A study of malwares attack on online shopping users in China

Chien Hua(Royce) Lu
Qihoo 360
lujianhua@360.cn

Abstract

Online shopping has become increasingly popular in China. 37.8% of the 513 million Internet users have online shopping experience. In 2011, the total sales volume of online shopping reached US$127 billion [1]. One of the largest online shopping sites, taobao.com, sells 48,000 items every minute [3]. It is no surprise that the users of online shopping sites have become a juicy target for malware authors.

In this paper, we will introduce malware that targets online shoppers in China. How does the malware propagate? How does this type of malware evade detection by security software? Most importantly, how does the malware steal money from the users? We will share detailed information about this kind of threat.

KEY WORDS: spreading channels; bypass reputation checking; abnormal compression format; modified payment page; keylogging;

1. Introduction

There are over 500 million internet users in China; around 40% of the users have online shopping experience. It is a big business market and a huge target for the malware authors to profit. The largest instant messenger in China, QQ, has 711.7 million active user accounts [2]. According to a Chinese browser statistic, IE has a 51.52% market share in Aug 2012 [4]. Chinese internet users share similar user habits, most of them using the same browser and instant messenger. If attackers found a way to profit, it would cover a large portion of Chinese internet users.

Here are some numbers to help us to understand how active malwares are in China. In 2011, 360SafeGuard intercepted around 1.056 billion malwares, based on file fingerprint [6]. Figure 1 shows November has more new malwares than any other months. 140 million, equates to 54 new malwares every minute. Under 360SafeGuard Cloud-based anti-malware system, most of the malwares were detectable shortly after being released into the wild. This forces attackers to use automation tools to speed up the malware variation.

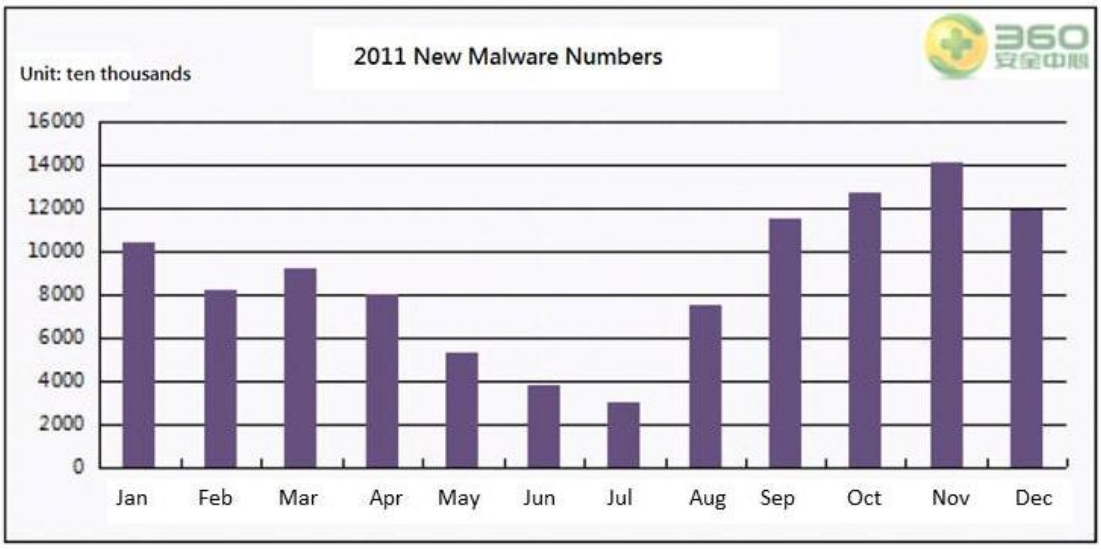

Figure 1: 2011 New Malware Numbers

We found a very cleaver type of malware that targets online shoppers on Windows; we call it "online shopping malware". Usually user will download it from a scam shopping site, thinking it is a coupon or a picture of the product. Attackers will also use instant messenger to spread the malware. Once on the user's system, it will cause financial loss whenever the user performs an online payment activity.

In section 2, we will discuss two primary spreading channels used by online shopping malwares. Section 3 describes the methods that online shopping malwares used to bypass the security software. In Section 4, we will explain how malware modify the payment page and other payloads that it can perform on the user's computer. Section 5 is the conclusion.

