How do economic hackers work?

It's the world of chat rooms, malware and sophisticated phishing plans. How are their inner activities? Hacking is no longer a children's game. It has become a big business. The th

It's the world of chat rooms, malware and sophisticated phishing plans. How are their inner activities?

When TJX was launched on January 17, 2006, computer systems stored data related to credit cards, debit cards and sales transactions that were destroyed. It is said that they have been hacked since December. Security agents at Visa recorded increasing fraudulent credit card and debit card related TJX attributes, such as in TJ Maxx, Marshalls, and HomeGoods stores from mid-November. That means you can completely steal user data floating on the Internet to sell to the black market via website and chat room, at least for two months or more.

Hacking is no longer a children's game. It has become a big business. The vibrant online black market with stolen credit card data, driver's license code. And malware, the program that allows hackers to exploit security vulnerabilities on commercial software, is a powerful tool for hackers. Terrorism became highly organized. They use peer-to-peer payment systems such as buying and selling on eBay without fear of being discovered when working together.

Independent hackers still exist, but the FBI has found organized crime to be part of the hacking community, especially in the Middle East. ' *Hackers are always ready to unlock computers, collect personal data and sell them for profit,* ' said Chris Stangl, the FBI's terrorist crime inspector, the third-ranked unit behind the Terror and Love division. according to newspaper.

Drawing a complete picture of economic hackers is not easy. It is a vibrant underground world but not everyone can catch them all. From 'gleaning' internal and external sources, you can only outline a part of this world.

Direct method

' *Now it's no longer a time for hackers to point out the vulnerability on the Net. They create sophisticated malware for commercial and profit purposes* ', eEye's Maffret. Some hackers use a direct method of ransom attack. Criminals infiltrate corporate computers with malware and encrypt data in computers. Next, they ask the company to pay ransom to get the decryption key. This form is very popular in Russia. Uriel Maimon, a senior customer researcher for RSA, an EMC-owned security firm, said he has seen such kinds of attacks in the past five months.

But direct attacks are not the most common form, because they are quite risky. Directly, that is, ' *there is a straight financial connection between the victim and the author or the malware owner* ' - David Dagon, a research specialist at the Georgia Tech Information Security Center, analyzed. The more popular form is the black data market. Online website abundantly on the Internet, is the place where busy trading activities such as debit card numbers, credit cards, cardholders' names, card verification values, three or four-digit codes are used to verify cards . Jeff Moss, manager of "The Dark Tangent" and the founder of Black Hat, a security training research firm (owned by the father of Informationweek CMP) said he knew there was a terrorist organization in Europe. Europe earns half a million dollars a year from buying and selling databases and customer name lists.

Information on credit cards is mostly sold in large quantities. When you buy, you will definitely not want to have each one but a collection, a lot, a group. Because anyone can cancel or participate in fraudulent compensation. Although some websites offer price lists, the information on basic cards is sold at least at $ 1 per card, depending on the quality of the data.

Credit card thieves call themselves 'carders' and often drop their malware via IRC chat rooms, public forums or private forums with names like CardersMarket or Carder.info, even e-commerce websites look very normal and harmless. Experienced hackers or carders are often tied to their own IRC, encrypted and password protected.

The forum is called CardingWorld.cc with over 100,000 articles from 13,000 registered members, most of them from Russia. And the English-speaking area on the website always refers to the US National Bank (Bank of America), Fidelity Bank, PayPal, credit card information from around the world, valid gift cards and translations. Safe transportation with large amounts of money. Most buyers and sellers on the forum require transactions and offers to take place on private messages in the message board system or ICQ instant messages.

Like Dumps International website, provide credit cards, equipment to encrypt and use credit cards as well as social security numbers (Social Security numbers), birth dates, mother's maiden names, codes Bank PIN number, patches of 'rendered' card with card number, card holder name, expiration date. The price charged for a card number can be up to $ 40 / standard card and $ 120 / a 'signed' card. If you buy a lot of 100 price cards, you can drop it to $ 30 / card.

The average lifetime for these websites is about 6 months before they are redirected in the new proxy server and have legal intervention. TalkCash.net, an active website until the summer of last year, also provided a list of 'ripper', who participated in the market but were not reliable, and firms 'verified', who proved that they can distribute the goods as promised.

