10 Deadliest Computer Viruses of All Time

By Azwan Jamaluddin in Internet. Updated on September 8, 2019.

Getting a computer virus has happened to many users in some fashion or another. To most, it is simply a mild inconvenience, requiring a cleanup and then installing that antivirus program that you've been meaning to install but never got around to.

However, in other cases, **it can be a complete disaster**, with your computer turning into a very expensive brick which which no amount of antivirus can protect.

In this list, we will highlight some of the worst and notorious computer viruses that have **caused a lot of damage in real life**. And since people usually equate general malware like worms and trojan horses as viruses, we're including them as well. These malware have caused tremendous harm, amounting to billions of dollars and disrupting critical real life infrastructure.

Here are the **10 most famous and malicious computer viruses**.

> **Recommended Reading:** 10 Signs Your PC Has Been Compromised

1. ILOVEYOU

ILOVEYOU is **considered one of the most virulent computer virus ever created**. It managed to wreck havoc on computer systems all over the world with around $10 billion worth of damages. 10% of the world's computers were believed to have been infected. It was so bad that governments and large corporations took their mailing system offline to prevent infection.

You might also like

Securing Your Computer from Identity Thieves
Armela Escalona

This Site Knows If Your Accounts Have Been Hacked
Sia

How to Sign In Password-Free to All Microsoft Accounts on Mobile Phone
Hadi Waqas

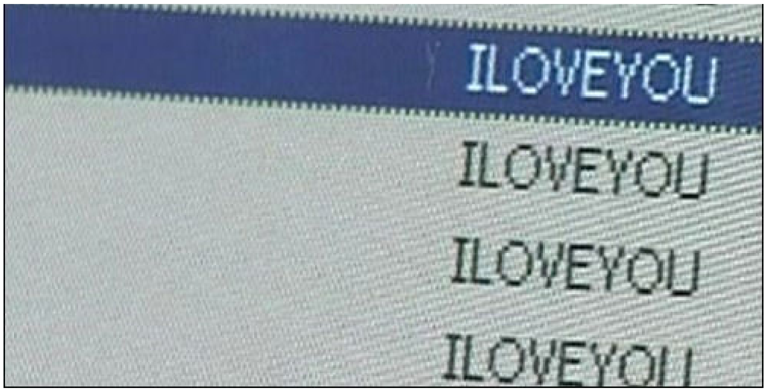
6 Safety Steps to Making Secure Mobile Transactions
Jake Rocheleau

20 Sites to Send Anonymous Emails (2018)
Ashutosh KS

50 Online Tools to Generate Pronounceable / Random Passwords
Hongkiat Lim

Tips & Tricks to Tighten up Your Gmail Security — Best of
Ashutosh KS

How to Reveal Passwords (Asterisks) in Browsers
Karrar Haider



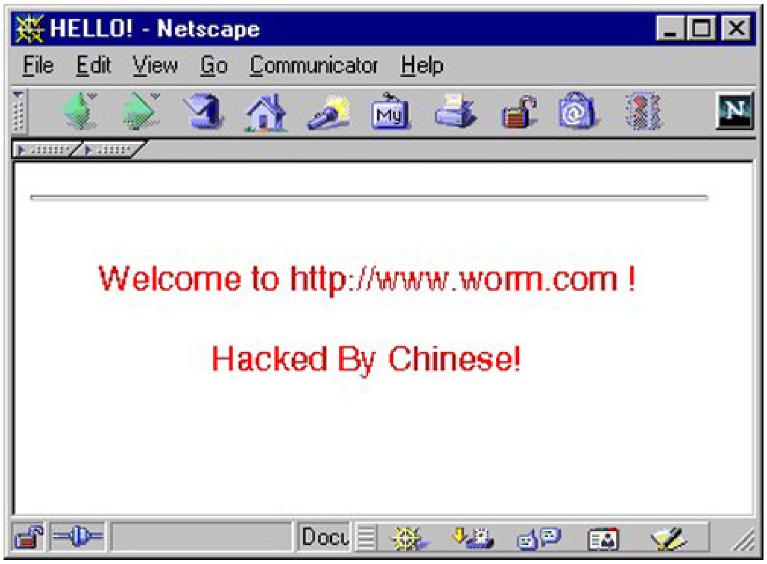
The virus was created by two Filipino programers, Reonel Ramones and Onel de Guzman. What it did was **use social engineering to get people to click on the attachment**; in this case, **a love confession**. The attachment was actually a script that poses as a TXT file, due to Windows at the time hiding the actual extension of the file.

Once clicked, it will send itself to everyone in the user's mailing list and proceed to overwrite files with itself, making the computer unbootable. The two were never charged, as there were no laws about malware. **This led to the enactment of the E-Commerce Law** to address the problem.

2. Code Red

Code Red first surfaced on 2001 and was discovered by two eEye Digital Security employees. It was named Code Red because the the pair were **drinking Code Red Mountain Dew** at the time of discovery.