2. Phishing site and instant messenger

Basiclly there are two channels used by the online shopping malware to spread, phishing site and instant messenger. Both methods are very effective because attackers know the expectation of the user.

Phishing Site

In 2011, 30.73% of phishing sites were scam shopping sites in China [6]. Ususally these online shopping sites hosting the malware will offer very low prices to attract users to contact the online customer service. The customer service, who is actually the attacker, will send the malware to the user disguised as a coupon or as pictures of the merchandises or as how to buy instruction. With a little icon trick, they can change the icon of the malicious executable to a Windows jpeg icon or a picture of some fancy clothes. Users will fall for the trick and double click and execute the malware. Figure 3 shows two examples of the malwares that change its icon to fool the user.

Figure 2: phishing link under the internet streaming player

Figure 3: two example of the icon trick

Instant messenger

Instant messenger is a great platform for social engineering. Sending the malware by making the malware to a file that will pique people's interest; broadcast discount news in shopping groups, or a picture of a pretty girl in chatting groups.

Sometimes attackers will use private message instead of broadcast message because broadcast messages will attract the user's attention, people will be more caution and will not be as easily taken in. Using private message there will be more space for social engineering.

Using stolen instant messenger account is another way to perform social engineering. By simple words and social engineering on the file name, ex "MyNewboyfriend.jpg", it is quite convincing for the user that the message could be trusted.

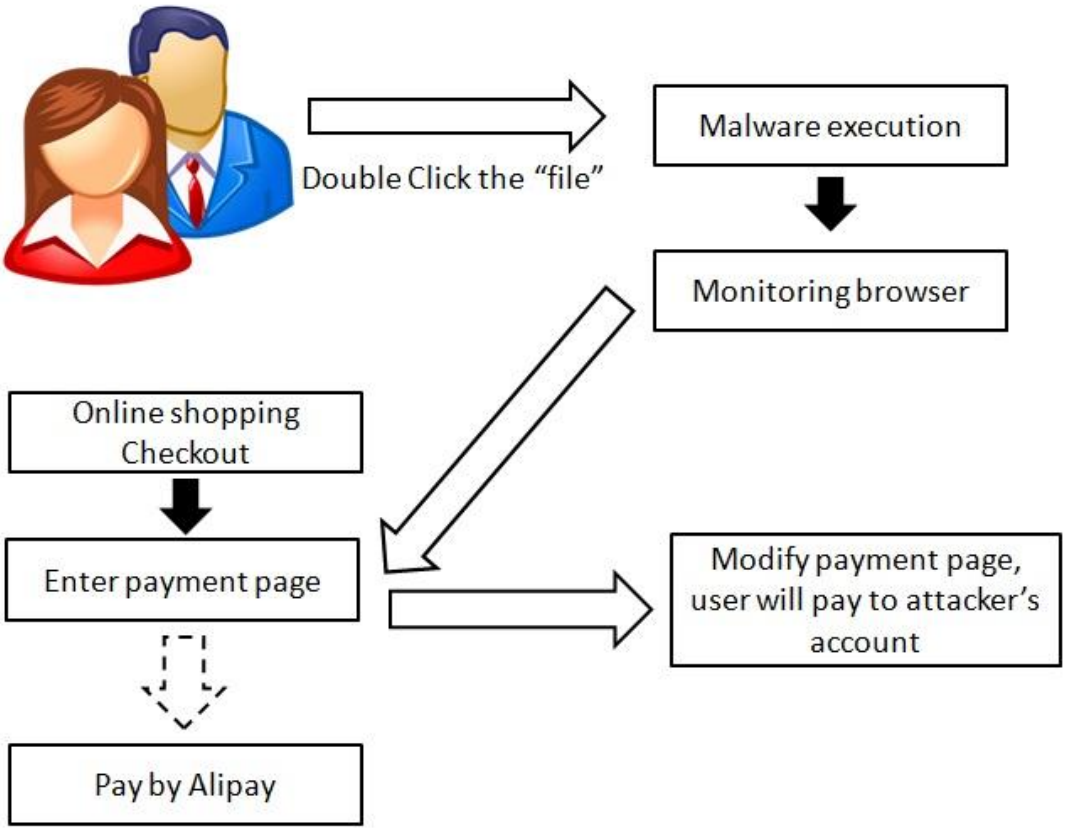

Figure 4: activity flow of the online shopping malware

After user executes the malware, the major thing it will do is monitor the browser, shown in figure 4. When it found the user is at a payment page, the malware will modify the request and the user's payment will actually go to attacker's bank account.

