

4 problems difficult for network security 2013

After a dizzying pace of development, it can be said that 2012 is a year when global internet in general and network security in particular show signs of slowing down. Many experts have predicted that some trends or trends have shaped the internet world in 2012 will continue to play an important role in her.

After a dizzying pace of development, it can be said that 2012 is a year when global internet in general and network security in particular show signs of slowing down. Many experts have predicted that some trends or trends have shaped the internet world in 2012 will continue to play an important role in the global network map next year.

And here are a few of them:

Internet: Tools of governments

'Ultimately, many governments have realized that the internet is a relatively perfect tool for monitoring, controlling, counterintuitive, or even fighting.' That's a spokesman for Mikko Hypponen, technical director of F-Secure, a Finnish network security enterprise in a letter to technology news website CNET. Luckily, we can be sure that in 2013, the internet will not completely become a fiery battlefield between government, businesses and on the other side dangerous hackers. But *'work'* prepares the internet to become a security front that has been prepared by many countries for a long time.



'There will definitely be projects like 'Olympic Games' coming out in the future. Later, we will see the first 20 years of Internet existence is indeed the Golden Age, when everything is still free. ' The "Olympic Games" here Hypponen wanted to mention the US government-related project, which created Stuxnet, Duqu and Flame, tools to attack the Iranian government's network to undermine the program. nuclear of this country.

Network security expert Chris Wysopal agrees that 'digital war' will not be too strange. 'Virtual war will certainly exist in parallel with real life combat.' More specifically, government-assisted attacks in some countries will soon become 'routine'.

However, not because the attacks have occurred more often, but they are less likely to make the experts feel surprised. Network security expert Tomer Teller at Check Point said he was amazed at the number of "accurate oriented attacks" from hacker groups.

Tim Rains, director of Microsoft's security department, pointed out that the consequences of government-assisted attacks will be far more dangerous than those operating in Iran and attacks. enterprise network.

Mobile: The fat prey of hackers

Obviously, the second trend is a big opportunity for businesses or startups, not worrying like the trend we mentioned above. Network security experts are beginning to care about protecting their smartphones or tablets from internet threats from the past few years. With the current growth rate, the protection of mobile devices against hackers is even higher than ever.

Protect your most personal computer

F-Secure Mobile Security makes your smartphone safe for today's connected life and protects your important data against mobile malware.

START MOVIE

MOBILE SECURITY

Features

- Antitheft
- Browsing Protection
- Antispyware
- Antivirus
- Firewall
- Automatic updates
- Light and efficient

BUY TRY

Derek Halliday, product manager of Lookout Mobile Security, points out two trends that his company has noticed in 2012: Currently only a few main malware attacks mobile devices. The second trend, Halliday said: Ignoring the poorness of the number of malware, we can even see the incredible contrast to the number of attacks via mobile devices. dynamic. 'If you try to trick someone over the phone in the US, you will encounter many problems and it will be difficult to succeed. However, things are different when the attack takes place in Russia or China. '

Halliday adds that Android 4.2 is currently the safest mobile operating system, with many upgrades in security from Google. But fragmentation will certainly make this operating system harder to choose, at least until the end of 2013.

Data theft

One of the hot issues in 2012, is the attacks that steal data from individuals, businesses or even governments. Behind the server system of Google, Facebook or simpler is the mobile application that allows data storage on the server, is extremely valuable information for many advertising organizations, businesses or bad rather than criminals.



Therefore, Halliday advises internet users to protect themselves by learning and using personal customization tools on social networks, as well as paying attention to controlling personal information. social networks or other applications.

You finished reading the article "**4 problems difficult for network security 2013**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.