The worm **targeted computers with Microsoft IIS web server installed**, exploiting a buffer overflow problem in the system. It leaves very little trace on the in the programming, it will duplicate even more and ends up eating a lot of the systems resources.



Welcome to http://www.worm.com !

Hacked By Chinese!

It will then launch a denial of service attack on several IP address, famous among them was the attack on the White House website . It also allows backdoor access to the server, allowing for remote access to the machine.

The most memorable symptom is the message it leaves behind on affected web pages, **"Hacked By Chinese!"**, which has become a meme itself. A patch was later released and it was estimate that it caused $2 billion in lost productivity. A total of 1-2 million servers were affected, which is amazing when you consider there were 6 million IIS servers at the time.

3. Melissa

Named after an exotic dancer from Florida, it was created by David L. Smith in 1999. It started as **an infected Word document** that was posted up on the alt.sex usenet group, claiming to be a list of passwords for pornographic sites. This got people curious and when it was downloaded and opened, it would trigger the macro inside and unleash its payload.

The virus will mail itself to the top 50 people in the user’s email address book and this caused an increase of email traffic, disrupting the email services of governments and corporations. It also **sometimes corrupted documents** by inserting a Simpsons reference into them.

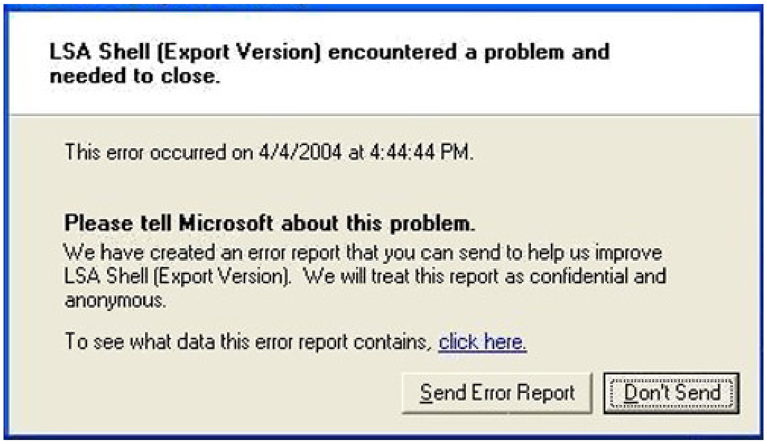
Smith was eventually caught when they traced the Word document to him. The file was uploaded using a stolen AOL account and with their help, law enforcement was able to arrest him less than a week since the outbreak began.

He cooperated with the FBI in capturing other virus creators, famous among them the creator of the Anna Kournikova virus. For his cooperation, he served only 20 months and paid a fine of $5000 of his 10 year sentence. The virus reportedly caused $80 million in damages.

4. Sasser

A Windows worm first discovered in 2004, it was created by computer science student Sven Jaschan, who also created the Netsky worm. While the payload itself may be seen as simply annoying (it slows down and crashes the computer, while making it hard to reset without cutting the power), t**he effects were incredibly disruptive, with millions of computers being infected, and important, critical infrastructure affected**.

The worm took advantage of a buffer overflow vulnerability in Local Security Authority Subsystem Service (LSASS), which controls the security policy of local accounts causing crashes to the computer. It will also use the system resources to propagate itself to other machines through the Internet and infect others automatically.



LSA Shell (Export Version) encountered a problem and needed to close.

This error occurred on 4/4/2004 at 4:44:44 PM.

Please tell Microsoft about this problem.

We have created an error report that you can send to help us improve LSA Shell (Export Version). We will treat this report as confidential and anonymous.

To see what data this error report contains, click here.

The effects of the virus were widespread as while the exploit was already patched, many computers haven't updated. This **led to more than a million infections**, taking out critical infrastructures, such as airlines, news agencies, public transportation, hospitals, public transport, etc. Overall, the damage was estimated to have cost $18 billion. **Jaschen was tried as a minor** and received a 21 month suspended sentence.

5. Zeus

Zeus is a Trojan horse made to infect Windows computers so that it will perform various criminal tasks. The most common of these tasks are usually **man-in-the-browser keylogging and form grabbing**. The majority of computers were infected either through drive-by downloads or phishing scams.

First identified in 2009, it managed to compromise thousands of FTP accounts and computers from **large multinational corporations and banks** such as Amazon, Oracle, Bank of America, Cisco, etc. Controllers of the Zeus botnet used it to steal the login credentials of social network, email and banking accounts.

In the US alone, it was estimated that **more than 1 million computers were infected,** with 25% in the US. The entire operation was sophisticated, involving people from around the world to act as money mules to smuggle and transfer cash to the ringleaders in Eastern Europe.

About $70 million were stolen and in possession of the ring. 100 people were arrested in connection of the operation. In late 2010, the creator of Zeus announced his retirement but many experts believe this to be false.