3. Challenge for Security Software

Challenges

Usually before releasing the malware, the author will make sure major anti-malware products with the latest update cannot detect the malware's presence. For the file signature detection, malware can obscure the binary to change the signature. For the file hash detection, malware can change the hash of the binary by adding random data at suitable places in the file. For the behavior monitoring detection, it can inject code into a process with a good reputation, executing payload under the host process's context. Behavior-monitoring engine usually will ignore good reputation process's actions for performance and compatibility considerations. If an unknown process has a legitimate digital signature, in most cases, behavior monitor will add it to the exception list. Disabling or terminating the anti-malware products is also an option.

Once a new malware pattern is available, the malware will be detected and will no longer be able to propagate. The length of the time window between the malware's release and a pattern update is proportional to how much profit the malware author can earn. The longer the malware stays unknown, the more profit the attacker can earn.

Automation tools are able to speed up the file signature and hash variation process. However, there is no automation tool to help bypass behavior monitor engine. In order to have a longer attack window, there are two points that malware authors will focus on.

1. Keep a low profile.
2. Running malicious code under the context of a process with a good reputation.

Through the icon trick introduced in the last section, it is easy to get user's trust. However, if a file with an unknown reputation is executed, most of the cloud-based security system will upload the features of the file, and the reputation will be established after analysis, which will result in a shorter attacking time window. In order to maximize profit, the online shopping malware authors utilize executable files with good reputations.

These good reputation executable file have one thing in common, they load certain DLLs, dynamic loaded libraries, with relative path, not full path. Attacker can place a DLL under the same folder and the good reputation process will load it. The DLLs in these folders are usually only loaders and will not exhibit any malicious behaviors. The true malicious instructions are encrypted in another file and the loader DLL will decrypt and perform the instructions. This approach will help the loader DLL avoid getting a bad reputation from the automation analyze system. So even after a DLL sample is captured, it will take longer than normal to be flagged as a malicious file, keeping the whole attack profile low. Figure 5 is an example.

Because some behavior monitor engines will add process with legitimate digital signature to the exception list, we observed that online shopping malwares were using stolen digital signature to sign their binary. Malware authors can also get digital signature by money. Combined with the icon trick and the loader DLL, it becomes a challenge for security software

to defend.

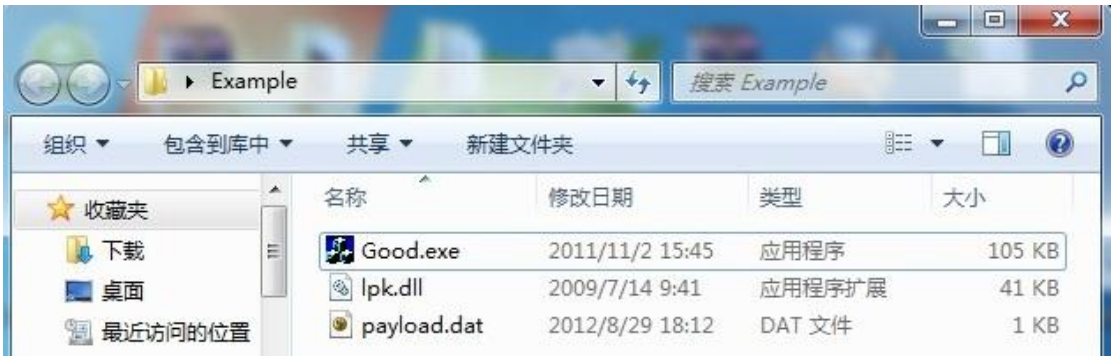

Figure 5: Malware use good reputation executable

Compressed file

In order to send several files through instant messenger at one time, attacker will compress all files into one file. Scanning a compressed file challenges the anti-malware decompression engine; if decompression fails, malware could bypass the defense or even crash the security software. Some engines employ open source library to decompress the file, if there is a vulnerability it could result in a very serious security issue. For example, CVE-2005-3051 [7] in 7-zip could allow attacker to execute arbitrary code remotely.

To help understand how compressed file challenge security software, we list several common "compression tactics" that are used by the online shopping malware:

1.Compression files with password. With password approach, the security software has to have the password for scanning. Anti-malware could popup a window to ask for the password. However, if the user enters the wrong password, the malware will remain undetectable.

