Detecting zero-day vulnerabilities in Internet Explorer helps hackers gain control of the computer

The research team from Qihoo 360's security unit discovered a zero-day vulnerability (the term refers to unpublished or unresolved vulnerabilities) on Internet Explorer.

The research team from Qihoo 360's security unit discovered a zero-day vulnerability (the term refers to unpublished or unresolved vulnerabilities) on Internet Explorer.

A group of hackers are actively exploiting this vulnerability to control computers running Windows operating systems.

This vulnerability infects Office documents containing malware downloaded from IE. Malware will infiltrate and control the "User Accounts" section of the operating system, and jump on pop-ups that cause the device to be paralyzed.

According to experts, this group of hackers are also "hard at work on their own" because very few people now use IE (only 17.55%, even lower than this number) and users also. Very wary when opening unidentified Office files.

Still, researchers are calling on Microsoft to release an emergency patch to fix the flaw, as a small number of people remain loyal to the browser, especially organizations, The agency still selects IE as the default browser on its system.

See more:

1. Warning: Detecting more than 1000 Cisco router and switch devices in Vietnam has a serious security error

2. Only charging the battery through a computer, your iPhone may also be hacked
3. Facebook awards 1 billion VND for those who find new data holes
4. Hackers attack the casino through a hole in the smart thermometer of the aquarium

You finished reading the article "**Detecting zero-day vulnerabilities in Internet Explorer helps hackers gain control of the computer**" 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.
