents.

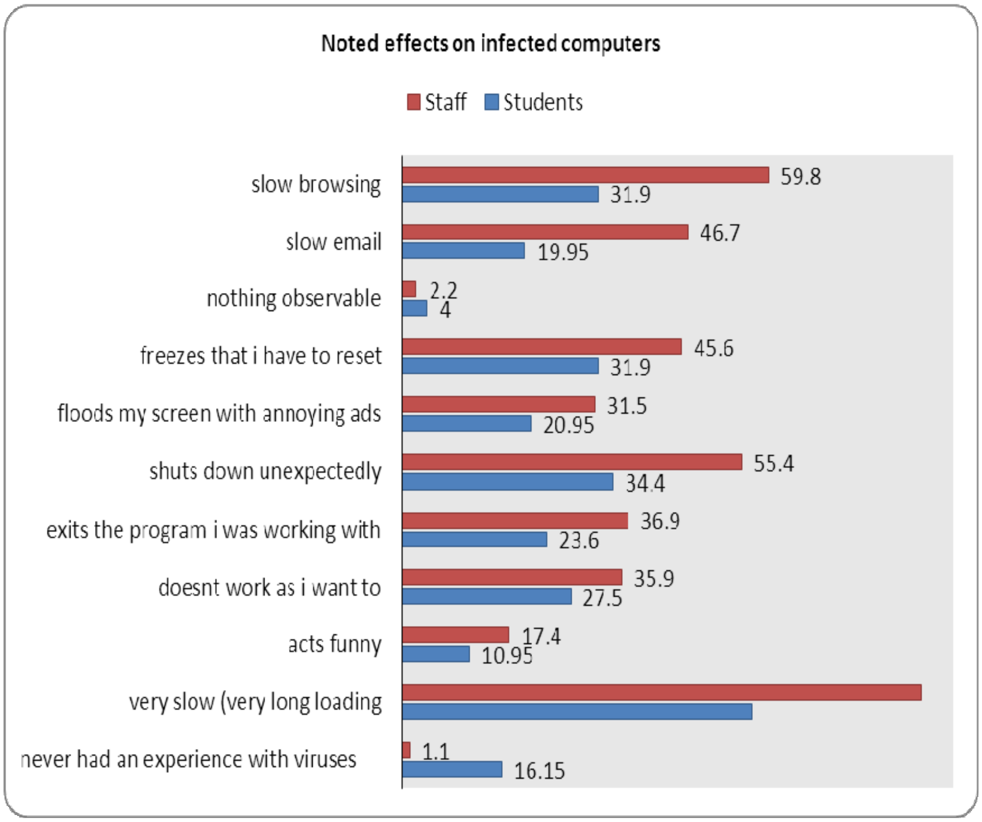


Figure 7: Effects of viral infection

Extent of user's knowledge related to viral contamination

Users subjected to the survey indicated a reasonable degree of understanding of viral infections in their workstations. However, they would consider their workstations as 'safe' with the installation of anti-virus software. It should be noted that this is not sufficient since the installation is easily outdated over a short period of time. However, they also have very limited knowledge on how to disable auto-run function, where the infection automatically performs the contamination without user intervention. Table 1 summarizes user knowledge about anti-virus programs and their active roles to protect the system they work with.

Table 1: Summary of user knowledge about anti-virus programs

	Students	Staff
Knowledge about AV programs	60%	85%
Uses an AV software	53%	80%
Updates AV programs	49%	69%
Knowledge about Computer viruses	77%	89%
Updates computer (security)	56%	71%
Scan drives before use	62%	77%
Knowledge about auto-run features	31%	49%
Virus experience	62%	88%

Staff interview

From the data generated above from this study, a questionnaire guide was created to summarize the findings. This guide then is used in an interview and was reconfirmed of what persons/students in-charge and assistants observe during computer breakdowns suspected due to viral infections. Most of those who assist users with flash drives plug their devices into the workstation without scanning. While these users are allowed to use their drives for mobile storage, they become either external carriers (contamination comes from sources other than those from the university workstations) or active carriers (they transmit the contamination they got from the infected workstations during their use).

A remarkable development in containing the contamination process is the installation of a program which allows system administrators to protect the core operating system and configuration files on a workstation or server by restoring a computer back to its original configuration each time the computer restarts. This has its own setbacks for both users and administrators, as additional program installation after the fresh-booted state is removed after restart. Infections that happen before the locked state will be permanently recurring, and updates to certain core files and AV's from security breaches are not properly applied as it 'no longer sees' added files after the restart is applied.

Conclusions and Recommendations

1. The digital structures of how the top ten viruses listed above replicate indicate that they attach themselves to flash drives from contaminated systems. Since the replication behavior does not require user intervention, it is highly essential that current PC users are informed of how the auto-run feature works, how to view the corresponding file and how to disable the feature. With this knowledge, users may then be aware of how user intervention prevents further contamination.

2. Majority of the flash disk users indicate ownership of more than 2 gigabyte (size) of disk space available for use. While excess space is actually good for emergency need, some drive owners carry around non-essential files because the user forgot what files were stored in the disk. Multiple file contents in the flash disk increase the range of damage a certain virus can inflict. Replicator worms scan for files and create executable files from the number of folders they see. This takes more time for scanning modules to complete the task because of the replicated folder and files in the disk. Other than that, installer files are also designed to use up minimal file space by being compressed using an external program. When a specific virus finds its way into this compressed form, this can result to a severe threat to core files as scanning modules usually bypass the installation file

types, or those compressed for this purpose. With this, it is recommended that users be advised to purchase flash drives according to use, not according to size. This will prevent users from keeping a large chunk of space in their flash drives that are not used according to purpose. It is also advised to get installation files from verified sources.