Figure 6: Ask user to help enter the password of the compression file

2.Compression file bomb (Arc.Bomb). For performance issue, some security software will simplify the checking flow on a very large file, for example skip calculating the hash value of a file that is larger than 1G. Attacker use this fact by creating malwares with a large file size and high compression ratio. After compression, the total file size is small enough to transmit without causing any user inconvenience. Malware could then bypass the

check because of the special treatment given to large files.

3. Large numbers of files. If there are too many files inside the compressed file, for performance consideration anti-malware will stop processing the files after meeting certain threshold. For example, some thresholds are set as more than one hundred files inside, twenty folders deep, and compression file in the compression file for over ten levels. These could cause high CPU issue or even an unresponsive computer. Attackers can pack the malware in the compressed file that meet one or all of these threshold conditions causing anti-malware high CPU issues, or bypass the security check completely if the anti-malware drop the processing.

4. Abnormal compression format. If the decompression error-handling ability is different between the anti-malware and the compression software, attacker could make a compression file that has abnormal compression format to bypass the scanning of the anti-malware. Figure 7 shows a RAR file with a header CRC Error. The open source library, 7zip [8], will stop processing after finding a CRC error. However, user can extract everything by winrar. Winrar will warning user header is corrupt, and extract the files as usual.

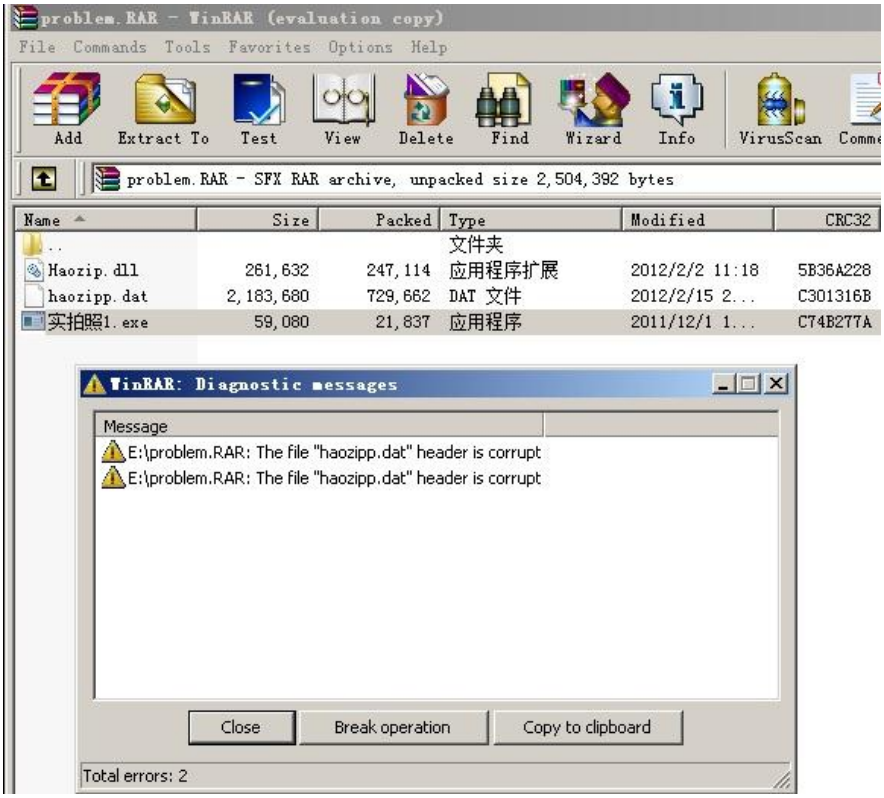

Figure 7: Winrar found a header CRC error, but the binary can be extract successfully.

Another example is modifying a ZIP header field, changing the uncompressed file size to zero. 7zip will output a file with zero size. Winrar can decompress the file with the correct size. If the error handling decision is different between the anti-malware and the user's compression tool, it is very possible malwares could use it to bypass the security check.

Figure 9: Uncompressed file size is zero.