Some terrorists use peer-to-peer payment systems like PayPal, E-gold to trade in gold and transfer back to cash in each country. Others use Western Union to create payments. E-gold says that 'there is no way to ignore' for anyone who uses its services for criminal purposes. PayPal's chief information security officer, Michael Barrett, said the company regularly works with legal organizations when there is any indication that criminal activity has occurred.

Money transfer activities are often very dangerous because hackers are always stalking for ways to usurp. If the amount of money is large, from more than 10,000 dollars or more, it is advised to notify the bank to follow up. Large transactions can be broken up by hackers like when customers pay for plasma TVs, invade large amounts of iTunes accounts, World of Warcraft appraisal information and even hack into routers.

Trading in Malware

Another valuable commodity in the economic hacker world is malware like viruses, worms, and Trojans. They provide hackers access to enterprise systems.

' *Hackers hope businesses will have to redeem their data* ' (Kaminsky).

A recent report by Internet Security Systems (owned by IBM last year) warns the industry's emergence of 'vulnerability exploitation service' with sophisticated distribution and production networks similar to Legal product channel of the computer industry. ' *Vulnerability vendors often buy faulty code from the black market, encrypt it to prevent piracy or piracy, sell it to top spammers* .'

For any market economy, the highest value goods will control the highest price. In December, a flaw found in Microsoft's new operating system Vista was found and sold on the Romanian Web forum for $ 50,000. Raimund Genes, chief technology officer of security firm Trend Micro, makes sure the malware industry controls more than $ 26 billion of the 2005 security firm.

That huge amount of money appeals to an equal number of criminals. The ze-ro day vulnerability was discovered last year and sold for between $ 20,000 and $ 30,000. Zero-day is a dangerous flaw, always creating new enhanced variants as soon as it is discovered, and before manufacturers can patch their products.

Although warned about the dangers of ze-ro and other security holes for companies and their customers, very few legal organizations can prevent someone from writing a chapter. process to exploit these vulnerabilities. You can't accuse someone of committing crimes when ' *pointing out unpatched holes on the Internet* ' - Marc Maiffret, founder and director of hacking department at eEye Digital Security said.

Phishing escalates

Phishing is also becoming an expensive underground business. Spammers often search for e-mail addresses on

the Web to sell to hackers. Hackers rely on it to find a potentially exploitable vulnerability, create phishing websites and tell spammers who send e-mail phishing. Meanwhile, carders buy information stolen from hackers, create fake credit cards, fake debit cards to steal money or sell to many other crimes. Of course a terrorist activity can do many other things.

The Anti-Phishing Working Group, a consortium of community and private organizations, says the tools used by phishing scammers are now becoming more sophisticated. The December report of this group recorded more than 340 new variants of keylogger (keyboard stealing software) and Trojan hours used by phisher in just one month. The number of days increased by 'better use of automated tools to create and test new variants,' the report said.

Potentially, these tools were spawned from Eastern Europe with phishing programs and automatic spam distribution mechanisms. Those who create them are mostly young, only in their twenties. Some are educated and educated, but others are not. Some live in countries like Romania, where Internet bandwidth is more in households than some companies in the US. They grew up on the Internet more than 10 years ago and the laws there are less strict than places like the United States.

Sophisticated technology is not the only aid tool for phishing commerce. It's unbelievable, but the '419' Nigerian scammers continue their work successfully with many users using e-mail. Those e-mails usually start with the phrase 'I need your help' and describe the situation that makes them need a lot of money to save someone and move to a country. That money is called an 'advanced fee' because they may require victims to send money to help them free up some huge account with the promise of double or a large amount of compensation. The number 419 is the criminal code Negerian once once caused fever and stormed famous scams.

Last month, Michigan's former treasurer Alcona County was arrested and forced to pay $ 1.2 million he had "tackled" and at least sent some to the infamous Nigerian e-mail scammer. The US Federal Trade Commission had to issue this warning on its website: ' *If you receive an email saying that you need help with a sum outside Nigeria or any other country, please send it to the Trade Council (FTC) at spam@uce.gov* '.

