RUNNING HEAD: Viruses

Viruses on Computer Systems

Aidan Hopper

ID: 42236214

CS 312

Dr. Donald Davendra

I pledge that this submission is solely my work, and that I have neither given,

nor received help from anyone.

**Abstract**

Viruses are a type of malware that infect executable files on a system. Much of the time they are spread using a worm, a type of malware that spreads through networks. Two notable examples of this are the “ILOVEYOU” virus and the Melissa virus. All viruses contain the same basic functionality. These are called the search routine and copy routine. Both these routines define what a virus is at a basic level. There are also optional aspects, these are the anti-detection routines and the payload. The anti-detection routine is a set of routines the virus will utilize to avoid detection from anti-virus software, and the payload is the function the virus is intended to perform. Viruses also all have a similar life cycle, with the first one being the optional dormant phase, where a virus will sit idle until a specified event occurs. The next phase is the propagation phase, where the virus will infect other files on the system using the search and copy routines. Next is the trigger phase, where some event occurs and which triggers the payload phase where the virus performs its set function.

Table of Contents

[Abstract 2](#1%19Abstract%19C)

[Introduction 4](#1%19Introduction%19C)

[What is a Computer Virus? 4](#1%19What_is_a_Computer_Virus?%19C)

[ILOVEYOU 4](#1%19ILOVEYOU%19C)

[ILOVEYOU Creation 5](#1%19ILOVEYOU_Creation%19C)

[Melissa Virus 6](#1%19Melissa_Virus%19C)

[Important Aspects of a Virus 7](#1%19Important_Aspects_of_a_Virus%19C)

[Computer Virus Life Cycle 8](#1%19Computer_Virus_Life_Cycle%19C)

[Conclusion 8](#1%19Conclusion%19C)

[References 9](#1%19References%19C)

**Introduction**

Malware on computer systems comes in many forms. There are Viruses, Spyware, Adware, Trojan horses, Rootkits, Key-loggers, and more. They all have one thing in common, they are intended to maliciously affect a computer at the expense of the user. This paper will discuss virus malware specifically, examining its inner workings, uses, virus examples, and a virus life cycle.

**What is a Computer Virus?**

The first question that is raised when discussing viruses is what are computer viruses? Specifically, what actions do viruses perform, and how do malicious attackers use them? The word virus originates from its real-life counterpart the virus, which infects the cells of a host to make copies of itself (*Virus*, n.d.). This parallels the computer virus which is an infectious block of code, which attaches itself to a program. When this program is executed, the malicious code is executed, which is used to spread itself to other programs.

When thinking of malware, think of the name virus as an aspect of malware, because a single piece of malware can contain multiple aspects. For example, viruses can be also worms, which copy themselves automatically through networks i.e., email, chat programs, etc. to spread themselves.

**ILOVEYOU**

One famous virus that made the news in 2000 was the “ILOVEYOU” computer virus, which caused the government to strengthen its infrastructure. The “ILOVEYOU” virus was also classified as a worm. Worms replicate on networks, attaching to files and searching for ways to access other computers on the network. The “ILOVEYOU” virus came in the form of an email, with a script attached (United States. General Accounting Office & Rhodes, 2000). The script was in the form of a Visual Basic Script, and as long as the recipient of the email did not run the script, the recipient was safe. If the recipient did run the script, then the system would be affected. This represents one limitation of viruses, in which they need to be attached to an executable file, and the victim needs to execute the file. Other types of malware such as the Trojan Horse do not need to be executed as a program, because the Trojan works by binding itself to non-executable files like image files, taking advantage of a vulnerability in the way the image is interpreted by the image viewing program in this example. When infected with the “ILOVEYOU” virus, the virus will send copies of itself out through email and send messages through online chat programs perpetrating further through the network. The virus would also steal passwords on internet explorer.

