



# The Panda Outlaw: W32.Fujacks

Robert X Wang  
Symantec Security Response, Dublin



# The Panda Outlaw: W32.Fujacks

## Contents

Introduction.....	4
What makes W32.Fujacks so successful.....	4
Who is paying for W32.Fujacks.....	6
Is it over yet.....	8
How to prevent this kind of attack.....	9
Conclusion.....	9

## **Introduction**

W32.Fujacks (Chinese name: Panda Shao Xiang) is a worm and file-infector virus, which is written in Borland Delphi. The W32.Fujacks outbreak started in November 2006 and its author has consistently released a considerable number of new variants. W32.Fujacks and its variants have spread widely throughout China since then. Finally, on 3rd Feb 2007, the author Mr. Jun Li was arrested by Hubei Police Department. Another 5 suspects Lei Lei, Lei Wang, Peixin Ye, Shun Zhang and Zhe Wang were arrested separately in Hubei Province, Shandong Province, Zhejiang Province and Yunnan Province over the following few days. This is the first case of organised cyber-crime in China, using a computer virus. However, according to a recent report, Mr. Li had already sold the source code for W32.Fujacks to other people before being arrested. By 1st March 2007, several new variants were found. Furthermore, the source code of W32.Fujacks has now been made public.

## **What makes W32.Fujacks so successful**

From a technical point of view, W32.Fujacks and its variants are not very complicated. There is no cutting-edge technique used. The question is “What on earth can make it so successful?”

### **Crazy updates driven by profit motivation**

Unlike most other common viruses, W32.Fujacks and its variants were updated with an astonishing frequency. Within 3 months, dozens of variants have been found. These variants are not only repacked with a new harder to detect packer – obviously, Mr Li and his friends are driven by profit – they also attempt to add more and more functions to make it spread widely and steal more valuable assets.

These frequent updates cause considerable trouble for the scanning and repairing of computers infected by the W32.Fujacks family.

### **Group spreading**

A large number of people had a keen interest in making sure that W32.Fujacks was successfully propagated. The fact that its core members were arrested individually in the East of China, Centre of China, and South West of China proves that the profit chain of W32.Fujacks is huge. According to a study, Mr Li sold W32.Fujacks and its variants to about 20 people directly. Next, these affiliates resold W32.Fujacks to another large group of people.

With help from all of these people, W32.Fujacks and its variants have spread explosively.

### **Botnet**

When W32.Fujacks infects a computer, it downloads several Trojan horses from the Internet. It then attempts to steal account information for several online games. It also attempts to steal account information from the Instant Messenger tool “QQ”, which is one of the most popular IM tools in China. Furthermore,

it also gains full control of the compromised computer and uses it to build a botnet. The hacker will use these compromised computers for further attacks.

### **Social Engineering**

Social engineering techniques have always been widely abused by computer viruses and malware. W32.Fujacks is no exception to this trend. When W32.Fujacks and some of its variants execute, the icon of all infected files will be changed to the following:



Many Chinese people love the Panda and are also looking forward to the coming year of the Golden Pig. Some Chinese people may be deceived into clicking and running this executable.

### **Terminates Antivirus and Firewall applications**

W32.Fujacks enumerates windows and all running processes. If any specified security application is found, W32.Fujacks will end that application. By doing this, all subsequent Trojan horses will be free to execute and cause more damage to the compromised computer.

### **Infects both executable and script files**

Unlike most other viruses, in addition to infecting .exe, .pif, .com, and .scr executable files, W32.Fujacks also injects malicious JavaScript into all .asp, .aspx, .htm, .html, .jsp, and .php files. If any of these infected files are uploaded to a Web server and then loaded by another vulnerable computer, the malicious code will exploit the MS06-014 vulnerability to download and execute W32.Fujacks and several other Trojan horses onto the compromised computer.

### **Spreads through network shares**

Unfortunately, most computer users have a lack of knowledge of network security. Many people use passwords that are simple and easy to remember. W32.Fujacks uses a long list of user names and passwords to connect to network neighbours. If successful, it copies itself to that compromised computer.

### **Auto-run feature of removable disks**

Along with the popularization of digital media, more and more people use removable hard disks and flash drives to save and transfer files and data. W32.Fujacks copies itself to the root folder and inserts the file autorun.inf in to that folder. When an infected removable disk is attached to another clean computer with an auto-run feature enabled and the computer user clicks the infected disk, then W32.Fujacks will be executed.

## **Destructive payload**

W32.Fujacks searches for and deletes all files with an extension of .gho, which is a hard disk image file, created by Symantec Ghost. By doing this, the backup data will be lost and it will be harder to restore the system.

Although W32.Fujacks and its variants are not highly complex, it can still be seen from the aforementioned reasons that due to the motivation of profit, it is widely spread and can have a large impact to Chinese users.

