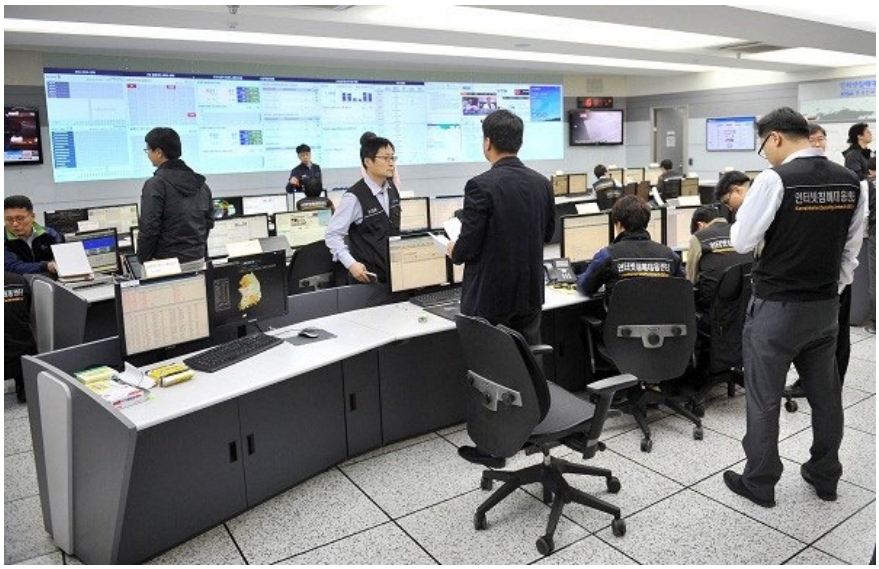
Network security challenges in 2014

Cyber ??security company Bkav afternoon 13/11 announced that DDoS attacks, spyware and malicious code on mobile phones were outstanding security issues in 2013 and will continue to be trend of 2014.

Cyber ??security company Bkav afternoon 13/11 announced that DDoS attacks, spyware and malicious code on mobile phones were outstanding security issues in 2013 and will continue to be trend of 2014.



Install the virus without exploiting the vulnerability

According to *Bkav* , virus dispersal has actually become an " *industrial* " *industry* in espionage activities in 2013. *Bkav* 's recognition shows that spyware has appeared in most important agencies from the Government. to the business. These spy software take advantage of security holes in text files (*Word, Excel, PowerPoint*) to spread.

By the end of 2013, taking advantage of spyware file text files had gone one step further. In the middle of December 2013, Bkav discovered a series of hackers inserting malicious code into a text file without using a vulnerability.

Specifically, malicious code is hidden in the form of a thumbnail that is directly embedded by a hacker into a text file. To read the content, make sure the user clicks to open a larger image and doing so will activate the malicious code.

' *With this form, any computer will have spyware installed without a vulnerability. This is a method that will be widely used and a trend in 2014* , 'said Ngo Tuan Anh, Bkav's vice president of cybersecurity.

Malware spreads between computers and smartphones

Viruses spread from phones and computers.

Besides, with the connection between computers and smartphones becoming popular, viruses have spread. In November 2013, *DroidCleaner* and *SuperClean* were the first virus lines to be able to carry out cross-behaviors between computers and smartphones.

Malicious multi-platform malicious code is very worrying amid the context of the world of smartphones and computers is almost one. This similarity makes it easy for hackers to create malware that can operate on different platforms at the same time, maximizing the likelihood of spreading.

In 2014, this trend will continue to be strong, even booming because the smartphone market is growing rapidly. More than 1 billion smartphones are sold worldwide in 2013 and this number will be 1.7 billion in 2017 (*IDC*). In Vietnam alone, in 2013 there were 17 million smartphone users and approximately 7 million computers were in use.

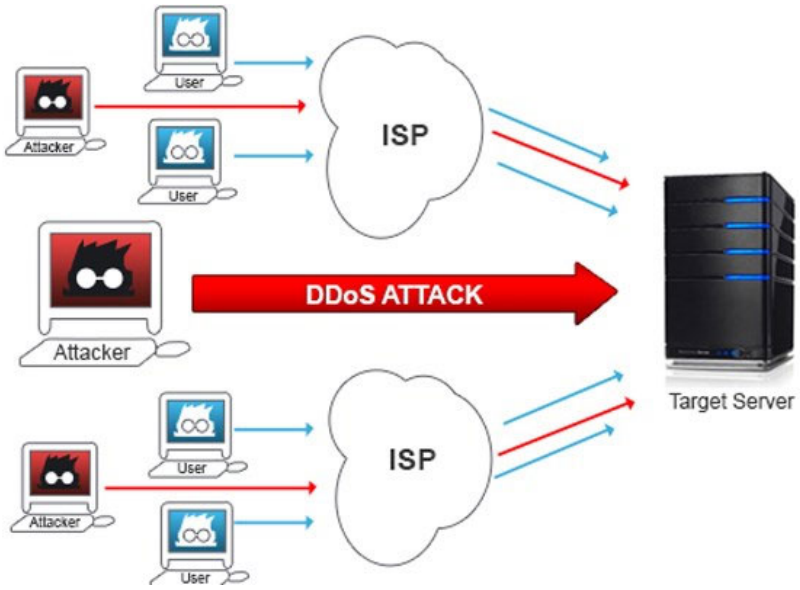
Fake browser Smartphone

In 2013, counterfeit software targeted at Smartphone not only increased in number, but also expanded counterfeit objects to bypass antivirus software and deceive users.

After the **Instagram** application, *Angry Birds* games and even antivirus software is borrowed by malware, in turn the most popular browsers today such as Firefox, Google Chrome . are also disguised by malware to attack users.

Last November, a series of fake updates of these browsers were posted on unofficial app markets, taking advantage of users' high search needs to spread malicious code.

DDoS continues



DDoS attack diagram.

In 2013, the denial of service (*DDoS*) *attack* caused many Vietnamese electronic newspapers to be paralyzed. Through analysis of network security experts Bkav, these attacks are made possible by a giant botnet system, made up of countless users' computers.

Specifically, taking advantage of users often arbitrarily download software, applications without regard to the origin, hackers spread viruses by inserting malicious code into popular software like *Unikey*, download management tool, edit videos . and post the forums. Users who download these fake software accidentally turn their computer into a zombie in the botnet system.

Therefore, when users have not changed the habit of arbitrarily installing software of unknown origin, it is still unintentional to lend a hand to hackers to implement **DDoS** attacks.

You finished reading the article "**Network security challenges in 2014**" 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.

© 2019 TipsMake.com