

## Russian Trojan targets bank account

SecureWorks warned a Russian criminal organization is using the Gozi trojan to steal personal information by exploiting an Internet Explorer vulnerability.

**SecureWorks warned a Russian criminal organization is using the Gozi trojan to steal personal information by exploiting an Internet Explorer vulnerability.**

According to a recent report, the trojan has been specifically designed to bypass banks' protection systems and has stolen information about 10,000 records.

A spokesman for SecureWorks, the first security firm that discovered Gozi said that in its code there are components that trick the account validation system used by banks. SecureWorks calls on the financial community to be alert to the next attacks.

Analysts from SecureWorks said Gozi started operations on December 13, 2006. It was only discovered 50 days later, when it stole about 10,000 records, with personal information of about 5,200 people and about 2,000 social security cards.



SecureWorks also provides data collected from banking applications, student forums, online job search software, electronic taxation tools, government applications and infected online phone stations. infected.

' *Interestingly, many banks that have customers attacked have a user identity system .* ' The representative of SecureWorks said via e-mail: ' *However, the information that Gozi collected allows people to pass through the security system quite easily* '. Stolen information includes account numbers and passwords of users at the world's leading banks, money transfer services and retailers. In addition, hackers also obtained login information of employees to bypass law applications. These data were sold by Russian hackers for about \$ 2 million.

Don Jackson, a specialist at SecureWorks, said many home computers are infected when users visit online gaming and entertainment forums.

SecureWorks said it had informed the US authorities in February, and is continuing to support the investigation.

Mr. Jackson confirmed that the mother server dispersed Gozi is located in Russia, belonging to a record business network 'not very clean' and is considered the gathering point of those who distribute trojans, spyware, phishing tools, . Places. Only selling stolen data has been deleted but the server is still active and continues to receive new data from Gozi.

## **Hoang Minh**

You finished reading the article "**Russian Trojan targets bank account**" 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.

---

