❖ MALWARES ATTACKED ON COMPUTER & NETWORKS

Malware Name	Which Type Of Malware	Details	Country Name	Financial Loss
MyDoom	Worm	**MyDoom** is the most damaging computer virus ever. The virus was first unearthed on 26th January 2004. It was designed to target Microsoft Windows Operating System and caused $38 billion in damages, which makes it the most expensive computer virus ever. The virus was so deadly that upon infecting a machine it created network openings which allowed the hacker to control the computer. It is estimated that about 25% of all emails sent in the year 2004 were infected with MyDoom.	North America	$38 billion
SoBig	Worm/Torjan	This virus was released in a series of editions starting January 2003. The various editions included **SoBig.A, SoBig.B, SoBig.C, SoBig.D, SoBig.E and SoBig.F**. Among all these variants the most widespread worm was SoBig.F which was released in August 2003. The SoBig.F variant was both a worm and a Trojan i.e. it could self-replicate and masquerade itself as something other than malware. The virus caused $37 Billion in damages and spread through spam emails.	_	$37 billion

Sasser/Netsky	Internet worm	Sasser and Netsky were two of the deadliest computer worms in history, and they share an author: German teenager Sven Jaschan. Sasser proliferated by scanning IP addresses on connected computers and directing them to download a virus, whereas Netsky spread through malicious emails. Combined, the worms created a devastating $31 billion of damage in the early 2000s, according to security software firm Norton.	Germany	$31 billion
StormWorm	Phishing backdoor & Trojan horse	The name StormWorm is something of a misnomer—the malware is actually a trojan horse, which is deceptive software that allows criminals to obtain access to sensitive data and spy on you. The malicious file preyed on curious email users, who clicked on a link that purported to be an article about a massive storm devastating Europe.	Europe & United States	$10 billion
NotPetya/ExPetr	Ransomware	NotPetya first poked its head up in Ukraine in 2017, but its damage wasn't limited to that country. It soon began infecting the computer systems of several multinational corporations, including Merck, FedEx, and the shipping giant Maersk. Intelligence agencies in the U.S. and U.K. have suggested that-	Ukraine	$10 billion

		the Russian military created the malware in order to damage Ukraine’s enemies, although the consequences were much more far-reaching.		
Conficker	Botnet	The Conficker worm wove its way into millions of computers, made them part of a botnet, which then could have stolen the information of millions of users, but...the vast network of bots did nothing. It just sat in the computers seemingly waiting to be activated. Curiously, the worm made it impossible for computers to contact third-party security sites like Symantec and MacAfee, and disabled Windows security systems, so the operating system couldn’t update itself to remove the virus.	-	$9.1 billion
WannaCry	Ransomware	The WannaCry ransomware left a path of destruction that affected roughly 150 countries around the globe. The malware even found its way onto hospital IT systems, where in many cases it put vital equipment out of service. Oddly, its creators asked Britain’s National Health Service for a minuscule $300 ransom to unlock its computers; that’s pretty small for an attack that cost about $4 billion in total financial losses.	-	$4 billion

Code Red	Computer worm	One of the most well-known viruses to date is the Code Red virus. It caused more than $2 billion in damages in 2001 and had the ability to break into computer networks and exploit weaknesses in Microsoft software. Once the virus infected a machine, it actively looked for other machines on the network to attack.	China	$2 billion
Slammer	Sql worm	The SQL slammer worm is a computer virus (technically, a computer worm) that caused a denial of service on some Internet hosts and dramatically slowed down general Internet traffic, starting at 05:30 UTC on January 25, 2003. It spread rapidly, infecting most of its 75,000 victims within 10 minutes. Although titled "SQL slammer worm", the program did not use the SQL language; it exploited two buffer overflow bugs in Microsoft's flagship SQL Server database product. Other names include W32.SQLExp.Worm, DDOS.SQLP1434.A, the Sapphire Worm, SQL_HEL, and W32/SQLSlammer.	-	$1.2 billion

CovidLock	Ransomware	This type of ransomware infects victims via **malicious files** promising to offer more information about the disease. The problem is that, once installed, CovidLock encrypts data from Android devices and denies data access to victims.	–	$ 100 per device.
Emotet	Trojan	Emotet is a trojan that became famous in 2018 after the U.S. Department of Homeland Security defined it as one of the most dangerous and destructive malware. The reason for so much attention is that Emotet is widely used in cases of financial information theft, such as bank logins and cryptocurrencies. The main vectors for Emotet’s spread are malicious emails in the form of spam and phishing campaigns.	United States	$ 2 million
Stuxnet	Worm	The Stuxnet deserves special mention on this list for being used in a political attack, in 2010, on Iran’s nuclear program and for exploiting numerous Windows zero-day vulnerabilities. This super-sophisticated worm has the ability to infect devices via USB drives, so there is no need for an internet connection.Once installed, the malware is responsible for taking control of the system	United States & Israel	$ 2 million

Zeus	Trojan	Zeus is a trojan distributed through malicious files hidden in emails and fake websites, in cases involving phishing. It’s well known for propagating quickly and for copying keystrokes, which led it to be widely used in cases of credential and passwords theft, such as email accounts and bank accounts. The Zeus attacks hit major companies such as Amazon, Bank of America and Cisco.	Eastern Europe	$3 billion
Melissa	Worm	The Melissa virus was a mass-mailing macro virus released on or around March 26, 1999. As it was not a standalone program, it was not classified as a worm. It targeted Microsoft Word and Outlook-based systems, and created considerable network traffic.	-	$ 80 million.