

## SMS becomes a trojan spread tool

Hackers are using text messages via mobile phones to entice users to access a malicious website to build the 'zombie' network. This is the content of the warning message that security firm Websense has just released.

**Hackers are using text messages via mobile phones to entice users to access a malicious website to build "zombie" networks.**

This is the content of the warning message that security firm Websense has just released.

Websense said the security attack uses "social engineering" techniques to entice people to access a dangerous website. An SMS text message is sent to the mobile phone of the user thanking them for registering to use a "virtual" service. The message said it would automatically charge \$ 2 a day for the service. This fee will be charged directly to the phone bill. The service can only be stopped when users announce to stop using the "virtual" service through a website.

SMS messages with similar content are also repeatedly sent to a variety of online forums online, security firm Websense warns.

The attack began on Thursday last week in the US and was first discovered by security firm Sunbelt Software.

Once users access the website mentioned in SMS to stop using the service, they will be "encouraged" to download a trojan. Not only that, the attacker also gives detailed instructions on how to bypass security alerts in Internet Explorer.



After Websense named "Dumador" - installed, it turned the victim's PC system into a "zombie" that allowed an attacker to control the system remotely. This PC will become part of the "bot" network that serves attacks online.

*" This is the first time we've seen this kind of attack ," said Ross Paul, Websense's senior product manager. " Basically, this attack uses" social engineering "techniques so it has tricked many victims. "*

Security firm Websense said the company is currently monitoring the attack but has yet to discover the attacker.

*" In general, these attacks are often organized by a group of people. In some cases we know their nicknames. But in some cases it is not ," Paul said.*

Websense cannot statistically determine how many people have become victims of this attack. Monitoring the performance of "botnet" networks is a difficult task because this network can be located in many different countries.

Dumador trojan allows an attacker to use the HTTP protocol to control controlled PC systems or trick victims into uploading personal information. The most popular form of "bot" control is through Internet Relay Chat (IRC) channels.

The emergence of new attacks via SMS has proven a new trend in hackers. They are not from any means to attack the victims in order to bring them illegal profits. Trojans, worms, viruses or malware are no longer a way to prove their ability or become as popular as they were in the past. They have become an instrument of real profit. This is a prominent trend of cyber criminals today.

## **Hoang Dung**

You finished reading the article "**SMS becomes a trojan spread tool**" 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.