## **Who is paying for W32.Fujacks**

Unlike most traditional viruses, the outbreak of W32.Fujacks is beneficated and driven by its large profit chain.

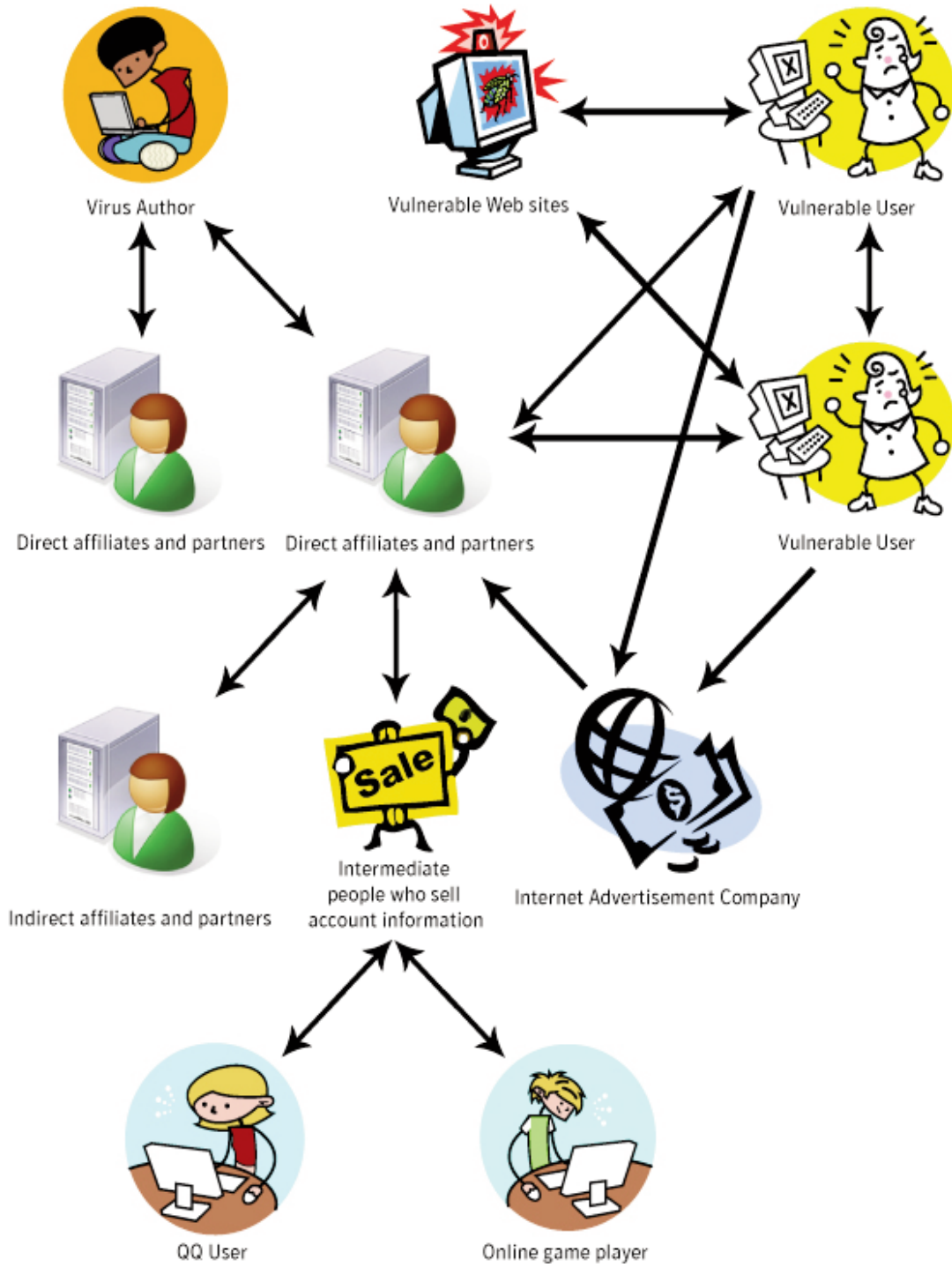
Mr Li is only the source of this profit chain. According to his testimony, he sold roughly 20 copies of W32.Fujacks for 500 to 1000 RMB (Yuan Renminbi) per copy (approximately 64 to 129 US dollars). On 24th Jan 2007, his classmate, Mr Lei Lei, sold 2000 compromised computers for him. Mr Shun Zhang is in charge of reselling and spreading W32.Fujacks. From the time Mr. Lei contacted Mr Li until he was arrested, he transferred between 3500 RMB and 6500 RMB (\$452-\$839) to Mr Li's account daily. Mr Li has received more than 150,000 RMB (\$19,374) from Mr. Lei. Compared to Mr Li, Mr Shun Zhang has made even more money.

The other core member, Mr Lei Wang, bought a Jeep with the money that he made from W32.Fujacks in less than 1 month. Mr Lei Wang has been quoted as saying: "This is a better money making industry than real estate."