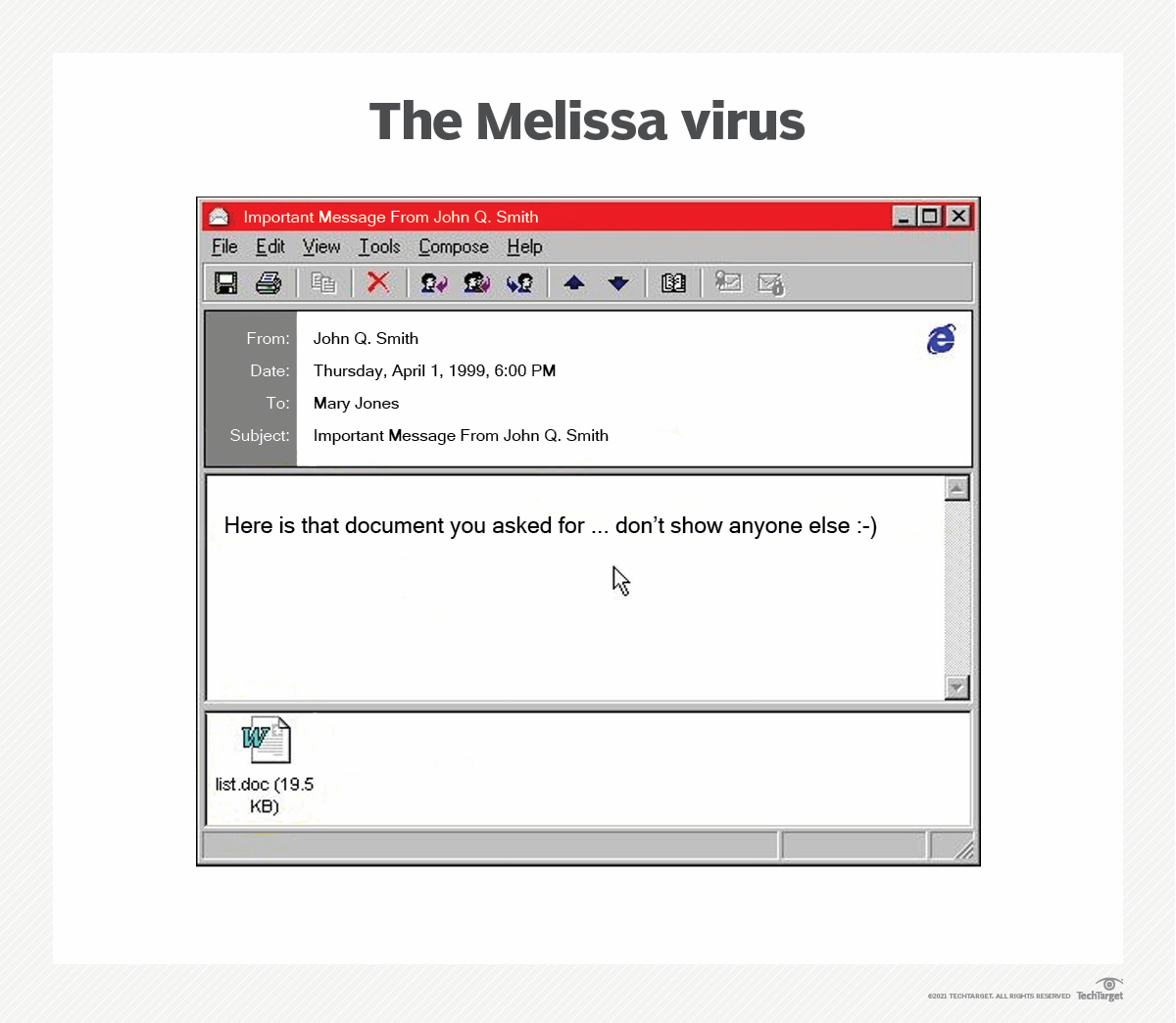
**ILOVEYOU Creation**

The “ILOVEYOU” virus was created by a 24-year-old student in the Philippines. The virus was used to steal passwords so the creator could use paid services that they could not use at the time due to monetary issues. The virus was originally limited to the city of Manilla but eventually was allowed to spread unrestricted. The creator did not expect “ILOVEYOU” to spread worldwide (White, 2020).

“ILOVEYOU” had a huge impact on the world, being the world’s biggest and most damaging computer virus outbreak at the time. It is estimated that 10% of the entire internet of computers were infected by the virus. The virus also had massive economic consequences, with an estimated total cost of $10 billion to remove or replace all infected files. The reason the virus was able to spread so quickly to so much of the internet is that users were complacent about its threat (Winder, 2021).

**Melissa Virus**

The “ILOVEYOU” virus was not a new development, because it closely resembled a previous virus outbreak that had happened in the previous year (Knight, 2000). The Melissa virus targeted Microsoft-based systems and networked itself through email, similar to the “ILOVEYOU” virus. The email would read “Important Message From [Senders name]” and attached was a document called list.doc, which contained a visual basic script and was disguised as a password dump. When executed and the system would be infected and the virus would propagate itself by emailing the first 50 names in outlooks address book. Even though the virus was not meant to steal passwords, it greatly damaged high-profile networks in the US government (Gillis, 2021).