5.Hybrid format. Some of the online shopping malwares employ hybrid format compression to bypass the scanning. Hybrid format compressed file has at least two formats in one file. As shown in figure 10, the compression file has the extension ".rar", but the beginning of the file is compound file format[9]. In the compound file format section it stores normal files. After the compound file format section is the RAR format which stores the malicious files. Take 7zip and winrar as comparison, 7zip only shows the files in the compound file format, while winrar only shows files in the rar format, figure 11 is the result. If the anti-malware only scans the compound file format and the user is using winrar, malicious files will bypass the protection of the anti-malware.

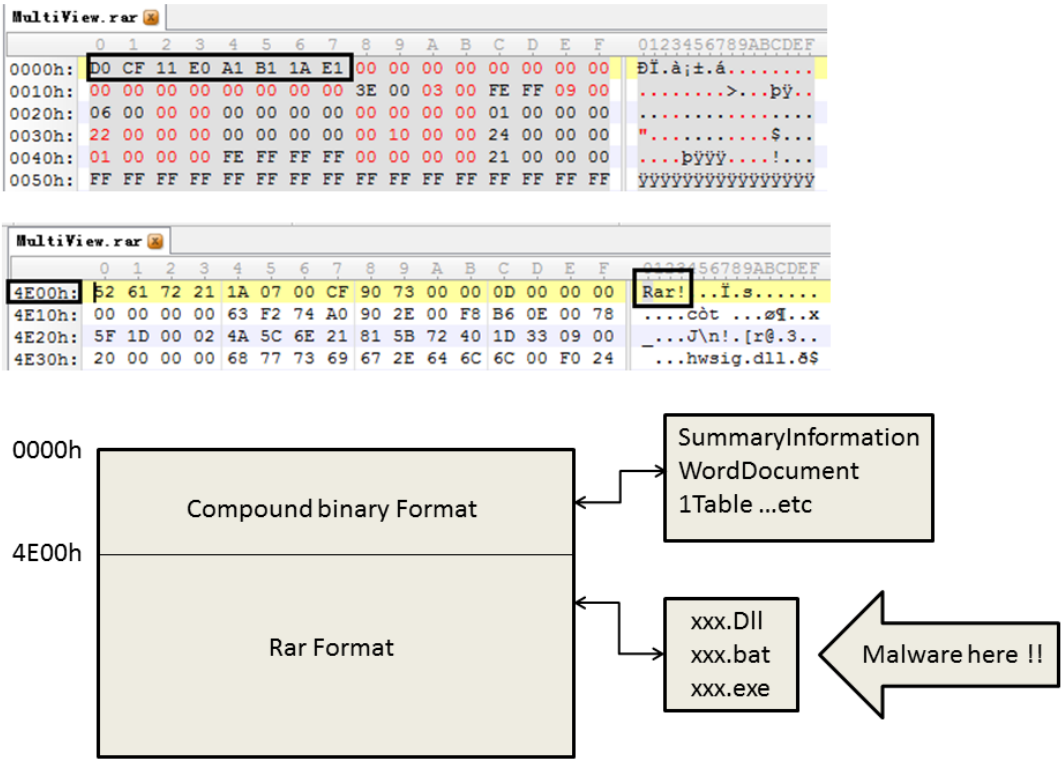

Figure 10: Hybrid format example

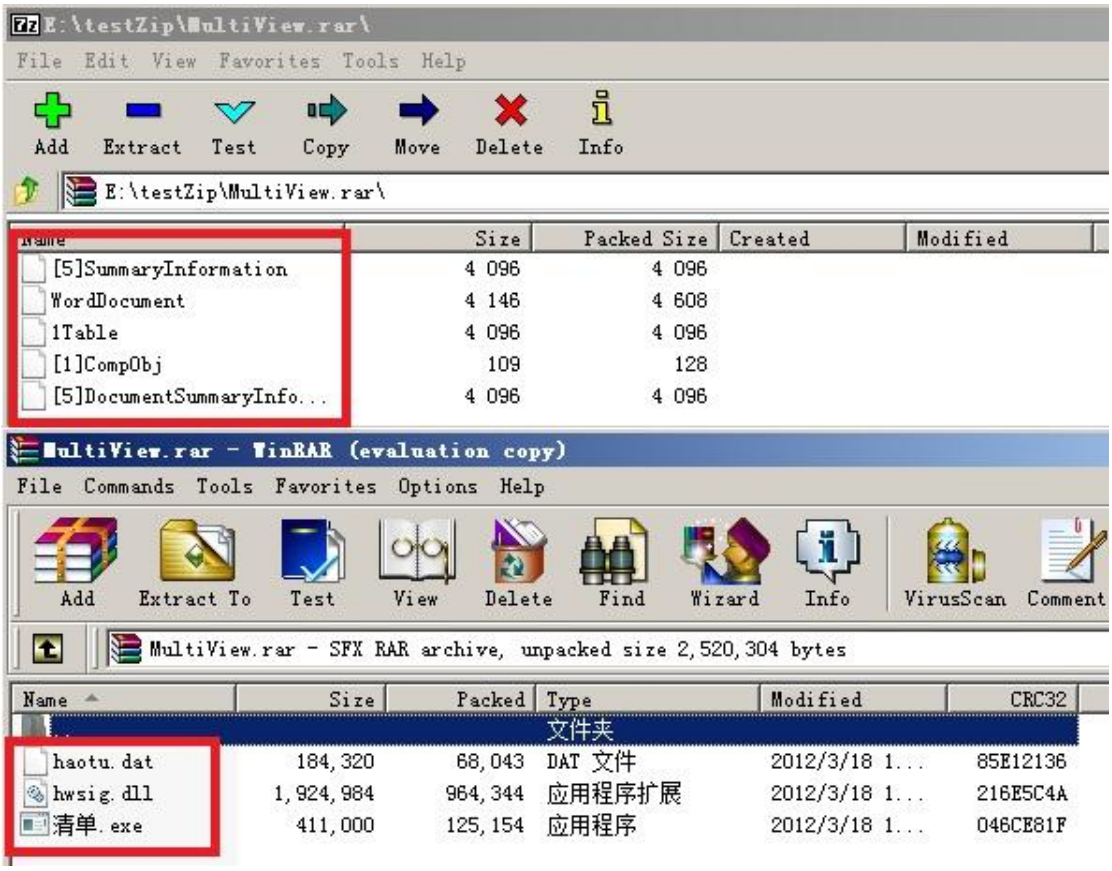

Figure 11: Different decompress engine list different files.

4. Attacking user

Modified payment page

The principle of the online shopping malware is to monitor the browser address bar, modify the webpage contents to redirect the money to malware author's account when the user is using the target payment page. This tecnique can be used when the victim is doing online shopping, online recharging or any other online payment. For the malware that is targeting IE, it can get window contents DOM-tree and COM interface by sending WM_HTML_GET_OBJECT message to IE. Through the interface malware can access and modify the webpage contents.

Take taboo.com checkout flow as an example, in Figure 12, there are two opportunities for online shopping malware to hijack the shopping process. After user checkout, taboo will forward the order information to Alipay. Alipay is a third party escrow-based online-payment platform. Malware can change the action of the checkout button and send a different order info to alipay.com. The victim will find that their own orders were never paid, but the alipay account history show they paid for someone else's cell phone bill or e-lottery tickets.

