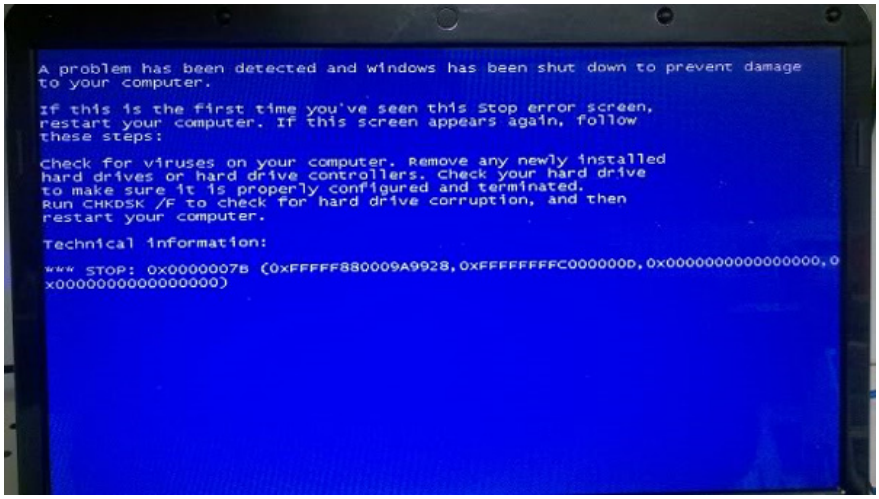
# Top 5 most dangerous viruses in the last 5 years

Virus - one of the most frequently encountered threats for computer users, we may still be living and working daily with them without knowing it. For technical and security experts, they are easy to identify and prevent, but most of the remaining users are often unaware of what is &

**QuanTriMang - Virus - one of the most frequently encountered dangers for computer users, we may still be living and working daily with them without knowing it.** For technical and security experts, they are easy to identify and prevent, but most of the rest users often find it difficult to know what the virus is, and what is the real program of the computer. In fact, viruses are software, but created with the purpose of undermining balance and security platforms in any computer system, they often cause abnormal phenomena such as increased performance. CPU's up to 100%, self-propagating, cloning and copying to directories and disk partitions . And since it began to appear, they have caused tremendous damage, consuming a lot people's money and effort in destroying and overcoming consequences. And below is a list of the 5 most dangerous viruses that have been reported over the past 5 years.

**1. Alureon (2010):**

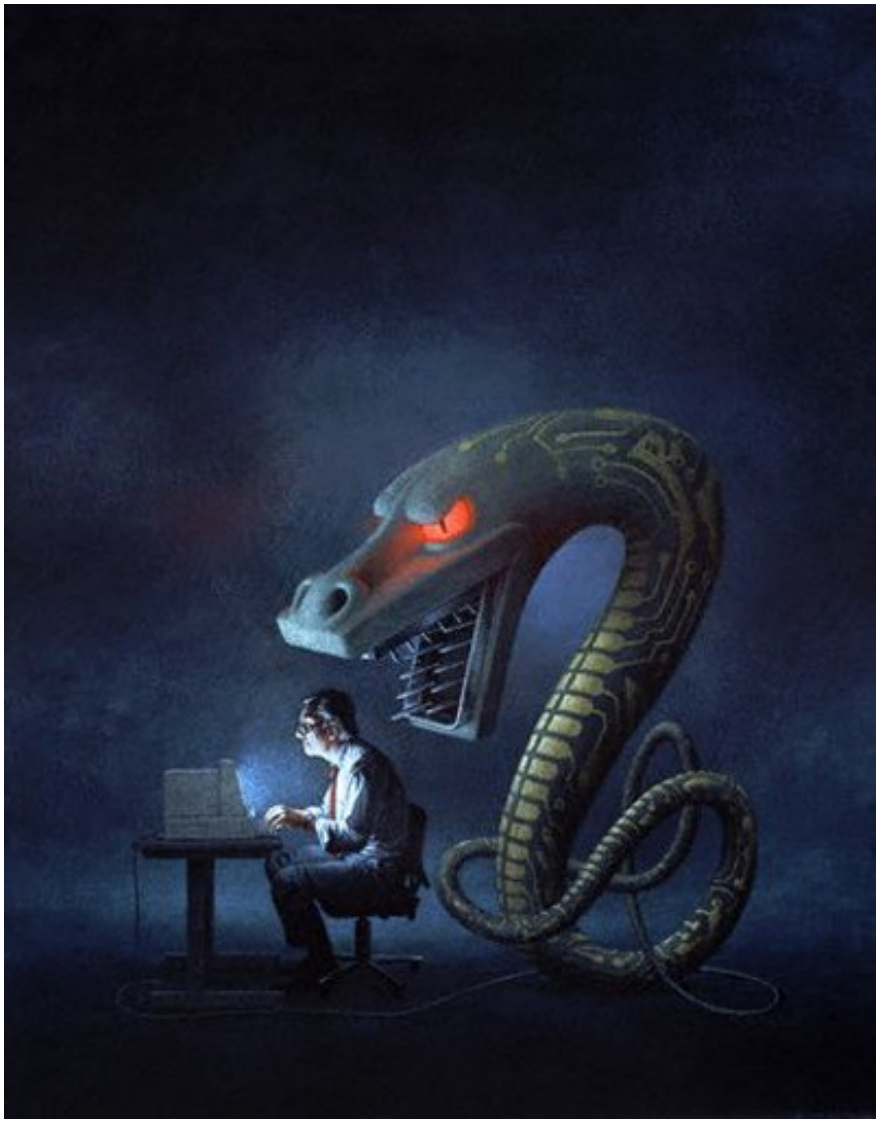
Let's start with the 'title' virus of 2010 - Alureon, extremely sophisticated and cunning in stealing user login names, passwords and data in credit cards by blocking data streams via the network. Besides, they also directly affect Microsoft's Windows operating system by creating a blue screen - *BSoD (Blue Screen of Death)* .