Figure 1: Melissa Virus Email

Source: Gillis, 2021

Figure 1 showcases how the Melissa virus email was formatted. The Melissa virus is very similar to the “ILOVEYOU” virus that would originate a year later.

**Important Aspects of a Virus**

Every good virus has a few crucial aspects, the first being a search routine. A search routine is an algorithm implemented in the viruses code which searches for new files to infect on the disk, which will determine where and how quickly the virus spreads throughout the disk, and if it can spread to multiple disks. The search routine is a balancing act between the size in bytes and effectiveness. An effective search routine will make a virus spread faster but will make the virus easier to identify due to an increase in size (Ludwig, 1998).

A virus must also contain a copy routine, which copies itself to the files the search routine finds. The copy routine only has a singular purpose, so it is optimized for size, the smaller the better. The types of files the virus infects will play a significant role in the size of the copy routine. This is because some types of files are more structurally complicated than others, i.e., EXE and COM files. EXE files are more complicated because they contain data structures for the operating system to interpret. This means that a virus would have more work to do to copy itself to a COM file than to an EXE file (Ludwig, 1998), therefore causing EXE infection support to be much more complicated than COM infection support.

Viruses can also include anti-detection routines, which are protocols ranging from complex to simple that attempt to hide the virus from antivirus programs. Search and copy routines can be designed around an anti-detection which can limit the scope of both. One such way an anti-detection routine could be implemented is by not changing the last modified date on the file on infection (Ludwig, 1998).

A can also contain routines unrelated to infection and propagation. These are the most malicious aspects of the virus, and perform the action the virus was created to do. This is referred to as the payload (Stallings & Brown, 2011). It can steal account information and other sensitive information. A virus could also be made to do damage to the system by deleting files.

**Computer Virus Life Cycle**

A virus will typically go through four phases during its lifetime after its first infection. First is the dormant phase where the virus will sit idle until some event like a signal or date. Not all viruses have this phase. The next phase is the propagation phase, where the virus will propagate itself throughout the system into files compatible with the copy routine. When this phase is finished the virus will have copies of itself all over the infected system. Not all versions of the virus will be identical which is one of a virus’s anti-detection strategies. The next phase is the triggering phase. When a specified event occurs in the system, the virus will activate to perform some intended function. The final phase is where the function is performed (Stallings & Brown, 2011).

**Conclusion**

Viruses are a type of malware that infects executable files on a system. When infected the virus will use a search algorithm to search for new files to be infected, then copy itself into those files. Viruses are very prolific in the computer world, having created billions of dollars in damage for world governments. This has caused the world to be far more cautious with the links they click and programs they download with the fear of getting infected with a computer virus.

**References**

Gillis, A. S. (2021, December 7). *Melissa virus*. SearchSecurity. https://www.techtarget.com/searchsecurity/definition/Melissa-virus

Knight, P. (2000). ILOVEYOU: Viruses, Paranoia, and the Environment of Risk. *The Sociological Review*, *48*(2\_suppl), 17–30. https://doi.org/10.1111/j.1467-954x.2000.tb03518.x

Ludwig, M. A. (1998). *The Giant Black Book of Computer Viruses* (2nd ed.). Amer Eagle Pubns Inc.

Stallings, W., & Brown, L. (2011). *Computer Security: Principles and Practice (2nd Edition) (Stallings)* (2nd ed.). Pearson.

United States. General Accounting Office, & Rhodes. (2000). *Information security : “ILOVEYOU” Computer virus emphasizes critical need for agency and governmentwide improvements : statement of Keith A. Rhodes, Director, Office of Computer and Information Technology Assessment, Accounting and Information Management Division, before the Subcommittee on Technology, Committee on Science, House of Representatives* [E-book]. Washington, D.C. : The Office.

*Virus*. (n.d.). Genome.Gov. https://www.genome.gov/genetics-glossary/Virus

White, G. (2020, September 12). *The 20-Year Hunt for the Man Behind the Love Bug Virus*. Wired. https://www.wired.com/story/the-20-year-hunt-for-the-man-behind-the-love-bug-virus/

Winder, D. (2021, June 30). *This 20-Year-Old Virus Infected 50 Million Windows Computers In 10 Days: Why The ILOVEYOU Pandemic Matters In 2020*. Forbes. https://www.forbes.com/sites/daveywinder/2020/05/04/this-20-year-old-virus-infected-50-million-windows-computers-in-10-days-why-the-iloveyou-pandemic-matters-in-2020/?sh=71ae0e5a3c7c