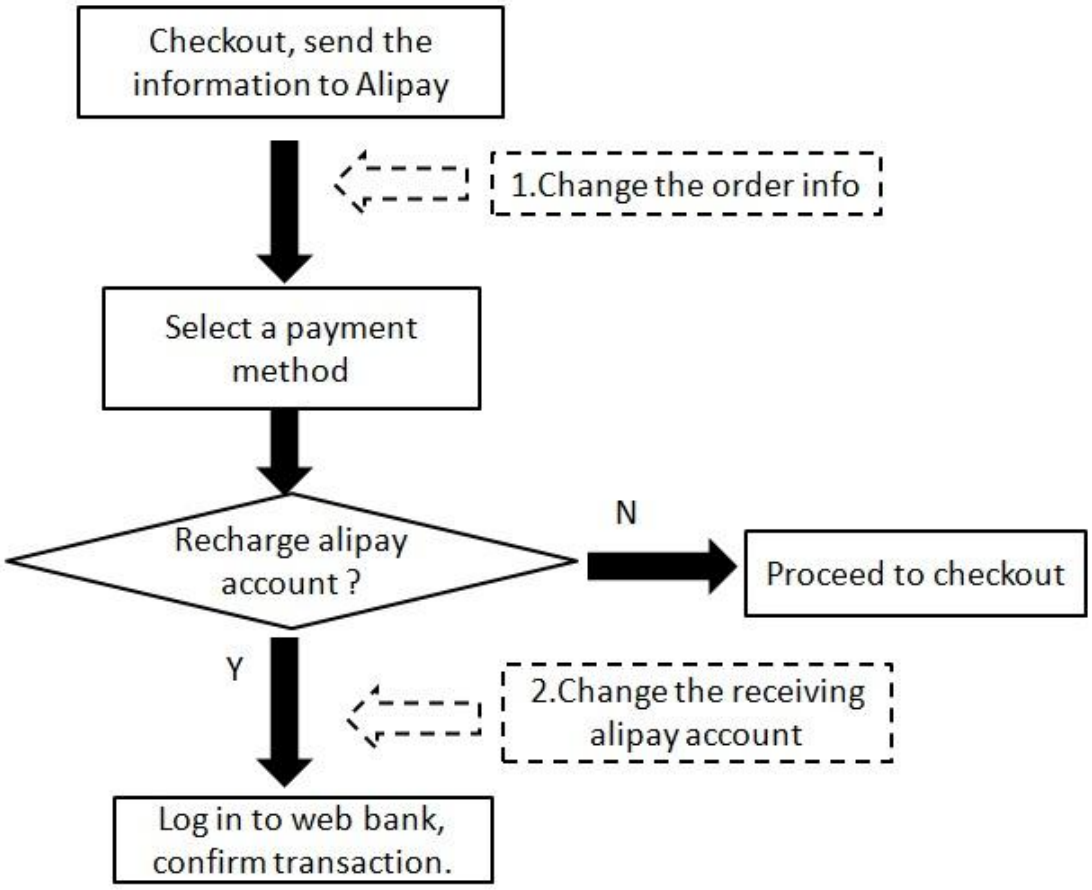

Figure 12: checkout flow at taboo.com, dash box indicate possible attacking methods

The second attack opportunity is when the user wants to recharge their alipay account. Malware change the action of the button "go to web bank", instead of sending a http GET to the alipay server, it sends a http POST to the malicioius server. The malicious server will

based on the online-payment protocol create a new request to the bank server and alipay server and return the new web bank payment page to the user. Once user confirm the transaction, the money will go to attacker's alipay account. The malware on the local machine will be responsible for modify the receiving bank account info and the amount of money on the web bank payment to fool the user. Figure 13 shows the attack steps.