6. Conficker

Also known as **Downup** or **Downadup**, Conficker is a worm of unknown authorship for Windows that made its first appearance in 2008. The name comes form the English word, configure and a German pejorative. **It infects computers using flaws in the OS** to create a botnet.

The malware was able to infect more than 9 millions computers all around the world, affecting governments, businesses and individuals. It was **one of the largest known worm infections to ever surface** causing an estimate damage of $9 billion.

The worm **works by exploiting a network service vulnerability** that was present and unpatched in Windows. Once infected, the worm will then reset account lockout policies, block access to Windows update and antivirus sites, turn off certain services and lock out user accounts among many.

Then, it **proceeds to install software that will turn the computer into a botnet slave** and scareware to scam money off the user. Microsoft later provided a fix and patch with many antivirus vendors providing updates to their definitions.

7. Stuxnet

Believed to have been created by the Israeli Defence Force together with the American Government, Stuxnet is **an example of a virus created for the purpose of cyberwarfare**, as it was intended to disrupt the nuclear efforts of the Iranians. It was estimated that Stuxnet managed to ruin one fifth of Iran's nuclear centrifuges and that nearly 60% of infections were concentrated in Iran.

The computer worm was **designed to attack industrial Programmable Logic Controllers (PLC), which allows for automation of processes in machinery**.

It specifically aimed at those created by Siemens and was spread through infected USB drives. It altered the speed of the machinery, causing it to tear apart. If the infected computer didn't contain Siemens software, it would lay dormant and infect others in a limited fashion as to not give itself away. Siemens eventually found a way to remove the malware from their software.

8. Mydoom

Surfacing in 2004, Mydoom was **a worm for Windows** that became one of the fastest spreading email worm since ILOVEYOU. The author is unknown and it is believed that the creator was paid to create it since it contains the text message, “andy; I'm just doing my job, nothing personal, sorry,”.

It was named by McAfee employee Craig Schmugar, one of the people who had originally discovered it. ‘mydom’ was a line of text in the program's code (my domain) and sensing this was going to be big, added ‘doom’ into it.

The worm spreads itself by appearing as an email transmission error and contains an attachment of itself. Once executed, it will send itself to email addresses that are in a user's address book and copies itself to any P2P program's folder to propagate itself through that network.

The payload itself is twofold: first it opens up a backdoor to allow remote access and second it launches a denial of service attack on the controversial SCO Group. It was believed that **the worm was created to disrupt SCO** due to conflict over ownership of some Linux code. It caused an estimate of $38.5 billion in damages and the worm is still active in some form today.

9. CryptoLocker

CryptoLocker is **a form of Trojan horse ransomware** targeted at computers running Windows. It **uses several methods to spread itself**, such as email, and once a computer is infected, it will proceed to encrypt certain files on the hard still remain encrypted. **The only way to unlock the files is to pay a ransom by a deadline**. If the deadline is not met, the ransom will increase significantly or the decryption keys deleted. The ransom usually amount to $400 in prepaid cash or bitcoin.

The ransom operation was eventually stopped when **law enforcement agencies and security companies managed to take control part of the botnet operating CryptoLocker and Zeus**.

Evgeniy Bogachev, the ring leader, was charged and the encryption keys were released to the affected computers. From data collected from the raid, the number of infections is estimated to be 500,000, with the number of those who paid the ransom to be at 1.3%, amounting to $3 million.

10. Flashback

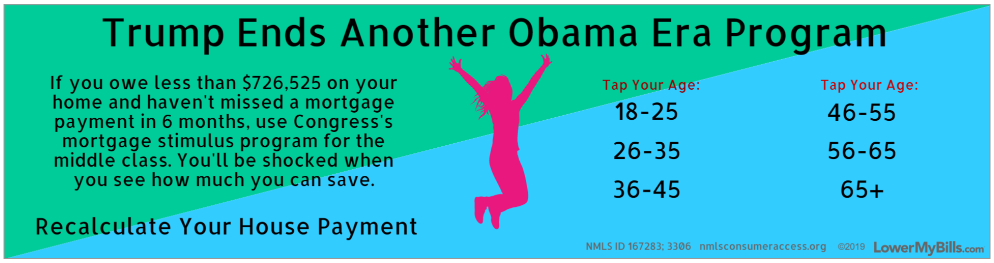
Though not as damaging as the rest of the malware on this list, this is **one of the few Mac malware to have gain notoriety** as it showed that Macs are not immune. The Trojan was first **discovered in 2011** by antivirus company Intego as a fake Flash install.

In its newer incarnation, a user simply needs to have Java enabled (which is

Mac becomes part of a botnet of other infected Macs.

The good news is that **if it is infected**, it is simply **localized to that specific user's account**. The bad news is that more than 600,000 Macs were infected, including 274 Macs in the Cupertino area, the headquarters of Apple.

Oracle published a fix for the exploit with Apple releasing an update to remove Flashback from people's Mac. It is still out in the wild, with an estimate of 22,000 Macs still infected as of 2014.



Show Comments