Computer viruses and threats.

Virus Alert!

Warning! Threat detected!

A malicious item has been detected!

By: Medetov Timur,

- **What is a Computer Virus and methods of spreading them.**
- A computer virus is a malicious program that self-replicates by copying itself to another program. In other words, the computer virus spreads by itself into other executable code or documents. The purpose of creating a computer virus is to infect vulnerable systems, gain admin control and steal user sensitive data. Hackers design computer viruses with malicious intent and prey on online users by tricking them.
- One of the ideal methods by which viruses spread is through emails – opening the attachment in the email, visiting an infected website, clicking on an executable file, or viewing an infected advertisement can cause the virus to spread to your system. Besides that, infections also spread while connecting with already infected removable storage devices, such as USB drives.
- It is quite easy and simple for the viruses to sneak into a computer by dodging the defense systems. A successful breach can cause serious issues for the user such as infecting other resources or system software, modifying or deleting key functions or applications and copy/delete or encrypt data.

- There are two types of ways in viruses operate, as soon as they land on a new device they begin replicating, while the second type plays dead until a particular trigger makes the malicious code to be executed. Thereby, it is highly important to stay protected by installing a robust antivirus program.
- Presently, the sophisticated ones come with evasion capabilities that help in bypassing antivirus software and other advanced levels of defenses. Subsequently, the polymorphic malware development in the recent times enables the viruses to dynamically change its code as it spreads. This has made the virus detection and identification very challenging.

- **The History of Computer Virus**
- Robert Thomas, an engineer at BBN Technologies developed the first known computer virus in the year 1971. The first virus was christened as the "Creeper" virus, and the experimental program carried out by Thomas infected mainframes on ARPANET. The teletype message displayed on the screens read, "I'm the creeper: Catch me if you can."
- But the original wild computer virus, probably the first one to be tracked down in the history of computer viruses was "Elk Cloner." The Elk Cloner infected Apple II operating systems through floppy disks. The message displayed on infected Apple Computers was a humorous one. The virus was developed by Richard Skrenta, a teenager in the year 1982. Even though the computer viruses were designed as a prank, it also enlightened how a malicious program could be installed in a computer's memory and stop users from removing the program.
- It was Fred Cohen, who coined the term "computer virus" and it was after a year in 1983. The term came into being when he attempted to write an academic paper titled "Computer Viruses – Theory and Experiments" detailing about the malicious programs in his work.

5 of the Most Famous Computer Viruses and Their Terrible Impact

- ## 1. The Morris Worm

Let’s start with one of the most important examples of malware. The Morris Worm was the first malicious program covered by mainstream media due to its mass repercussions.

- On November 2, 1988, the worm was released and within 24 hours, an estimated 10 percent of computers connected to the internet were affected. The malware slowed down thousands of systems by creating files in temporary folders in an effort to replicate itself.
- These PCs were rendered useless (within 90 minutes of infection) until the software was removed. This took around two days to do. It naturally took even longer to expunge it from an entire network. The University of California, Berkeley, for instance, estimated that it took 20 working days to completely get rid of the worm from its computers.
- However, it wasn’t meant to be malicious. Robert Tappan Morris had created the program as a way of testing the size of the internet. It was a coding error that was estimated to have cost up to $53,000 per institution—at least according to the judge in the case against Morris. One estimate places the total cost of the worm at between $250,000 and $96 million.
- Morris, now one of the world’s most famous hackers , was the first to be found guilty under the 1986 Computer Fraud and Abuse Act.

2. Melissa Virus

- From the prophetic Curious George and the Ebola Virus to our adoption of the term “frogurt”, The Simpsons has influenced a great deal of society. Perhaps the most surprising is the Melissa virus, inspired by a 1990 episode of the show… and a stripper working in Miami.
- Let’s rewind. Infected Word documents were nothing new.
- Although rumor had it that the first “wild” macro virus to affect Word could be contracted via email, this wasn’t true. The Concept virus was instead spread, accidentally, by professional firms. Microsoft itself was partly responsible when it shipped Windows 95 Software Compatability Test CD-ROMs containing the virus.
- But Concept acted as a forerunner to the Melissa virus. A Word file was uploaded to the Usenet discussion group, alt.sex in March 1999. This contained a list of passwords for 80 porn websites, so you can imagine how many downloaded it. Once they did so, it automatically forwarded onto the first 50 contacts in the Microsoft Outlook address book.
- It then sent on other Word files, meaning personal details could’ve been sent to family, friends, and colleagues. This cost an estimated $80 million in damages to private, and corporate networks.
- One quirk was in corrupting files with the phrase, “22, plus triple-word-score, plus 50 points for using all my letters. Game’s over. I’m outta here.” This comes from Bart the Genius, in which Bart cheats at Scrabble with Kwyjibo, meaning “a big, dumb, balding North American ape, with no chin and a short temper”.
- The Melissa virus was named after a stripper its creator, David L Smith had met in Florida. Smith, who served 20 months of his 10-year sentence, didn’t do it for any financial gain. Still, he subsequently aided the FBI in catching hackers, for which his rent, insurance, and utilities were paid for…