'Pump and Dump' - Information and profit

On January 25, the Securities and Exchange Commission seized a 21-year-old boy in Florida when he destroyed a series of online brokerage accounts, then had to eliminate many names. his item. Investors say that the Aleksey Kamardin of Tampa, during the last five weeks of the summer, has earned more than $ 82,000 when using compromised accounts funds in Charles Schwab, E-Trade, JPMorgan Chase, TD Ameritrade. and many other online brokerage agencies to gently buy shares of trading companies. These purchases create a virtual craze for legitimate commercial activity, raising stock prices. After that, Kamardin sold the shares he bought first at high prices and caused the stock market to decline.

That's the new bottle of old wine 'pum and dump', a form of stock fraud based on secret information. Thieves will invest in cheap stocks, using accounts on the Cayman Island or somewhere far away from land that can set up anonymous account information. When a thief buys or steals identity information, he will set up a fake account, or infiltrate someone else's account (as in the case of Kamardin) and buy large quantities of cheap stocks, hold price control.

This creates a sensitive situation for financial services providers. ' *They do not want to prevent everyone's business. Therefore, creating these fraudulent accounts has become a risky part of their businesses,* 'said Marc Gaffan, marketing director of RSA consumer solutions. Likewise, it is difficult to scrutinize the business order because they are strongly influenced by time. Delay causes investors to lose money and hesitate to invest in that company. Last year, E-Trade encountered a similar dilemma when a computer was attacked, open to terrorists running pump-and-dump on the E-Trade client, leading to fraudulent activity. on the $ 18 million loss reported in the third quarter.

What to do before this situation?

The New York Electronic Crimes Task Force of Secret Service conducted the largest search in 2002 when

claiming a former database administrator of Prudential Insurance, Donald McNeese stole identity and fraud information. Credit card and money laundering. McNeese stole the logs on a Prudential database containing information of 60,000 employees. When he tried to sell this information through the Web, Bill Moylan, a former inspector of Long Island's Nassau County Police Department, who performed secret missions discovered and contacted him. McNeese sent Moylan about 20 employee identification information and advised him to use it to create fake credit cards, some of which were sent to McNeese's home in Florida. McNeese was finally sentenced to three years in prison and forced him to spend $ 3,000.

Secret Service is a US federal organization responsible for investigating terrorist plots and economic hackers. In 2004, the organization found a group of hackers using the Shadowcrew.com website for illegal purposes. Six years later they were brought to federal court and forced to hire defense attorneys to steal credit cards, bank codes and identity information. Last March, Secret Service announced the capture of seven out of 21 suspects three months under Operation Rolling Stone, a program to investigate identity theft and online fraud "through Web criminal forums."

Even so, economic hackers still don't falter. At the RSA Security Conference, which took place in San Francisco last week, RSA Art Coviello chairman said that the identity theft market has reached one billion dollars and malware has increased by 10 in five years.

' *The fundamental problem is that we have geographic enforcement organizations geographically, but there are no geographic elements on the Internet,* ' said Dan Kaminsky, a security researcher at DoxPara Research. And: ' *We can't eavesdrop on phones through the ocean or surprise someone's home in Romania without local cooperation. We only have talent and personnel in our country.* '

As a result, law enforcement must be based on close cooperation of many private sectors such as financial institutions, Internet service providers and telecommunications companies. There are many criminals operating in local legal organizations throughout the country. Many of them have access to FBI InfraGard, the information sharing system between FBI and private areas. InfraGard has been a subsidiary of the FBI in the intellectual field since 1996 to support IT professionals and academia, serving as FBI-related terrorist investigations.

IT companies are also partly responsible for opening up the 'underground' online market with malicious codes and stolen data when releasing software with vulnerabilities. security. IBM's ISS has recorded a total of 7247 software vulnerabilities in 2006, an increase of nearly 40% compared to 2005. In particular, the vulnerability comes from Microsoft, Oracle and Apple as the largest.

Businesses and end users must stand together with some loose responsibility or security, sometimes simply storing too much data. In the case of TJX, the reason is that storing credit card data against Vista's regulations. ' *The operating system will assume that it is wrong for everyone to leave the data* '.

Companies need to carefully provide the data they are managing and assess the actual ability to protect it. If not, they may see these data on a black market website.