The question is "who is paying for W32.Fujacks?"

The diagram on the following page shows the profit chain of W32.Fujacks.

# The Panda Outlaw: W32.Fujacks



Partners usually register a domain and server with a fake name or use a vulnerable Web site for spreading the Trojan horse and collecting stolen information.

*Domain name: 21380.COM*

*Registrant Contact:*

*hygfyhjgkj*

*hgh jkgkjgkkg (weiyudns@56.com)*

*+21.236525687*

*Fax: +21.236525687*

*lkjl;k;lk;lk*

*kjlhkjlh, jialila 023652*

*US*

When partners bought W32.Fujacks, they may have used Internet cafes, email and many other approaches to spread W32.Fujacks. These infected users may infect many others, and they may accidentally upload an infected page to some Web sites. All infected computers will automatically connect to a predefined address to download and execute more Trojan horses.

Next, these computers will be controlled by the partner. The partner may then use the computer for ad clicking. These clicks may generate a huge amount of money for the partner.

Furthermore, the partner may also sell access permission to the compromised computer to other intermediate persons. These intermediate people may use network exchange Web sites and BBS to sell the account information to other QQ users or online game players. According to a study, in Li Sui, Zhejiang province, which is the city where Mr Shun Zhang was arrested, a whole malware industry has already been found. Some people in charge of spreading the virus, some people in charge of collecting stolen account information, and some other people in charge of reselling accounts are all working for the malware industry. Infostealer.Lingling is another example its operator also comes from Li Sui, Zhejiang.

These partners may also resell W32.Fujacks to other indirect partners and make more money from them. All of these people are helping W32.Fujacks to spread more rapidly in order to increase their own profits.

## **Is it over yet**

Although the author of W32.Fujacks and his associates have already been arrested, according to recent reports, along with the publishing of W32.Fujacks's source code, several new variants have been found. W32.Fujacks and its variants may continue to spread and challenge anti-virus vendors.

On the other hand, the new Chinese Criminal Act has defined cyber crime. Unfortunately, it is still insuffi-

cient. The outbreak of W32.Fujacks by Mr Li and his friends, the oldest of whom is 25 years old and the youngest is only 21 years old, demonstrates the problem of young people undertaking cyber crime in China. Due to the motivation of profit and a lack of knowledge of Criminal law, such attacks may continue to cause more impact.

## **How to prevent this kind of attack**

How do we prevent this kind of attack and minimize the potential loss?

1. Never run executable from unknown source. As an online game player, it is also very important not to run any third party tools. Many viruses and Trojan horses use social engineering techniques to disguise themselves as assistant tools or crack programs and mislead a user to run the program.
2. Install latest security updates in time. This can prevent infection from threats that exploit known vulnerabilities.
3. Install antivirus software and update its definition set in time. Enable auto-protect function to ensure that the computer will not be infected with any unknown threats
4. Install a firewall to block malicious network scans and secure local data.
5. Use a strong password and change it frequently.
6. Disable the auto-run feature to prevent infection from starting a program by mistake.
7. If possible, backup all important data to non-erasable media, such as CDs, DVDs, etc.
8. Use online backup programs to backup contents onto a secure server.

## **Conclusion**

As a nationally treasured symbol, the Panda has never had its name darkened as it has of late. The outbreak of W32.Fujacks has highlighted several implications for a whole spectrum of people including law enforcement, IT services, security providers, and end users.

Organised crime motivated purely by profit is proving to be a serious issue to be dealt with. There is a need to improve our understanding, detection and deterrent of such activities.

Improvements in security products will only address part of this problem. Computer users need to become more aware of the techniques used by cyber criminals in order to recognize and avoid such threats when they are encountered. There are lessons to be learned from W32.Fujacks and we all need to learn them fast.



## **About Symantec**

Symantec is the global leader in information security, providing a broad range of software, appliances, and services designed to help individuals, small and mid-sized businesses, and large enterprises secure and manage their IT infrastructure.

Symantec's Norton™ brand of products is the worldwide leader in consumer security and problem-solving solutions.

Headquartered in Cupertino, California, Symantec has operations in 35 countries.

More information is available at [www.symantec.com](http://www.symantec.com).

Symantec has worldwide operations in 35 countries. For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 800 745 6054.

Symantec Corporation  
World Headquarters  
20330 Stevens Creek Boulevard  
Cupertino, CA 95014 USA  
408 517 8000  
800 721 3934  
[www.symantec.com](http://www.symantec.com)

Symantec and the Symantec logo are U.S. registered trademarks of Symantec Corporation. Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Other brand and product names are trademarks of their respective holder(s). Any technical information that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation. NO WARRANTY. The technical information is being delivered to you as-is and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained herein is at the risk of the user. Copyright © 2007 Symantec Corporation. All rights reserved.  
04/05 10406630