3. ILOVEYOU

- Three words everyone wants to hear—but not in this form.
- This took a similar approach to the Melissa virus, yet was far more devastating. It was a worm spread via an email with the subject line "ILOVEYOU". It came with the attachment, "LOVE-LETTER-FOR-YOU.txt.vbs". Once opened, it would send itself to everyone in the Outlook address book, making this one of the fastest-spreading viruses at the time.
- It was said to have reached over 50 million users within 10 days.
- Far more troubling was its capacity to overwrite files. If you didn't have back-ups (and comparatively few personal networks did), you would have to kiss goodbye to your JPEGs and audio files. Further file types that were overwritten include CSS, HTA, and JSE.
- What's more, it vacuumed up private information, notably passwords, from the internet.
- After some companies became wise to this subject line, hackers introduced variants reading "Mother's Day Order Confirmation", "Joke", and "VIRUS ALERT!!!", the latter supposedly from Symantec.
- In May 2000, just a few hours after it originated in the Philippines, a number of places were forced offline to protect themselves from further damage. These included the Pentagon, and the Ford Motor Company.
- It's estimated to have cost $15 billion for firms across America to expunge the worm.

4. MyDoom

- Here it is: the fastest-spreading email worm ever.
- This exceeded the impact of ILOVEYOU and has yet to be surpassed. Fingers crossed it never will be. Because MyDoom and variations of it have caused an estimated $38.5 billion in damages worldwide.
- The worm acts on a similar principle as ILOVEYOU: an email—with misleading subjects like “Mail Delivery System”—includes an attachment which, once opened, sends itself to addresses found in local files. Whereas previous worms targeted a limited number of contacts, MyDoom wasn’t picky.
- It attempted to go under the radar by not targeting addresses of governmental agencies and security firms. MyDoom could further stop a device from running updates to security software!
- The most concerning part of the virus was its ability to open a back-door vulnerability in systems for hackers to exploit. Some of these back-doors remain open.
- It caused chaos online: the initial strain began **distributed denial of service (DDoS)** attacks on mainstream sites, like the SCO Group and Microsoft. Subsequent iterations affected Google and other search engines when an influx of requests from corrupted PCs attempted to crash servers.
- Part of its impact stems from its longevity. MyDoom was first spotted in January 2004, but deviations have resurfaced across many years since. This included the July 2009 cyberattacks which hit infrastructure in America and South Korea.
- Its creators have never been found, which seems strange considering its prolificacy. MyDoom’s point of origin was Russia. A clue might come from the message within the worm: “andy; I’m just doing my job, nothing personal, sorry”.

5. WannaCry

- Cast your minds back to May 2017 and you'll recall a lot of panic about WannaCry. There was fair reason for it. Despite only lasting a few days, the ransomware spread across between 200,000 and 300,000 computers worldwide.
- It was particularly cruel: using a back-door exploitation in Microsoft Windows, it would encrypt all data on the device and hold your files to ransom. It would apparently cost up to $600 (using Bitcoin) to decrypt the information, although even paying the fee wouldn't save your PC in reality. Nonetheless, some users paid, however futile the effort. Cybercriminals received payments of over $130,600.
- Once infected, a computer's screen locks, showing a red warning and two countdowns, one until the ransom demand would rise and the other until files would be permanently deleted.
- Fortunately, Microsoft acted quickly by issuing updates to combat the threat.
- One of the biggest victims was the National Health Service (NHS) in the UK. Many medical institutions run older operating systems, (OS) including Windows XP.

- **How To Get Rid Of Computer Virus**
- Never the neglect to take action on a computer virus residing in your system. There are chances that you might end up losing important files, programs, and folders. In some cases, the virus damages the system hardware too. Thereby, it becomes mandatory to have an effective anti-virus software installed on your computer to steer clear of all such threats.
- **Signs of Virus Infection**
- It is vital for any computer user to be aware of these warning signs –
- • Slower system performance
  • Pop-ups bombarding the screen
  • Programs running on their own
  • Files multiplying/duplicating on their own
  • New files or programs in the computer
  • Files, folders or programs getting deleted or corrupted
  • The sound of a hard drive
- If you come across any of these above-mentioned signs then there are chances that your computer is infected by a virus or malware. Not to delay, immediately stop all the commands and download an antivirus software. If you are unsure what to do, get the assistance of an authorized computer personnel. If you are confident enough, start investigating on your own by following the below mentioned step-by-step procedures.

What Can We Learn From Computer Viruses?

- It’s true that we should always learn from the past. What can we learn from these security threats?
- The first is certainly to install solid security software. That’s your first line of defence. You should also create a back-up of all your files—and, most importantly, unplug that backup once finished protect yourself from ransomware.
- You need to stay skeptical as so many worms are spread via email. Even with people you know. Don’t download anything unless you’re absolutely sure what it is and who sent it!