3. Computer usage time is not a factor in the contamination process. Users may take hours to finish an activity that concerns the use of a computer; it only takes a few seconds for a virus from a flash drive to transfer to the host system. Therefore, it is also recommended that all flash disk users be informed that prior to use, their drives need to be scanned with the most updated anti-virus programs, both to protect the system they're going to use and to clean the files that has been infected prior hand.
4. Further study on the development of a non-Operating System dependent AV program is also recommended. These can be in form of checking beforehand actual file/files size as considered secure, and a systematic confirmation of the same value when re-activated on another computer. Differences in the values could indicate that a digital infection has occurred.
5. A strong information campaign on the benefits and its associated responsibilities when handling thumb/flash drives. It should highlight the need to be vigilant against common transmission methods, as well as the risks in plug-and-play functionality that viruses exploit to ride on.
6. It is very notable that staff respondents exercise more caution in the protection of their files against students. It is therefore recommended to increase the awareness level of students by integrating simple concepts viral transmission, effects and preventive actions in subjects that talk about community extension. In the Philippines, the National Service Training Program (NSTP) or the Civic Welfare Training Service (CWTS) or any social graces courses can use the output of this study to inform and educate IT service users.
7. An information campaign should extend also beyond the academe as where this research first took place. These should include LAN café's and internet café's that offer IT-related services to computer users. Simple information drive can use the following:
    a. Modest stickers that can be attached to flash/thumb drives as a reminder to users.
    b. Keychain accessories
    c. Bookmarks
    d. Sticker/information paraphernalia attached to IT related service providers
    e. Information seminar/drive/campaign during enrolment, etc.
8. System behavior is notable on infected computers. At first instance of security breach, users should be advised to seek professional IT help in controlling the infection and prevent replication when the virus starts to use mobile drives as the medium to transport themselves and contaminate other systems. It is also recommended that they perform regular updates on the installed AV programs in their computers.
9. For systems with core system files protection, it is recommended that users be advised or informed about how this protection systems work. Disappointments on losing a downloaded file from the internet after restart are a common problem with those individuals who invested time to acquire the said file. It is should also be noted that such protection is not real-time. Virus contamination can happen (infect and transmit) during the time a computer is subjected to an attack. Restarting the computer cleanses the host system, but

not the flash drive. It was not part of the drive sets protected by this product during the installation process.

Local Implementation as an Extension Service

The findings of this study are initially disseminated in the academic community to help strengthen the policy recommendations presented, especially from the prospective of the laboratory administrators. They were the source of firsthand information from which their daily task is to keep IT services systems in pristine condition to cater to its users. The existing policies from which this study intends to improve is then subjected to the same findings and from its derived recommendations, it is then reformulated to cater to the developments of the viral study.

It is also the intention of the research proponents to immediately disseminate the said findings, along with the recommendations, to the IT community in Cagayan de Oro City, Philippines, as part of the University's thrust and involvement of the institution not only in the development of the academic resources, but also as a community member in improving the current state of living in the city.

References

Bradbury, D. (2009, May 8). Comparison of free anti-virus software with paid-for products. *Computer Weekly*. Retrieved November 18, 2009, from: http://www.computerweekly.com/Articles/2009/05/08/235952/comparison-of-free-anti-virus-software-with-paid-for.htm

Health Promotion Board. (2008). *AIDS: Myths and misconceptions*. Singaporean Government. Retrieved November 15, 2009, from: http://hpb.gov.sg/sexualhealth/article.aspx?id=6260

Herrmann, D. S. (2002). *Security engineering and information assurance*. New York Auerbach Publications.

Jadad, A. R., & O'Grady, L. (2008). *How should health be defined?* Retrieved November 18, 2009, from http://www.bmj.com/cgi/content/full/337/dec10_1/a2900

Reubenking, N. J..(February 2010). *The AV challenge*. Retrieved March 24, 2011, from 2010 Security Suites: Best and Worst: http://www.pcmag.com/article2/0,2817,2351871,00.asp

Pütz, M. M., Alberini, I., Midgley, C. M., Manini, I., Montomoli, E., & Smith, G. L. (2005). Prevalence of antibodies to Vaccinia virus after smallpox vaccination in Italy. *Journal of General Virology, 86*(Pt 11), 2955-2960.

Slade, R. (2006). *Dictionary of information security*. Syngress. pp. Front. ISBN 1597491152.

Zakorzhevsky, V. (2009, November 13). *Rogue viruses: A growing problem.* Retrieved November 18, 2009, from http://www.viruslist.com/en/analysis?pubid=204792090

Biographies

Jake Neri spends most of his time behind his newfound passion-amateur photography. He focuses on subjects ranging from landscape photography to ultra-wide perspective imaging. He is considering ways to adapt this passion as a productive tool for research… along with partnerships and research collaborations in Educational Technologies and IT in Education. He is looking for venues to enrich his appreciation for the SCORM platforms, bridging teaching methodologies and methods with how Information Technology evolves through this generation

He breeds exotic Siamese cats for friends and interested individuals. He runs to keep fit, looks forward to fun runs and cause-related run activities. He also juggles research outputs from the College of Education and the College of Computer Studies.

Mr. **Adrian Ranido** is a multi-tier Computer Science / Information Technology Professor at Capitol University. His research interests include Human-Computer Interaction, Systems Analysis & Design and Information Management. His current affiliations include the Philippine Society of Information Technology Educators. He was once affiliated with NCR, a Research and Development Company, in Cebu City, Philippines. He was sent for further training to Atlanta, Georgia, USA for the upgrade of skills in fastlane support training.

His main research goal is to provide student a background on Human and Computer Interaction for better IT solutions. He plays basketball twice a week to balance work and play. He's also an avid collector of beer labels.