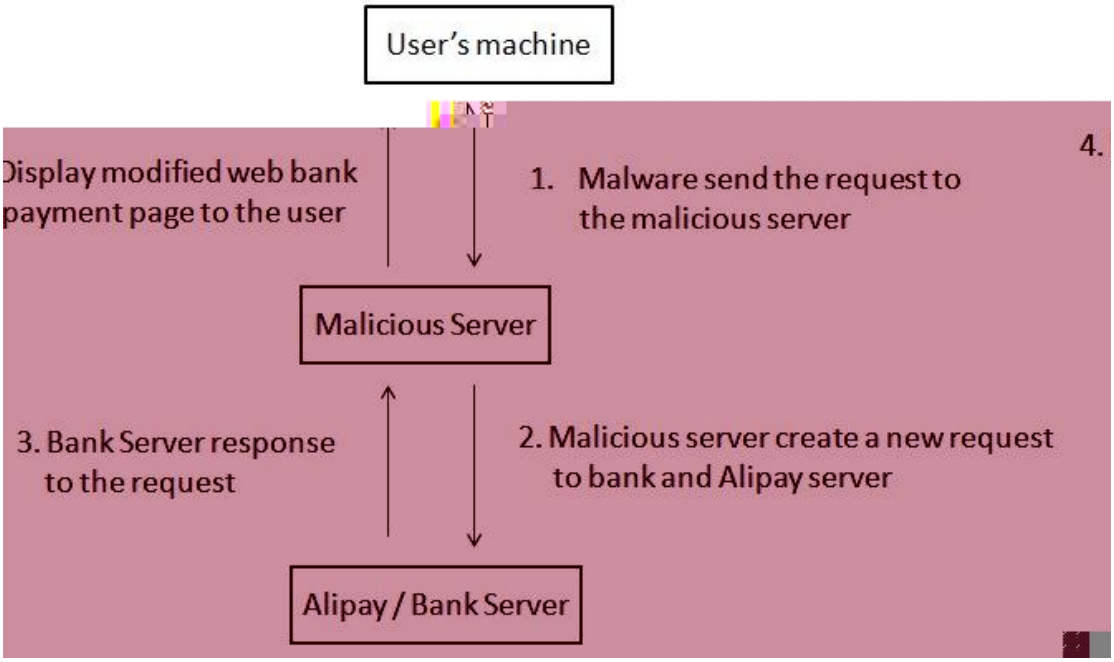

Figure 13: attack steps of the online shopping malware

Online account theft

Stolen online account could result in privacy disclosure and loss of virtual assets. Some of the online shopping malware also pack keylogging ability, targeting popular online platform accounts. Take QQ as an example, we saw many clever methods for stealing QQ passwords:

1. Cover a transparent window on the QQ password window to get the password input
2. Insert a window to become the parent of the password window, it will get the input message.
3. Make QQ main window invisible then draw a fake QQ main window
4. Use AttachThreadInput API
5. Use a transparent window to get input, then send input to QQ, as shown in Figure 14 and 15.

Malware gets input and send it to the password window, user is unaware. In the picture we removed transparent property of the malware.

Figure 14: Stealing QQ password

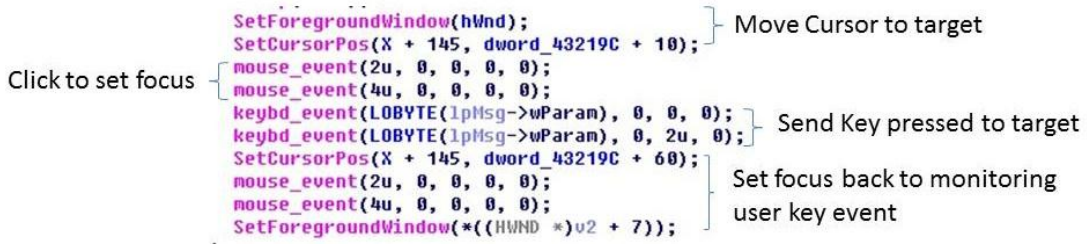

Figure 15: analyze of the malicious sample in figure 14

5. Conclusion

Online shopping malware could cause financial loss. The propagation through phishing site and instant messenger is very easy if users don't have enough security awareness. We conclude three important anti-malware rules to mitigate the threat of online shopping malware, these rules could also apply to mitigate other malware threat:

Run more strict security policy at important user scenario. This rule also help to balance the user experience and security. For example, avoiding interrupting user when playing game or watching movie; executing more strict policy when user is doing online shopping activity or receiving file from external source. Anti-malware could run security rule like only allow execution of good reputation code until the online transaction end.

Speed up response. Speeding up the response time could cut the profit from online shopping malware. For cloud-base security solution it could add defence policies at the back-end server and respond very quick to the threat, instead of updating the rules on millions of users's machines. Once the profit is below a certain degree, the malware author will stop the activity.

Have multiple defense mechanisms. Preventing user from visiting phishing sites, compression file checking, file signature checking, behavior monitoring, file reputation checking, online shopping protection…etc. Like military strategy, defence in depth. Making the malware bypass all defense mechanisms will also raise the cost for the malware authors.

6. Acknowledgements

Thanks the support of my colleagues. Xia Orui, Sun Xiaojun and Wei Zhijiang provided many information on the compression file section and modified payment page section. Wang Liang, Hama Xianren, and Fred Jeng gave many valuable suggestion to this paper.

7. References

[1] China internet network information center. http://www.cnnic.net.cn/hlwfzyj/

[2] Tencent QQ. http://en.wikipedia.org/wiki/Tencent_QQ

[3] Taobao reveals online shopping trends for 2010. http://news.alibaba.com/article/detail/alibaba/100433518-1-taobao-reveals-online-shopping-trends.html

[4] China Internet Browser Market Share for Augest 2012. http://www.chinainternetwatch.com/1571/china-internet-browser-market-share-for-aug-2012/

[5] Qihoo 360 http://corp.360.cn/

[6] "2011-2012China Internet Security Report" http://wenku.baidu.com/view/f3cf76a4b0717fd5360cdc32.html

[7] Vulnerability Summary for CVE-2005-3015. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-3051

[8] 7Zip. http://www.7-zip.org/

[9] Daniel Rentz. Microsoft Compound Document File Format. http://www.openoffice.org/sc/compdocfileformat.pdf