**2. Daprosy Worm (2009):**

The worm was discovered in 2009, and was named *Daprosy Worm by* Symantec, a security *firm.* This is a type of malicious code that spreads through the LAN model, distributing spam via email and USB storage devices. Usually their original files are read1st.exe, then continue to spread, duplicate and rename them according to the

archives. The most recognizable symptom is the appearance of **Classified.exe** files or **Do not open - secrets! .Exe** in the attached folder. They are 'famous' because of their ability to cripple the system, break the stability of programs operating in the operating system and constantly cause many other errors.



**3. Conficker (2008):**

Also known as *Downup, Downadup, Kido* , their attack target is Microsoft Windows operating system. Beginning to be vigorous and discovered in 2008, their attack process consisted of two main stages: first, security vulnerability MS08-067 in Server Service to allow execution of remote commands This step allows hackers to run binary code on the victim's computer without having to verify the account, and also have full control of the system. Next, the Conficker worm uses these computers to break admin account passwords in the local network, thereby easily spreading to the next computers. You can imagine their terrible devastation as millions of personal, business and government computers were affected only in 2008 across 200 countries worldwide, total losses. It was estimated at about 9.1 billion USD, mainly in Asia, South America and Europe. After "beating up" the victims, imagine that from a normal worm, they have "evolved" into Anaconda - a giant reptile monster.

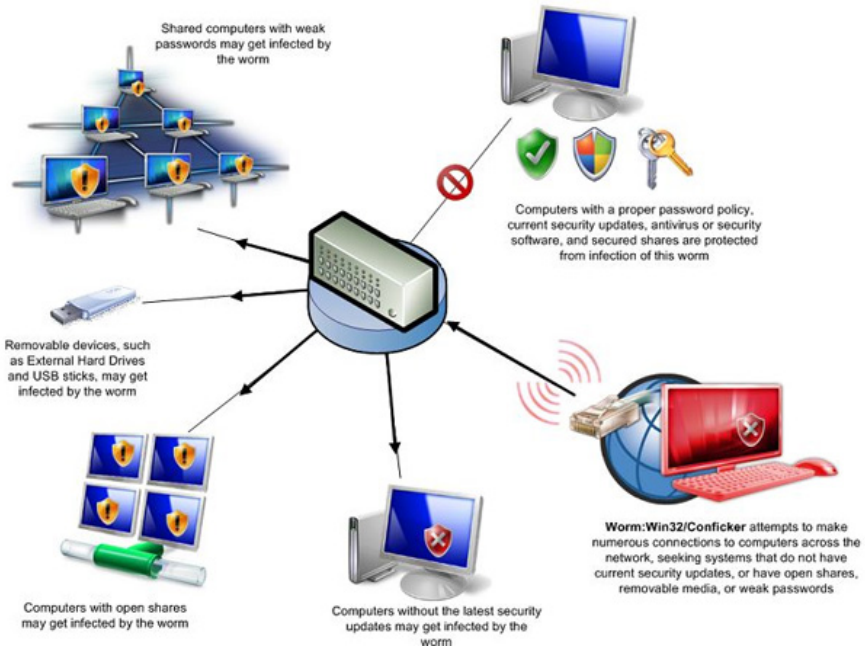
It seemed like everything was over but really, Conficker came back a little while later and many more dangerous features:

- Disable DNS lookups.

- Prevent Auto Update feature.

- 'Clearing' security programs.

- Review, and interrupt the operation of processes with the names of security applications, patches, security updates or other utilities.




**4. Storm Worm (2007):**

Or also called *Small.dam, Trojan.Peacomm, Trojan.Peed, Trojan.Tibs, W32 / Zhelatin* . This can be considered the king of viruses in 2007 - *Storm Worm* , often attached to itself. in emails with the title 230 dead as storm batters Europe, and immediately spread it to the curious user 's computer and open the email, then continue to replicate and spread through the victims themselves.


**5. Nyxem (2006):**

Also known by some other names such as: *Mywife, Hunchi, I-Worm.Yyem, Blackmal, Blueworm, Blackworm* . First appeared in March 2006, Nyxem mainly works and spreads. via email using SMTP protocol. The worm can replicate and send e-mails to victims via different titles, content and attachments, and replicate and spread to all partitions on the hard drive. . The most dangerous part of Nyxem is the ability to remove security programs, if installed on the same location specified in the source code, or delete components in the Windows Registry, so antivirus applications Do not start automatically with the system. Besides, it also comes with a GIF file used to make the recipient think that this email has been censored and safe by *Norton Anti-Virus* , but in fact it is not.