Red alert on computer viruses in Vietnam

In 2010 alone, 58.6 million computers in Vietnam were infected with viruses. Accordingly, on average, more than 160 thousand computers are infected with virus every day. Network security experts assess that this is an alarming number about computer virus situation in Vietnam.

In 2010 alone, 58.6 million computers in Vietnam were infected with viruses. Accordingly, on average, more than 160 thousand computers are infected with virus every day. Network security experts assess that this is an alarming number about computer virus situation in Vietnam.

>>> Avoid threats from the Internet

Red alert on virus problems

In 2010, 57,835 new strains of virus appeared, but the most widespread virus was an old strain of **W32.Conficker.Worm** . This virus has been " *popular* " globally since the end of 2008. Thought has been " *sunk* ", but according to the statistics of network security company Bkav, up to 6.5 million computers were infected with Conficker. in 2010.

Super polymorphic viruses (Metamorphic virus) continue to be among the top 3 most contagious viruses of the year and an obsession with computer users in Vietnam. With the ability to ' *change shape* ' to hide, the two strains of Vetor and Sality have spread over 5.9 million computers.

In the report of computer virus situation at the end of 2009, network security experts have predicted, ' *2010 will be the year to witness the sudden increase of fake antivirus programs* '. And in fact, 2010 saw an explosion in the

amount of computers infected with antivirus software, up to 2.2 million, 8.5 times higher than the number of 258,000 in 2009.

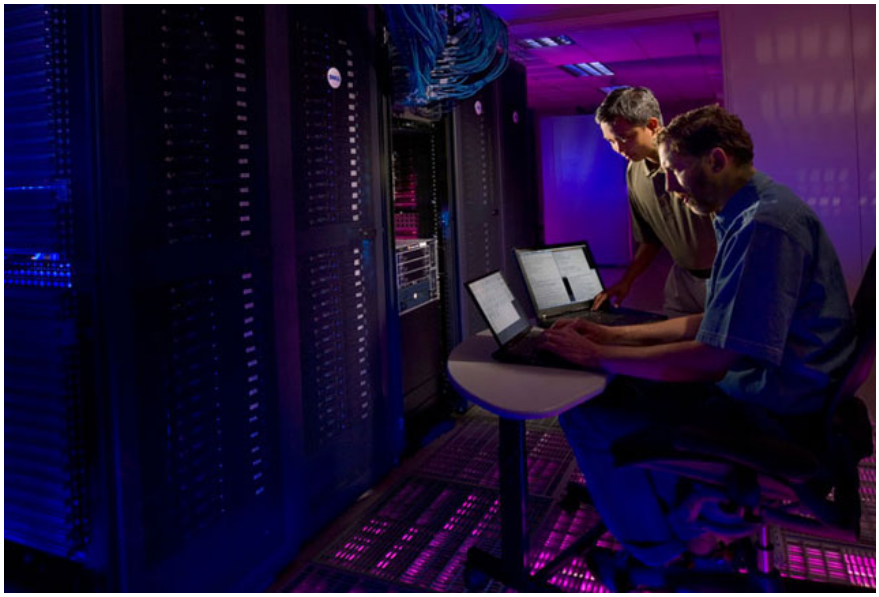
Leads users to fake online virus scanning websites, to install malicious code on the computer is a common feature of **FakeAV** . The main reason that many users in Vietnam have been infected with these types of virus is due to the habit of using floating software, without copyright. With this habit, although it has been warned by experts, the user is still " *innocent* " to click on every link even though it is unclear what it is. This is a deadly loophole so that Fake AV infects computers.

Along with that, more than 1.4 million computers were infected with fake virus folder, forged image files, word files, excel files. By using the icon to disguise, the executable file of the virus looks exactly like a folder or a data file in image format, word file, excel file .

This easily deceived the user's senses, even experienced professionals, making them easy to open virus files and infected without any doubt. This is also the reason why this virus strain has just appeared but has spread at a dizzying speed.

According to the law of spiral development, the return of this virus to a new form will be more sophisticated than those that destroyed data in the 1990s. Virus lines destroy new data equipped with fast spreading techniques over the Internet, so the speed of spread is much higher than the silently spreading of viruses that destroyed previous data. Therefore, the level of danger is thousands of times.

Alarm system intrusion status, DDoS attack



In 2010, many large websites in Vietnam have been invaded by viruses, revealing important information or being attacked by DDoS in recent years is a cause of concern in society.

Experts have discovered that some groups of hackers have installed viruses to infiltrate network systems in Vietnam, thereby stealing internal confidential information of organizations. In addition, they control websites that download software to install viruses on computers that download software from these websites. From there they can control the ghost computer network - **botnet** - to DDoS attack on large systems in Vietnam.

This is an alarming situation because in addition to large systems that can be attacked at any time, there are tens of thousands of computers across the country being controlled by hackers, which can affect national security. .

To prevent your computer from falling under the control of these hackers and network security experts, users need to be very alert when downloading software to their computers. At the same time, users also need to regularly update anti-virus software on their computers to promptly prevent virus from entering.

2011: Be careful with security on mobile networks

Network security experts predict that there will be many attacks and phishing attacks on mobile phones in 2011. It is possible to record the first malicious code releases on mobile phones, in tons of forms. Public mainly in the form of trojans, hiding and stealing personal information.

Rootkit will be a new trend when it becomes a ' *massification* ' tool, not a ' *privilege* ' of some " *knowledgeable* " hackers. Super-polymorphic viruses will incorporate new techniques to create persistent spreads that last for many years.

Along with the popularity of Windows 7 with the ability to ensure high security and every important implementation decision on the computer will belong to the user, the trend of deceiving virus users will thrive. Where the virus fakes data files (Fake icon) are the first manifestations and this trend will continue in 2011.

The virus takes advantage of sites that download popular software to spread, create **botnets** , purposely attack predetermined targets, steal confidential information of organizations and individuals will appear more.

List of the 15 most contagious viruses in 2010:

first

2

3

4

5

6

7

8

W32.Conficker.Worm

W32.Vetor.PE

W32.Sality.PE

W32.AutoRunUSB.Worm

W32.SecretCNC.Heur

W32.ForeverX.Worm

W32.CmVirus.Trojan

W32.UpdateUSBA.Worm

9

ten

11

twelfth

13

14

15

W32.StuxnetQKE.Trojan

X97M.XFSic

W32.SilityVJ.PE

W32.BedolabD.Worm

W32.Regsvr.Trojan

W32.DownRefronE.Worm

W32.SysdiagTHA.Trojan